НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломної роботи
фахового молодшого бакалавра

на тему: **Аналіз технологій і протоколів передачі даних на різних відстанях та передачі повідомлень**

Виконав студент IV курсу, групи ТК-41
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Телекомунікації та комп'ютерні технології»
Хомик Максим Петрович

Керівник _____ Олександра ЗАГОРЯНСЬКА
(підпис)

Нормоконтролер _____ Володимир ПЛІШ
(підпис)

Рецензент _____ Олег ЛЕЩАК
(підпис)

Голова ЕК _____ Андрій ВАХ
(підпис)

Члени ЕК _____ Ігор ТИБЕЛЬ
(підпис)

_____ Володимир ПЛІШ
(підпис)

Дипломна робота захищена в ЕК «__» _____ 2025 р.

з оцінкою «_____»

Львів 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Циклова комісія ***Телекомунікації***
Освітньо-професійний ступінь ***Фаховий молодший бакалавр***
Освітньо-професійна програма ***Телекомунікації та комп'ютерні технології***
Спеціальність ***172 Телекомунікації та радіотехніка***

ЗАТВЕРДЖУЮ
Завідувач відділення
«Телекомунікацій та
комп'ютерних технологій»
_____ Ігор ТИБЕЛЬ
« 25 » квітня 2025 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ ЗДОБУВАЧУ

Хомику Максиму Петровичу
(прізвище, ім'я та по батькові)

1.Тема роботи *Аналіз технологій і протоколів передачі даних на різних відстанях та передачі повідомлень*

Керівник роботи *Олександра ЗАГОРЯНСЬКА*
викладач вищої категорії,
(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом директора від " 20 " березня 2025 року № 20-СТ

2. Строк подання студентом роботи "10" червня 2025 року

3. Вихідні дані до роботи *3.1 Розглянути моделі IoT згідно рекомендації Y.2060;*

3.2 Проаналізувати основний механізм функціонування Інтернету речей

3.3 Порівняти переваги та недоліки IoT;

3.4 Дослідити можливості бездротового зв'язку в інтернеті речей на малих відстанях.

4. Зміст розрахунково-пояснювальної записки

4.1 Принципи дослідження та функціонування мережі IoT

4.2 Дослідження та аналіз протоколів та технологій передачі даних у мережах IoT

4.3 Тенденції та перспективи розвитку технологій передачі даних IoT в Україні

4.4 Техніко-економічне обгрунтування.

4.5 Охорона праці та безпека життедіяльності

5. Перелік графічного матеріалу

5.1.	*Структура мережі Інтернету речей*
5.2.	*Структура IoT*
5.3.	*Архітектура мережі LoRaWAN*
5.4.	*Принцип роботи безпілотних транспортних засобів*
5.5	*Квадрокоптери в розумних містах*

6. Консультанти розділів дипломної роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	Завдання отримав
Техніко-економічне обґрунтовування	*Мар'яна СМУК викладач вищої категорії*	*25.04.2025р.*	*25.04.2025р*
Охорона праці та безпека життєдіяльності	*Олена МЕЛЬНИКОВА викладач першої категорії*	*25.04.2025р.*	*25.04.2025р.*

7. Дата видачі завдання « 25» квітня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання	Примітка
1	*Вступ.*	*25.04-01.05*	
2	*Принципи дослідження та функціонування мережі IoT*	*02.05-08.05*	
3	*Дослідження та аналіз протоколів та технологій передачі даних у мережах IoT*	*09.05-15.05*	
4	*Тенденції та перспективи розвитку технологій передачі даних IoT в Україні*	*16.05-22.05*	
5	*Техніко – економічне обґрунтування*	*23.05-29.05*	
6	*Охорона праці та безпека життєдіяльності*	*30.05-03.06*	
7	*Висновки*	*04.06-05.06*	
8	*Підготовка графічного матеріалу.*	*06.06-09.06*	

Здобувач _____ *Максим ХОМИК*
(підпис) (ім'я, прізвище)

Керівник роботи _____ *Олександра ЗАГОРЯНСЬКА*
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Текстова частина дипломної роботи: 73 с., 22 рис., 5табл., 10 джерел.

Об’єкт дослідження – є технології передачі даних в рамках Internet of Things (IoT)

Мета роботи – є здійснення порівняльного аналізу характеристик протоколів та технологій передачі даних на довгі та короткі відстані та протоколів передачі повідомлень.

Метод дослідження –включав аналіз науково-технічної літератури, статей, публікацій та офіційних документів з питань Internet of Things (IoT)

Дана дипломна робота складається з трьох основних частин, які охоплюють аналіз архітектури, моделі та принципів дії Internet of Things (IoT), порівняльний аналіз характеристик протоколів і технологій передачі даних на довгі та короткі відстані, а також аналіз сучасного стану та перспектив розвитку технологій передачі даних в Україні.

Досліджено принцип роботи цих систем, а також розглянуто їх переваги та недоліки. Проведено порівняльний аналіз базових характеристик цих протоколів та технологій передачі даних та повідомлень.

Здійснено аналіз сучасного стану та перспектив розвитку технологій передачі даних IoT в Україні, враховуючи специфіку використання та інфраструктуру країни.

IOT, МЕРЕЖА, ДАТЧИК, РІВЕНЬ, ПРОТОКОЛ, ПЕРЕДАЧА ДАНИХ.

ЗМІСТ

ВСТУП

Інтернет речей (IoT) відкриває новий етап розвитку Інтернету, роблячи можливим з'єднання кожного об'єкта нашого повсякденного життя з мережею. Це значно посилює здатність до аналізу, передачі, збору та розподілу даних. Тепер кожна людина може трансформувати ці дані в структуровану інформацію, а потім у знання. IoT дозволяє нам ефективніше здійснювати збір, аналіз та отримання даних, які кілька років тому були недосяжними для звичайного користувача.

Концепція IoT не лише полягає в з'єднанні фізичних об'єктів за допомогою Інтернету для обміну інформацією між ними, але й сприяє розвитку методів аналізу, збереження та структурування цих даних. Під поняттям Інтернету речей розуміють не лише широкий спектр датчиків та пристроїв, що з'єднані з Інтернетом через безпровідні та провідні технології передачі даних, але також взаємодію між віртуальним та реальним світами, де відбувається взаємодія між пристроями та людьми.

Інтернет речей представляє собою глобальну мережу різноманітних пристроїв, які, під керуванням програмного забезпечення, приймають рішення щодо виконання різних дій без прямої участі людини. Окрім звичайних побутових приладів, таких як конвеєрні стрічки, чайники, годинники та пилососи, до цієї мережі також можуть бути підключені різні датчики (наприклад, ваги, вібрації, температури тощо). Такі пристрої здатні збирати інформацію та керувати різними процесами автоматично.

1 ПРИНЦИПИ ДОСЛІДЖЕННЯ ТА ФУНКЦІОНУВАННЯ МЕРЕЖІ IOT

1.1 Основні поняття архітектура та терміни, що характеризують мережу IoT

Мережа наступного покоління (NGN) – це інфраструктура з пакетною комутацією, яка забезпечує послуги електрозв'язку та використовує різноманітні широкосмугові технології транспортування, у тому числі з функцією якості обслуговування (QoS). Вона надає послуги без залежності від конкретних технологій транспортування, що використовуються.

Пристрій – це технічний засіб, який має основні можливості зв'язку, а також додаткові функції, такі як вимірювання, виконання операцій, збереження та обробка даних.

Інтернет речей (IoT) – це глобальна мережа, яка об'єднує фізичні та віртуальні об'єкти, забезпечуючи їх взаємодію та спільне використання інформаційних технологій для надання різноманітних послуг.

Архітектура пристроїв Інтернету речей включає чотири основних рівні: рівень сенсорів, мережевий рівень, рівень обробки даних та додатковий рівень з використанням рис.1.1. Нижче наведено детальний опис кожного з цих рівнів.

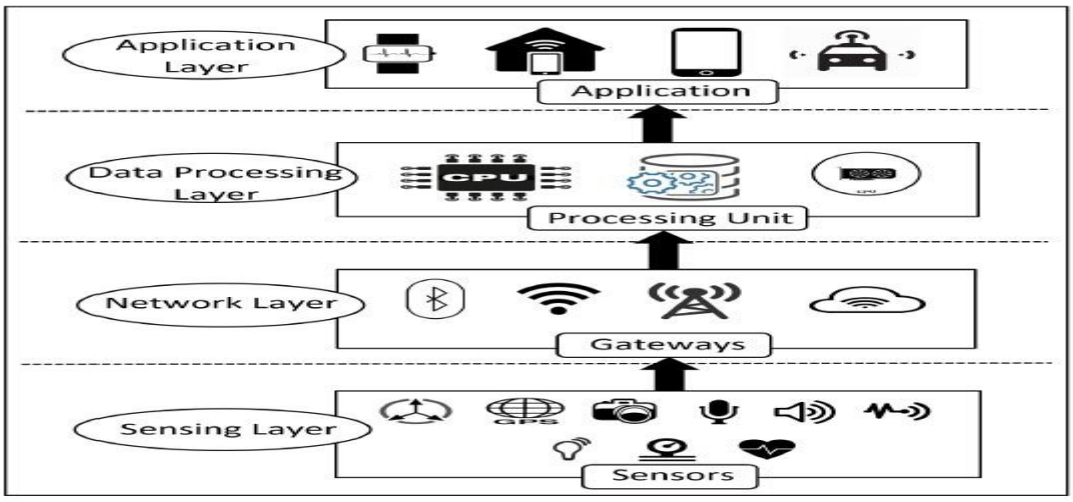

Рисунок 1.1 – Структура мережі Інтернету речей

На рівні датчиків головною метою є збір інформації про різні параметри навколишнього середовища за допомогою різноманітних периферійних пристроїв. Цей рівень включає різні типи датчиків, які вимірюють різні параметри. Для ефективного збору та передачі даних з датчиків до оброблювального блоку пристрою, використовується концентратор датчиків. Концентратор є центральною точкою з'єднання для декількох датчиків і забезпечує передачу даних до оброблювального блоку. Для забезпечення зв'язку між датчиками та оброблювальним блоком використовуються різні транспортні механізми, такі як Inter-Integrated Circuit (I2C) або Serial Peripheral Interface (SPI). Ці механізми забезпечують передачу даних між датчиками та програмними додатками для збору та обробки інформації.

Датчики в пристроях Інтернету речей можуть бути класифіковані на три основні категорії:

– Датчики руху, вони вимірюють зміни у русі та орієнтації пристроїв. Тут можна виділити два типи рухів: лінійний та кутовий. Лінійний рух відноситься до прямолінійного переміщення пристрою, тоді як кутовий рух вимірює обертальні зміни.

– Датчики навколишнього середовища, ці датчики, такі як датчики світла та тиску, реагують на зміни у параметрах навколишнього середовища. Вони допомагають пристроям приймати автономні рішення відповідно до отриманих даних. Наприклад, вони застосовуються у розумних замках, системах домашньої автоматизації та освітленні.

– Датчики місцезнаходження, ці датчики взаємодіють з фізичним розташуванням пристрою. Серед них можна виділити магнітні датчики, які допомагають фіксувати орієнтацію пристрою, та GPS-датчики, які використовуються для навігаційних цілей.

Мережевий рівень в мережі IoT використовується для забезпечення комунікаційного каналу між датчиками та іншими підключеними пристроями. Цей рівень реалізується через різноманітні комунікаційні технології, такі як Z-

Wave, LoRa, Wi-Fi, Bluetooth та інші, що дозволяють ефективно передавати дані між різними пристроями всередині мережі IoT.

Рівень обробки даних в мережі IoT відповідає за аналіз та обробку зібраних даних, які надходять від датчиків. Цей рівень виконує аналіз і приймає рішення на основі результатів обробки. У більшості IoT пристроїв, таких як смарт-годинники, розумні домашні системи та інші, рівень обробки даних також може зберігати отримані результати для подальшого використання. Крім того, він може передавати оброблені дані з одного пристрою на інший через мережевий рівень.

Рівень додатків в мережі IoT відображає результати аналізу та обробки даних, що проводиться на рівні обробки даних, за допомогою різних додатків на пристроях IoT. Цей рівень орієнтований на користувачів і відповідає за виконання різноманітних завдань для них. Наприклад, через рівень додатків користувач може керувати розумним будинком, взаємодіяти з розумними транспортними системами та виконувати інші завдання, пов'язані зі зручністю та автоматизацією в їхньому повсякденному житті.

1.2 Основний механізм функціонування Інтернету речей

На рис. 1.2 зображено схему простої мережі Інтернету речей (IoT). Найпростіша мережа IoT може складатися з трьох основних компонентів: сенсорів, які збирають дані, пристроїв для передачі цих даних (наприклад, мікроконтролерів або модулів зв'язку) і сервера або хмари, де дані аналізуються та обробляються.

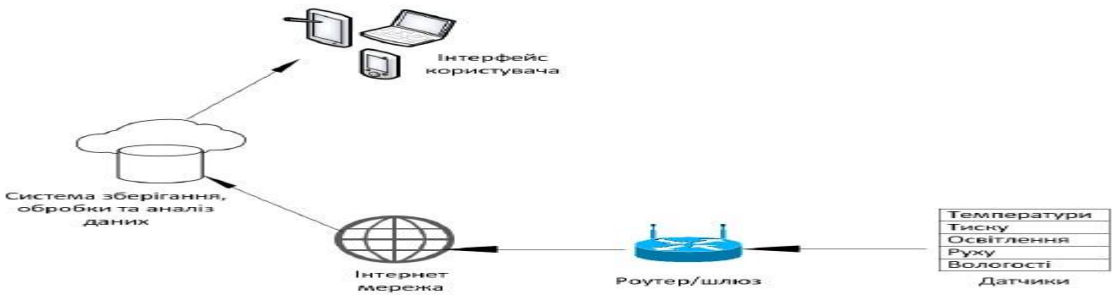

Рисунок 1.2 – Структура IoT

Сенсори розміщені у середовищі, яке вони моніторять (наприклад, в землі для вимірювання вологості, в промисловому обладнанні для виявлення відхилень у роботі тощо). Вони збирають дані про стан оточуючого середовища, які потім передаються через пристрої передачі даних.

Пристрої передачі даних можуть бути зв'язаними з сенсорами безпосередньо або через бездротові мережі, такі як Wi-Fi, Bluetooth, або навіть через провідне підключення. Вони отримують дані від сенсорів і пересилають їх до сервера або хмари, де дані обробляються.

Сервер або хмара приймає дані від пристроїв передачі даних, аналізує їх і може вживати різні заходи, такі як зберігання, візуалізація або навіть надсилання команд для керування пристроями на основі зібраних даних.

Принцип роботи Інтернету речей (IoT) ґрунтується на наступних основних етапах:

– Сенсорний рівень. На цьому етапі дані збираються за допомогою різноманітних сенсорів або пристроїв зібрання інформації. Ці дані можуть включати інформацію про температуру, вологість, рух, освітлення тощо.

– Мережевий рівень. Після збору даних вони передаються через мережу до центрального вузла або хмарного сервісу для подальшої обробки та аналізу.

– Обчислювальний рівень. На цьому етапі дані обробляються, аналізуються та інтерпретуються. Можливі дії на цьому етапі включають у себе фільтрацію даних, виявлення патернів та виконання різних алгоритмів аналізу даних.

– Дієвий рівень. Після обробки дані можуть бути використані для прийняття рішень або взаємодії зі світом. Це може включати автоматизацію пристроїв, надсилання повідомлень або звітів, керування системами тощо.

На першому етапі роботи IoT датчики або пристрої збирають різноманітні дані з оточуючого середовища. Це можуть бути прості вимірювання, такі як температура або вологість, або складніше, наприклад, запис відео на відеокамеру відеоспостереження.

Крім того, на цьому етапі можуть використовуватися не лише датчики, але й різноманітні пристрої. Наприклад, смартфон – це пристрій, обладнаний

кількома датчиками (камера, акселерометр, GPS тощо). Смартфон виконує роль не лише датчика, а й комплексного пристрою, здатного аналізувати та обробляти дані.

Таким чином, на цьому етапі інформація збирається з навколишнього середовища за допомогою датчиків або пристроїв, які можуть виконувати різні функції, що допомагають збирати дані для подальшої обробки та аналізу.

На другому етапі роботи IoT дані, зібрані датчиками або пристроями, передаються до хмарних сховищ за допомогою різних методів зв'язку. Це може включати стільникові мережі, супутникові мережі, Wi-Fi, Bluetooth, технології малопотужних широкосмугових мереж (LPWAN), або підключення безпосередньо до Інтернету через Ethernet.

Кожен метод підключення має свої переваги та обмеження, такі як споживання енергії, діапазон покриття та пропускна здатність. Вибір конкретного методу залежить від конкретних вимог і умов використання IoT в конкретній області.

Незалежно від методу підключення, головна мета - це передача даних до хмарного сховища для подальшої обробки, аналізу та використання. Це дозволяє зберігати дані в безпечному та доступному місці, забезпечуючи їх доступність з будь-якого пристрою або місця через Інтернет.

Після того, як дані потрапляють до хмарного сховища, вони піддаються обробці за допомогою програмного забезпечення. Цей процес може включати різноманітні операції, спрямовані на аналіз, інтерпретацію та використання отриманих даних.

Наприклад, програмне забезпечення може виконувати аналіз отриманих даних для виявлення певних патернів або трендів. Це може включати перевірку температурних даних на відповідність певним стандартам або порівняння їх з попередніми вимірами для виявлення змін.

Крім того, обробка даних може включати ідентифікацію об'єктів на відео, отриманому з камери відеоспостереження. Наприклад, програмне забезпечення

може використовувати алгоритми комп'ютерного зору для виявлення рухомих об'єктів або навіть розпізнавання осіб для забезпечення безпеки в приміщенні.

На етапі передачі інформації на інтерфейс користувача, інформація яка була оброблена і аналізована, передається кінцевому користувачеві через різні інтерфейси. Це може включати сповіщення користувача, такі як електронні листи, текстові повідомлення або сповіщення в додатках. Наприклад, користувач може отримати текстове повідомлення, яке попереджає його про високу температуру в холодильному приміщенні його компанії.

Крім цього, користувач може мати доступ до інтерфейсу, через який він може активно перевіряти систему. Це може бути мобільний додаток або веб-сторінка, через які користувач може перевірити стан системи, наприклад, переглянути відеозаписи з відеоспостереження в своєму будинку.

Проте це лише частина можливостей. Залежно від програми IoT, користувач може взаємодіяти з системою на відстані та впливати на її роботу. Наприклад, він може дистанційно регулювати температуру в приміщенні за допомогою мобільного додатка на своєму телефоні.

Деякі дії можуть виконуватися автоматично, без прямого втручання користувача. Наприклад, система може автоматично регулювати температуру в приміщенні відповідно до попередньо встановлених правил або повідомляти відповідні служби про події безпеки без необхідності у втручанні користувача.

Отже, система IoT забезпечує передачу корисної інформації користувачеві через різноманітні канали зв'язку та надає можливості для взаємодії та контролю за системою як на відстані, так і автоматично.

1.3 Розгляд моделі IoT згідно рекомендації Y.2060

На рис. 1.3 показана стандартна модель Інтернету речей (IoT) [4], яка описана в рекомендаціях Y.2060. Ця модель складається з чотирьох основних рівнів, а також з двох додаткових рівнів: рівня управління та рівня безпеки.

Основні рівні включають:

– Рівень застосування. Цей рівень охоплює всі різноманітні застосування Інтернету речей, включаючи промислові, побутові, медичні та інші.

– Рівень підтримки послуг та додатків. На цьому рівні забезпечується інфраструктура для підтримки різноманітних послуг та додатків, що працюють в середовищі Інтернету речей.

– Мережевий рівень. Цей рівень включає в себе мережеві технології, необхідні для забезпечення зв'язку між пристроями та системами в Інтернеті речей.

– Рівень пристроїв. На останньому рівні знаходяться самі пристрої, які збирають, обробляють та передають дані.

Додаткові рівні включають:

– Рівень управління. Цей рівень відповідає за управління ресурсами, конфігурацією та координацію різноманітних компонентів системи Інтернету речей.

– Рівень безпеки. Останній рівень забезпечує захист від різних загроз та атак на систему Інтернету речей, включаючи захист від несанкціонованого доступу, втрати даних та інших потенційних загроз.

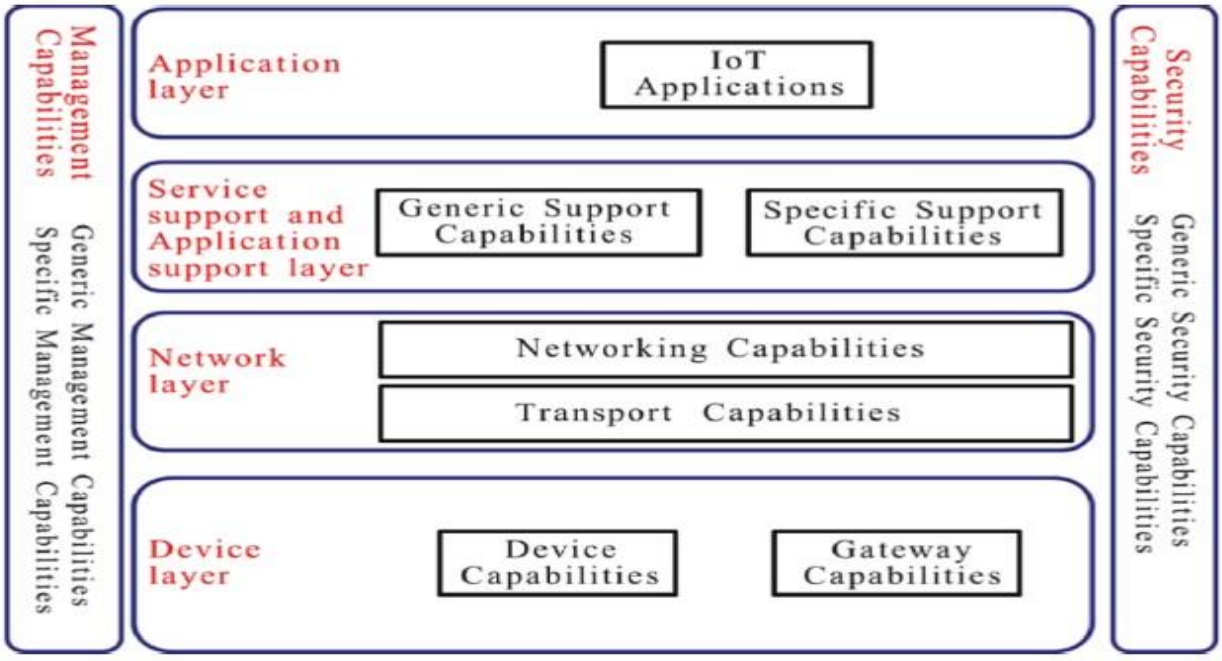

Рисунок 1.3 – Еталонна модель IoT

Прикладний рівень в Рекомендації Y.2060 не розглядається.

Рівень підтримки послуг та додатків включає дві групи можливостей:

– Загальні можливості підтримки, які можуть бути використані різними додатками. Ці можливості включають обробку та зберігання даних. Вони можуть бути активовані за допомогою спеціалізованих можливостей підтримки.

– Спеціалізовані можливості підтримки, які призначені для задоволення вимог різноманітних додатків. Ці можливості складаються з різних груп чітко визначених функцій, щоб надавати різні типи підтримки для різних програм IoT.

Мережевий рівень складається з двох типів можливостей:

– Можливості організації мереж, які забезпечують управління мережевим з'єднанням. Ці можливості включають функції керування доступом та ресурсами, управління мобільністю та автентифікацію, авторизацію та облік (AAA).

– Можливості транспортування, які забезпечують з'єднання для передачі даних, пов'язаних з послугами та додатками IoT, а також інформації щодо контролю та управління, пов'язаних з IoT.

Рівень пристроїв має різноманітні можливості, які можна логічно розділити на два види:

1. Можливості пристроїв:

– Пряма взаємодія з мережею зв'язку, пристрої можуть збирати та передавати інформацію безпосередньо у мережі зв'язку, не використовуючи шлюз.

– Непряма взаємодія з мережею зв'язку, пристрої можуть взаємодіяти з мережею зв'язку через шлюз. Це дозволяє пристроям отримувати та передавати інформацію за допомогою шлюзу, який обробляє комунікацію з мережею.

– Режим сну та пробудження, пристрої можуть мати можливість входити у режим сну для збереження енергії та пробудження для виконання завдань.

2. Можливості шлюзу:

– Підтримка декількох інтерфейсів, шлюз може підтримувати різні дротові та бездротові технології для з'єднання з пристроями.

– Перетворення протоколу, шлюз може конвертувати протоколи, щоб забезпечити сумісність між різними пристроями та мережами зв'язку. Наприклад, він може перетворювати протоколи на рівні пристроїв або мережевому рівні для забезпечення взаємодії між пристроями з різними технологіями.

Можливості управління в контексті Інтернету речей (IoT) включають традиційні класи управління несправностями, конфігурацією, обліком, показниками роботи та безпекою (FCAPS), що аналогічні засобам управління в традиційних мережах зв'язку.

Можливості управління IoT можна розділити на загальні та спеціалізовані:

1. Загальні можливості управління включають:

– Управління пристроями: дистанційне керування пристроями, діагностика, оновлення прошивки та програмного забезпечення, а також контроль стану пристроїв.

– Управління топологією локальної мережі.

– Управління трафіком і навантаженнями: виявлення умов перевантаження мережі та реалізація резервування ресурсів для термінових або життєво важливих потоків трафіку.

2. Спеціалізовані можливості управління тісно пов'язані з вимогами конкретних додатків IoT, таких як:

– Контроль лінії передачі електроенергії в розумних електричних мережах.

Можливості забезпечення безпеки поділяються на два види: загальні та спеціалізовані.

Загальні можливості забезпечення безпеки, які не залежать від конкретних додатків, включають:

– На рівні застосування, авторизація, автентифікація, збереження конфіденційності та цілісності даних, захист приватності, аудит безпеки та застосування антивірусних програм.

– На мережевому рівні, авторизація, автентифікація, захист конфіденційності та цілісності даних передачі та сигналізації.

– На рівні пристроїв, автентифікація, авторизація, перевірка цілісності пристрою, управління доступом, захист конфіденційності та цілісності даних.

Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами конкретних додатків, наприклад, забезпечення безпеки мобільних платежів або інших конкретних сценаріїв застосування.

1.4 Переваги та недоліки IoT

До переваг Інтернету речей можна віднести:

– Взаємозв'язок між пристроями. IoT сприяє взаємодії між пристроями, що відомо як зв'язок між машинами (M2M). Це сприяє покращенню комунікації та співпраці між різними пристроями, що в результаті забезпечує більшу ефективність та зручність у використанні. Такий зв'язок дозволяє фізичним пристроям залишатися підключеними та співпрацювати один з одним, що робить систему більш гнучкою та функціональною.

– Переваги в області автоматизації та управління в IoT полягають у можливості підключення та керування фізичними об'єктами через цифрові технології та бездротову інфраструктуру. Це відкриває широкі можливості для автоматизації процесів та контролю за ними. Без необхідності втручання людини, пристрої можуть взаємодіяти один з одним, що пришвидшує та удосконалює обмін інформацією.

– Перевага в області інформації в IoT полягає у тому, що доступ до більшої кількості даних допомагає у прийнятті кращих рішень. Незалежно від того, чи маєте ви потребу у знаннях щодо продуктів у магазині, чи ж потрібно оцінювати запаси в компанії, наявність інформації надає вам перевагу у вирішенні проблем і оптимізації процесів.

– Перевага моніторингу в IoT полягає в здатності точно вимірювати та відстежувати різні параметри. Наприклад, моніторинг може допомогти визначити кількість залишків товарів або якість повітря у приміщенні. Це надає користувачеві додаткову інформацію, яка раніше була важко доступною.

Наприклад, якщо ви знаєте, що у вас закінчується молоко або чорнила для принтера, ви можете запланувати свої покупки заздалегідь, що дозволяє економити час та зусилля. Крім того, моніторинг термінів придатності продуктів може сприяти підвищенню безпеки.

– Перевага економії часу в IoT полягає в можливості оптимізувати рутинні процеси та забезпечувати швидший доступ до інформації. У сучасному світі, де час – цінний ресурс, IoT дозволяє нам ефективніше використовувати цей ресурс, звільняючи час для важливіших справ і розваг.

– Економія грошей є ключовою перевагою використання IoT. Ця технологія дозволяє оптимізувати використання енергії та ресурсів, запобігаючи витратам на непотрібне витрачання. Завдяки моніторингу та попередженню можливих проблем або поломок, IoT дозволяє ефективно управляти та зберігати енергію та ресурси, що веде до значних економічних вигод. Крім того, заощадження коштів на витрати на обладнання для з'єднання та моніторингу також сприяє широкому прийняттю IoT, що в свою чергу сприяє підвищенню ефективності та зменшенню витрат у повсякденній діяльності людей.

– Автоматизація завдань за допомогою IoT є важливою перевагою цієї технології. Вона дозволяє контролювати та автоматизувати рутинні процеси без прямого втручання людини. Зв'язок між пристроями, відомий як M2M, сприяє збереженню прозорості в процесах та рівномірному розподілу завдань. Це також сприяє підтримці високої якості обслуговування (QoS). Завдяки IoT ми можемо автоматично реагувати на надзвичайні ситуації та вживати необхідні заходи для їх вирішення.

– Взаємодія між пристроями сприяє підвищенню ефективності роботи. Це дозволяє швидко отримувати точні результати завдяки автоматизації процесів. Такий підхід дозволяє зекономити час, який можна витратити на виконання інших, більш творчих завдань, замість повторення однотипних робіт щодня.

– Завдяки IoT покращується якість життя через підвищення комфорту, зручності та ефективного управління. Ця технологія дозволяє створити

сприятливіші умови для життя, забезпечуючи доступ до різноманітних сервісів та оптимізуючи використання ресурсів.

До недоліків Інтернету речей можна віднести:

– У зв'язку з підключенням пристроїв різних виробників до однієї мережі виникає проблема сумісності, яка може ускладнити їх з'єднання та моніторинг. Хоча узгодження загального стандарту може сприяти зниженню цього недоліку, технічні питання все ще залишатимуться актуальними. Навіть за наявності пристроїв з підтримкою Bluetooth можуть виникати проблеми сумісності. Це може призвести до обмеження вибору споживачів та сприяти монополізації ринку деякими виробниками.

– IoT мережа складна і різноманітна, що може створювати виклики в управлінні та підтримці. Навіть найменші помилки в програмному або апаратному забезпеченні можуть мати серйозні наслідки. Навіть випадкове відключення живлення може призвести до порушень у роботі системи.

Наприклад, уявіть ситуацію, коли ваша розумна система повідомляє вас і вашу дружину про те, що молоко закінчилося. Ви обидва зупиняєтеся в магазині, щоб купити молоко на шляху додому, не знаючи, що робить інший. Це може призвести до непотрібних витрат і перевитрати ресурси.

Також можливі сценарії, коли помилка в програмному забезпеченні призводить до надмірного замовлення товарів або послуг. Наприклад, якщо система автоматично замовляє нові картриджі для принтера кожну годину протягом декількох днів, навіть коли вам потрібна лише одна заміна, це може викликати витрати, які можна було уникнути.

– За допомогою автоматизації рутина стає менш залежною від людської присутності, що може вплинути на зайнятість некваліфікованих працівників. Внаслідок цього можуть виникнути проблеми з безробіттям в суспільстві. Ця ситуація може бути вирішена шляхом введення високоякісної освіти та перепідготовки працівників, щоб вони могли адаптуватися до змін на ринку праці.

Автоматизація може знизити потребу у людських ресурсах, зокрема серед робітників та менш освічених працівників. Це може спричинити проблеми з

безробіттям, але одночасно відкриває можливості для створення нових видів робіт, пов'язаних з розвитком та підтримкою автоматизованих систем. Важливою є не тільки адаптація людей до змін, але й створення нових можливостей для їхнього професійного росту.

– З технологічними інноваціями наше життя стає все більш залежним від цифрових рішень, що може вплинути на нашу незалежність та приватність. Молоде покоління вже звикло до того, що багато аспектів їхнього життя контролюються за допомогою технології, такої як доступ до Інтернету через Wi-Fi. Важливо зрозуміти, який рівень автоматизації та контролю над нашими життями ми готові прийняти, зберігаючи баланс між зручністю та приватністю.

– Зі збільшенням обсягу даних, які обробляються в рамках Інтернету речей, зростає й ризик порушення конфіденційності. Наприклад, в разі виникнення помилок у роботі системи можливе навіть відкриття особистої інформації перед сторонніми. Це може включати такі деталі, як ваше фінансове становище чи покупки, здійснені вами в магазині, що може порушити вашу приватність та безпеку.

– З поширенням Інтернету речей зростає загроза безпеці. Пристрої побутового та промислового призначення, а також інфраструктура державного сектору стають більш вразливими перед потенційними кібератаками. Це може призвести до несанкціонованого доступу до особистих та конфіденційних даних, що становить серйозну загрозу як для приватності, так і для безпеки користувачів.

Після ретельного аналізу переваг та недоліків моделі IoT можна прийти до висновку, що хоча переваги переважають над недоліками, проблеми безпеки та конфіденційності залишаються серйозними перешкодами для повноцінного впровадження цієї технології. Тим не менш, ці проблеми не є невирішеними, і вони продовжують привертати увагу виробників та дослідників. Шлях до безпечного та приватного використання IoT вимагає спільних зусиль у сфері розробки стандартів безпеки, застосування шифрування даних та захисту від кіберзагроз.

2 ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПРОТОКОЛІВ ТА ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ У МЕРЕЖАХ IOT

2.1 Передача даних в IoT мережах за допомогою новітніх технологій та протоколів на великі відстані

2.1.1 LoRaWAN

У перспективі, з поширенням Інтернету речей, значна кількість пристроїв буде працювати на батарейках, тому довга автономність стане ключовою характеристикою. Для цього були розроблені нові мережі, спеціально адаптовані під потреби IoT, такі як LPWAN (Long Power Wide Area Network). Ці мережі використовують різні технології, такі як NB-IoT, Weightless, LoRa, SIGFOX та інші, для підключення широкого спектру пристроїв, які збирають дані для хмарних серверів[9].

З'явлення технології LoRaWAN викликало значний інтерес на ринку бездротового зв'язку, що призвело до необхідності уніфікації стандартів для глобальних мереж з низьким енергоспоживанням – LPWAN. Акронім LoRa поєднує в собі метод модуляції LoRa, який використовується у бездротових мережах LPWAN і був розроблений компанією Semtech, та відкритий протокол LoRaWAN.

Технологія LoRa (Long Range) та відповідний метод модуляції, розроблений компанією Semtech, базується на розширенні спектру (spread spectrum modulation) та використовує варіацію лінійної частотної модуляції (chirp spread spectrum, CSS). За цим методом дані кодуються широкосмуговими імпульсами, частота яких змінюється протягом певного часового інтервалу. Порівняно з технологією прямого розширення спектру, LoRa робить приймач стійким до змін частоти та спрощує вимоги до тактового генератора, дозволяючи використовувати більш економічні кварцові резонатори. Крім того, LoRa використовує пряму корекцію помилок (forward error correction, FEC) та працює в субгігагерцовому діапазоні частот.

Технологія LoRa відкриває можливість демодулювати сигнали на рівні, що низьше на 20 дБ порівняно з рівнем шумів, що є великим покращенням у порівнянні з більшістю систем, що використовують частотну маніпуляцію (FSK), які працюють на рівні 8-10 дБ вище рівня шумів. Модуляція LoRa може бути використана на фізичному рівні в різних типах мереж – від mesh-мереж і мереж зірки до точка-точка та інших.

Завдяки високій чутливості (148dbm), LoRa ідеально підходить для пристроїв, які вимагають низького споживання електроенергії та мають великі відстані між собою.

LoRaWAN – це відкритий протокол канального рівня для мереж з високою ємністю та великим радіусом дії, який стандартизувала LoRa Alliance для мереж LPWAN [10].

Поряд з протоколом LoRaWAN можуть працювати різні типи пристроїв, як показано на рис. 2.1. У LoRaWAN ці пристрої класифікуються наступним чином:

– Двонаправлені кінцеві пристрої "класу А" (Bi-directional End Devices, Class A). Ці пристрої відправляють дані до сервера та очікують відповіді в певні часові інтервали. Вони мають можливість відкрити два вікна для прийому даних в певний час після передачі.

– Двонаправлені кінцеві пристрої "класу Б" (Bi-directional End Devices, Class B). У цих пристроїв, окрім відправлення даних, є можливість отримувати дані в певні часові інтервали, які синхронізуються з сервером.

– Двонаправлені кінцеві пристрої "класу С" з максимальним приймальним вікном (Bi-directional End Devices, Class C). Ці пристрої мають безперервне вікно для прийому даних, яке закривається лише під час передачі. Вони ідеально підходять для завдань, які вимагають постійного прийому великого обсягу даних.

Рисунок 2.1 – Типи пристроїв LoRaWAN

Архітектура LoRaWAN включає наступні ключові компоненти: кінцеві вузли, шлюзи, мережевий сервер та сервер додатків. Ці компоненти працюють разом для забезпечення зв'язку та обробки даних у мережі LoRaWAN, як показано на рис. 2.2.

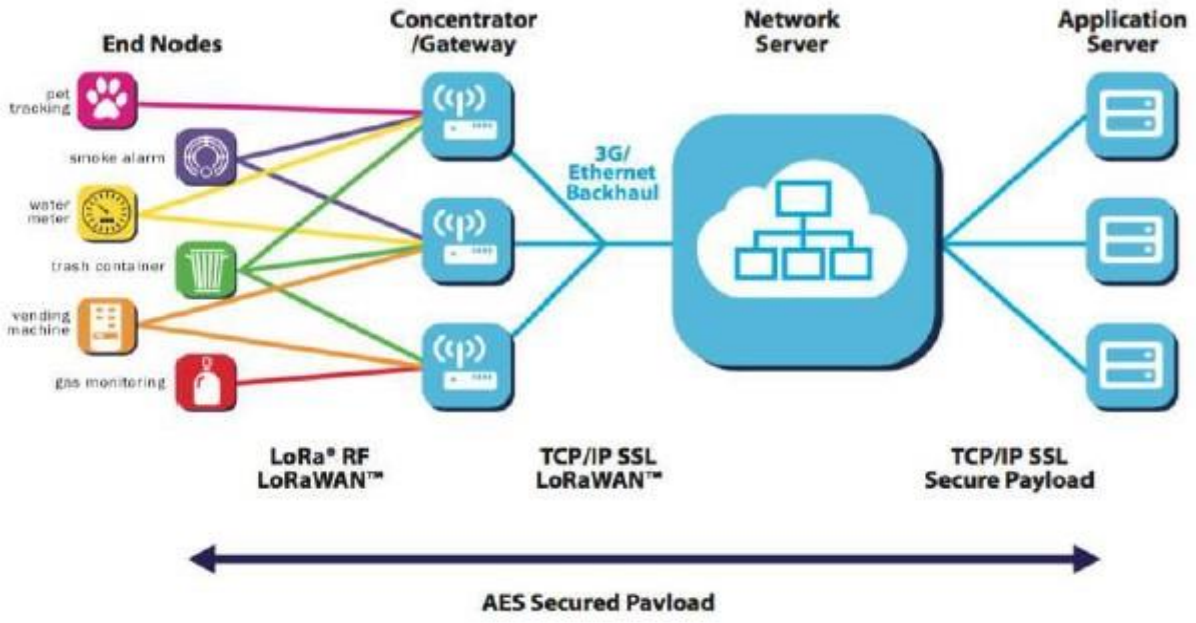

Рисунок 2.2 – Архітектура мережі LoRaWAN

Кінцеві вузли (End Nodes) представляють собою пристрої, які виконують вимірювання, контроль та управління в системі. Кожен вузол зазвичай містить набір датчиків для вимірювання та керуючі елементи. Через те, що більшість кінцевих вузлів живляться від батарейок, для економії енергії вони відправляють дані лише протягом коротких періодів часу, після чого відкривають два тимчасові вікна для прийому даних.

Шлюз LoRa (Gateway/Concentrator) – це пристрій, що отримує дані від кінцевих вузлів через радіоканал та передає їх у транзитну мережу. Транзитна мережа може включати в себе WiFi, Ethernet, мобільні мережі та інші телекомунікаційні канали. Кінцеві пристрої та шлюзи утворюють типову мережеву топологію "зірка". Часто шлюзи складаються з багатоканальних пристроїв прийому та передачі, що дозволяє їм обробляти сигнали, одночасно отримані з різних каналів. Такий підхід забезпечує повне покриття мережі та надійну двонаправлену передачу даних між мережевим сервером та кінцевими вузлами.

Мережевий сервер (Network Server) виступає як центральний вузол управління мережею. Він відповідає за регулювання швидкості передачі, аналізує, обробляє та зберігає дані, отримані від шлюзів.

Сервер програм (Application Server) – це пристрій, спрямований на збір інформації від кінцевих вузлів та здійснення віддаленого контролю їх роботи.

Один LoRa-шлюз може обслуговувати до п'яти тисяч кінцевих пристроїв завдяки кільком особливостям:

– Особливостям топології мережі, яка дозволяє ефективно координувати та обробляти дані від багатьох пристроїв.

– Адаптивній швидкості передачі даних та адаптивній вихідній потужності пристроїв, які регулюються мережевим вузлом для оптимального використання ресурсів.

– Тимчасовому поділу доступу до середовища, що дозволяє кінцевим пристроям взаємодіяти з шлюзом у визначених інтервалах часу.

– Частотному поділу каналів, що дозволяє розділити доступ до радіочастотного спектру між різними пристроями.

– Особливостям LoRa модуляції, що дозволяє одночасно демодулювати сигнали на різних швидкостях передачі в одному частотному каналі.

Поява енергоефективних бездротових технологій, таких як LoRaWAN, зробила можливим будівництво глобальних мереж передачі даних, що є водночас простими в реалізації. Їх важливі переваги включають розширений радіус дії, довгий час автономної роботи та надійне виявлення корисного сигналу навіть у присутності перешкод.

2.1.2 SigFox

Технологія SigFox відкриває нові можливості для розбудови мереж та стратегій зв'язку в Інтернеті речей. Розроблена групою з Labège, Франція, компанія SigFox є мережевим оператором, спеціалізованим на впровадженні IoT у бізнес та промисловість. Архітектура мережі SigFox схожа на традиційні стільникові мережі, такі як GSM та GPRS, проте вона відрізняється меншою вартістю та більшою енергоефективністю.

Мережа SigFox покриває зону приблизно 30-50 км у міських та сільських районах. У містах, де є багато електромагнітних шумів, діапазон роботи скорочується до 3-10 км.

На рис. 2.3 зображена архітектура мережі технології SigFox [13]. Загальна топологія мережі розроблена для створення масштабованої, високопродуктивної системи з дуже низьким енергоспоживанням.

SigFox використовує надвузьку смугу частот UNB (Ultra Narrow Band) для підключення пристроїв до глобальної мережі. Використання UNB є ключовим фактором для забезпечення дуже низької потужності передавача, яка використовується для створення надійного з'єднання та передачі даних.

Пристрої надсилають свої дані до базової станції SigFox. Це відбувається за допомогою протоколу point-to-point (P2P). Після цього базова станція підключається до Інтернет бази даних, де дані декодуються і надсилаються.

Нарешті, хмарний сервер SigFox розсилає ці дані до клієнтських серверів та платформ через API.

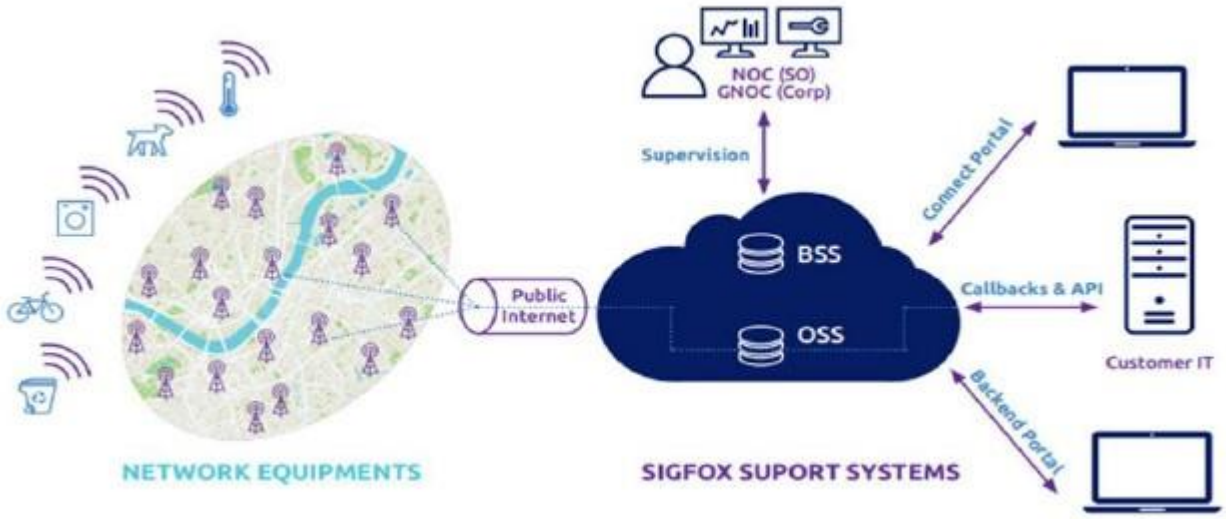

Рисунок 2.3 – Архітектура мережі SigFox

Технологія SigFox розроблена для ефективного використання в ситуаціях, де важливо забезпечити доступність зв'язку за низьку ціну та великій зоні покриття. Існує багато сфер, де можна використовувати цю бездротову технологію:

– Системи дому та розподілених споживчих товарів;

– Системи енергетичних мереж та зв'язку;

– Застосування в медичній сфері для моніторингу здоров'я;

– Транспортні системи та моніторинг руху транспорту;

– Віддалений моніторинг і контроль різних процесів та систем;

– Системи безпеки та захисту об'єктів.

Стандарт SigFox має ряд переваг порівняно з іншими базовими технологіями LPWAN мереж. Деякі з них:

Переваги:

– велика зона покриття;

– висока проникність сигналу через перешкоди;

– довгий термін служби від однієї батареї, можливо до 20 років роботи сенсора на двох батареях AA;

– низьке енергоспоживання;

– низька вартість.

Незважаючи на ці переваги, технологія SigFox також має деякі обмеження:

– низька швидкість передачі даних;

– залежність від існуючої стільникової інфраструктури;

– обмежена стійкість до перешкод.

В більшості країн Європи та США ця технологія дійсно є популярною через свою енергоефективність та доступність.

2.1.3 NB-IoT

NB-IoT – стандарт стільникового зв'язку, призначений для пристроїв телеметрії з низьким об'ємом передачі даних. Розроблений організацією 3GPP як еволюція мобільних стільникових мереж. Перша версія цього стандарту була представлена в 2016 році.

NB-IoT, або також відомий як LTE-CAT.M2, має численні переваги, такі як:

– низьке енергоспоживання, що забезпечує тривалий термін роботи батареї до 10 років;

– широка зона покриття;

– можливість швидкої модернізації мережі;

– висока надійність.

NB-IoT – це розвиток стільникового зв'язку, який дозволяє операторам працювати з різними сферами Інтернету речей, такими як системи інтелектуального відстеження та обліку.

Технологія NB-IoT розглядається як крок у напрямку розвитку стільникового зв'язку для потреб Інтернету речей. Вона представляє собою бездротовий варіант глобальних мереж з низьким споживанням енергії і розроблена для взаємодії між пристроями M2M.

NB-IoT може працювати в практично всіх тих же діапазонах частот, що і 2G/3G/4G в "низьких" діапазонах, таких як 800МГц, 900МГц і 1800МГц. Використання більш високих частот може призвести до більшого затухання сигналу, тому вони не так часто використовуються для NB-IoT.

Існують три способи виділення частотного ресурсу для NB-IoT:

1.Stand-Alone (автономний):

– В цьому випадку виділяється частотний канал шириною в 200 кГц. Цей метод є найбільш ефективним для роботи NB-IoT, але вимагає значних ресурсів. Для його реалізації може знадобитися від 300 до 600 кГц цінного спектру, включаючи захисні інтервали. У такому випадку взаємні перешкоди з іншими технологіями мінімізуються рис. 2.4.

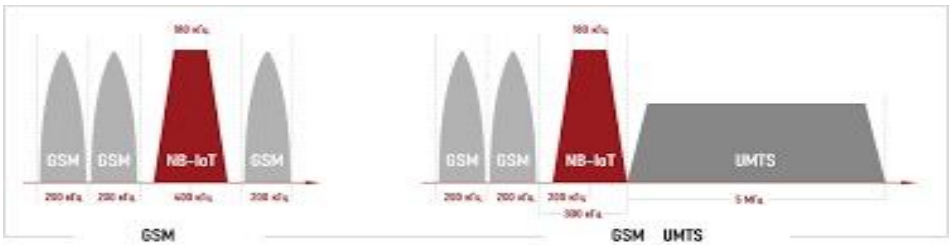

Рисунок 2.4 – Варіанти розміщення NB-IoT в режимі Stand - Alone

В полосі Band (в середині) використовуються ресурси для NB-IoT всередині наявної LTE несучої. Проте, NB-IoT несуча має значно вищу потужність на 6 дБ порівняно з LTE ресурсами. Цей підхід сприяє ефективній утилізації частотних ресурсів, але може виникнути проблема взаємного впливу з LTE мережею рис. 2.5.

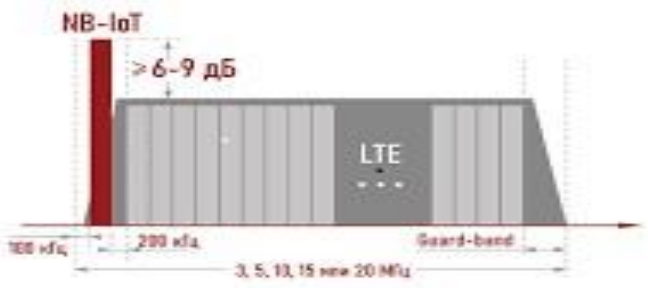

Рисунок 2.5 – Розміщення Nb IoT в режимі in Band

У захистній полосі частот NB-IoT працює в так званому захистному інтервалі. Наприклад, у смузі LTE 10 МГц, 500 кГц вільного спектру використовується як захистний інтервал. Аналогічно режиму In Band, для забезпечення більшої дальності передачі, NB-IoT несуча має підвищену потужність на 6-9 дБ порівняно з ресурсними блоками LTE рис. 2.6. Цей підхід дозволяє ефективно використовувати частотний ресурс та зменшує взаємний вплив на LTE мережу. Однак, у цьому випадку може відбуватися погіршення показників позамагістральних випромінювань для LTE.

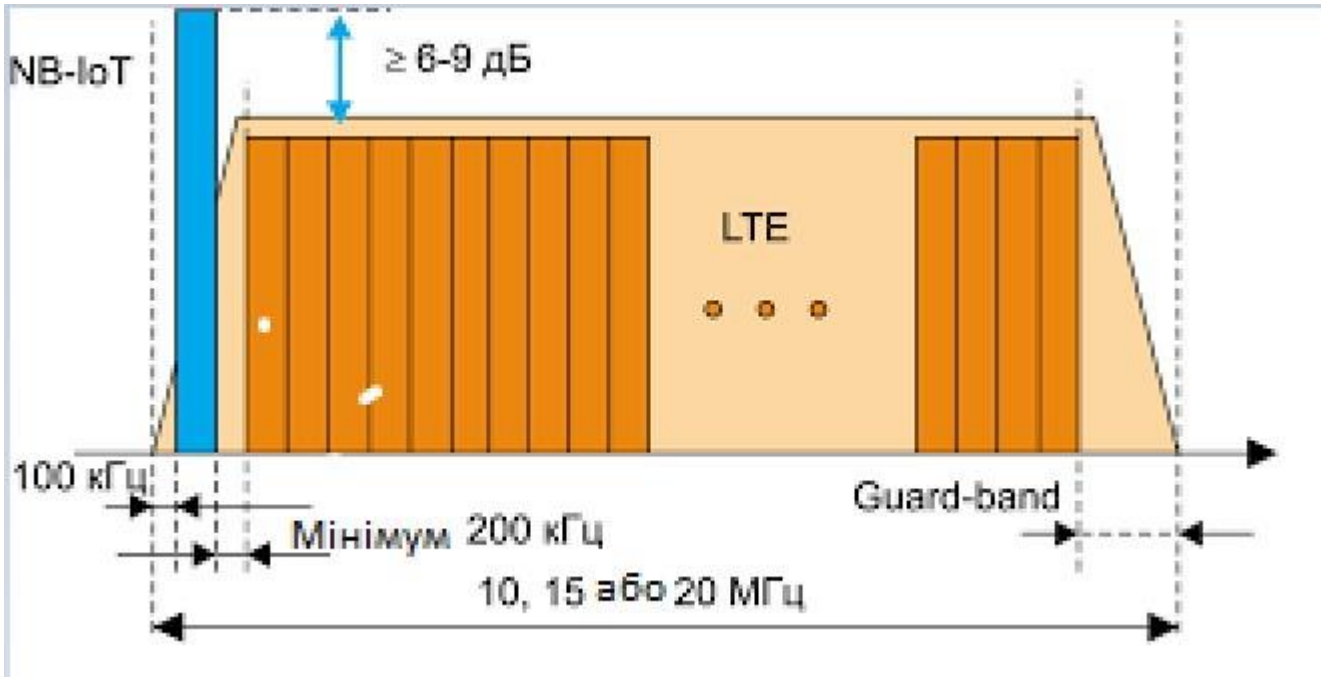

Рисунок 2.6 – Розміщення NB-IoT в режимі Guard Band

Weightless-P – це LPWAN технологія, спеціально розроблена для Internet of Things (IoT). Вона застосовується там, де необхідна довготривала робота від одного заряду батареї, двонаправлений зв'язок і висока щільність кінцевих пристроїв. Ця технологія відрізняється широкою зоною покриття, масштабованістю мережі, тривалим терміном роботи батареї та надійністю. Weightless-P підтримує невеликий діапазон груп модуляцій і забезпечує можливість двонаправленого зв'язку для забезпечення високої якості зв'язку. Одна

базова станція може обслуговувати більшу кількість кінцевих пристроїв, порівняно з іншими технологіями LPWAN.

У відміну від інших технологій, базова станція в Weightless-P має повний контроль над своєю мережею і кінцевими пристроями у будь-який момент. Це робить її більш розвиненою технологією порівняно з іншими LPWAN рішеннями.

Weightless-P забезпечує гарантовану доставку повідомлень, що дозволяє уникнути необхідності відправляти повідомлення кілька разів, як у LoRa та SigFox. Це призводить до економії заряду пристроїв і підвищує ефективність використання енергії.

Крім того, у Weightless-P використовується метод підтримки адаптивної швидкості передавання інформації, що призводить до збільшення тривалості роботи батареї та підвищує продуктивність мережі.

Крім того, Weightless-P підтримує адаптивне налаштування швидкості передачі даних, що забезпечує оптимальну продуктивність мережі та збільшує тривалість роботи батареї кінцевих пристроїв. Це досягається шляхом регулювання фактичної швидкості передачі даних в залежності від відстані кожного вузла до базової станції. Вузли, що знаходяться ближче до базової станції, працюють з вищою швидкістю передачі даних, що дозволяє скоротити час передачі та знизити вихідну потужність. У той час, як вузли, які знаходяться найдалі від базової станції, використовують нижчу швидкість передачі даних та вищу вихідну потужність.

Цей більш оптимізований та компактний протокол сприяє зменшенню вартості системи та спрощує її експлуатацію у порівнянні з NB-IoT та іншими стільниковими M2M системами. Ця технологія застосовується у різних системах спостереження, моніторингу стану здоров’я людини, розумних пристроях та інших сферах.

Порівняльна характеристика технологій передачі даних на довгі відстані в мережі IoT.

Таблиця 2.1 – Порівняння основних технічних характеристик мереж з високою дальністю дії LPWAN

Характеристика	LoRaWAN	SigFox	NB-IoT	Weightless-P
Частотний діапазон	Sub-1 GHz	868 MHz (EU), 915 MHz (US)	Licensed bands	Sub-1 GHz
Швидкість передачі даних	Декілька кбіт/с (залежно від налаштувань)	До 100 біт/с	До 250 кбіт/с	До 100 кбіт/с
Дальність зв'язку	Декілька кілометрів до декількох десятків кілометрів	До 30-50 км (в лінії видимості)	Декілька кілометрів	Декілька кілометрів
Енергоефективність	Висока	Висока	Висока	Висока
Масштабованість мережі	Велика кількість підключених пристроїв	Велика кількість підключених пристроїв	Велика кількість підключених пристроїв	Велика кількість підключених пристроїв

2.2 Можливості бездротового зв'язку в інтернеті речей на малих відстанях

2.2.1 Z-Wave

Z-Wave – це бездротова технологія з низьким енергоспоживанням для передачі даних в інтернеті речей (IoT). Вона працює на частоті до 1 ГГц та спеціалізується на передачі простих команд для керування пристроями з мінімальними затримками. Вибір цієї частоти має на меті уникнути перешкод від інших технологій, які вже використовуються в повсякденному житті, таких як Wi-Fi, особливо на частоті 2,4 ГГц.

Технологія Z-Wave – це рішення для повноцінного контролю над безпекою та енергоефективністю вашого будинку, з мінімальними турботами. Завдяки Z-Wave ви можете створити власну систему автоматизації, що охоплює освітлення, опалення, кондиціонування повітря, кухонні прилади та навіть системи безпеки.

Ця технологія проста у використанні, енергоефективна та допомагає зекономити час.

Ця система працює через дистанційне керування і використовує радіосигнали з низькою потужністю. Завдяки своїй сіткоподібній структурі, вона охоплює всі зони будинку, проникаючи через стіни, поверхні та меблі. Це забезпечує практично 100% надійне з'єднання.

2.2.2 NFC

Технологія NFC (Near Field Communication), розроблена компаніями, такими як Sony та NXP Semiconductors, поєднує безконтактні технології зв'язку та радіочастотну ідентифікацію. Вона призначена для обміну різними видами інформації, такими як фотографії, аудіофайли, контактні дані, або ключі авторизації, між двома пристроями з підтримкою NFC, які знаходяться недалеко один від одного. Ці пристрої можуть включати смартфони, планшети, або навіть RFID-читачі. NFC може застосовуватися для безконтактного доступу до даних або послуг, таких як електронні замки або безготівкова оплата.

На відміну від інших технологій безконтактного зв'язку, які передають дані тільки від активного пристрою до пасивного, NFC дозволяє обмінюватися інформацією між двома активними пристроями. Вона також використовується для взаємодії з пристроями радіочастотної ідентифікації RFID, де здійснюється перевірка цифрового протоколу для забезпечення сумісності між різними картами RFID та мобільними телефонами. Під час цього процесу проводяться вимірювання всіх важливих параметрів радіочастотного сигналу, включаючи тимчасові характеристики, чутливість та амплітуду приймача в активному режимі, та частоту несної амплітуди сигналу.

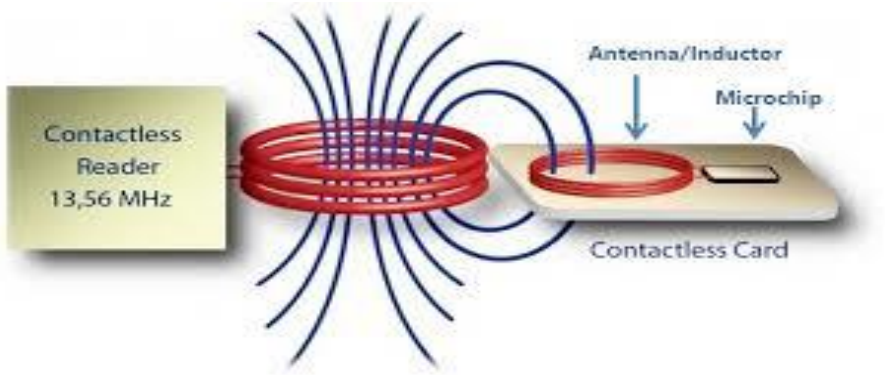

Рисунок 2.7 – Принцип роботи NFC

Під час передачі інформації від активного до пасивного пристрою використовується амплітудна маніпуляція ASK. Обидва пристрої вважаються рівноправними, і кожен має власне джерело живлення. Після завершення передачі сигнал несної відключається. Через індуктивний зв'язок між пристроями пасивний пристрій впливає на активний, змінюючи імпеданс. Це викликає зміну амплітуди або фази напруги на антені активного пристрою, що сприяє з'єднанню і передачі даних. Якщо відстань між пристроями перевищує 20 см, електромагнітний зв'язок розривається, і передача даних автоматично припиняється.

На практиці, NFC можна розглядати як розширення вже добре відомої технології радіочастотної ідентифікації RFID. RFID широко використовується в безконтактних картах та мітках. Однак NFC відрізняється тим, що вона не лише може зчитувати інформацію з пасивних електронних міток, але й забезпечує можливість двостороннього бездротового зв'язку між пристроями.

2.2.3 RFID

RFID (Radio Frequency IDentification) – це метод автоматичної ідентифікації об’єктів, що використовує радіосигнали для зчитування або запису даних, що зберігаються в транспондерах, відомих як RFID-мітки. Кожна RFID-система складається з зчитувального пристрою (зчитувача або рідера) та транспондера (RFID-мітки або тега).

Більшість RFID-міток складаються з двох основних частин. Перша частина - інтегральна схема, що відповідає за обробку та зберігання інформації,

демодуляцію та модуляцію радіочастотного сигналу, а також виконання інших функцій. Друга частина - антена, призначена для прийому та передачі сигналів. Для коректної роботи цих міток необхідне відповідне програмне забезпечення - програми, які відповідають за аналіз та збір інформації, що надходить із RFID-міток.

Мітки RFID бувають двох видів: активні та пасивні. Активні мітки мають власне джерело живлення, тому вони можуть самостійно передавати сигнали і бути зчитані з великої відстані. З іншого боку, пасивні мітки не мають власного джерела енергії і активуються лише тоді, коли отримують сигнал від пристрою зчитування, після чого передають збережену в них інформацію.

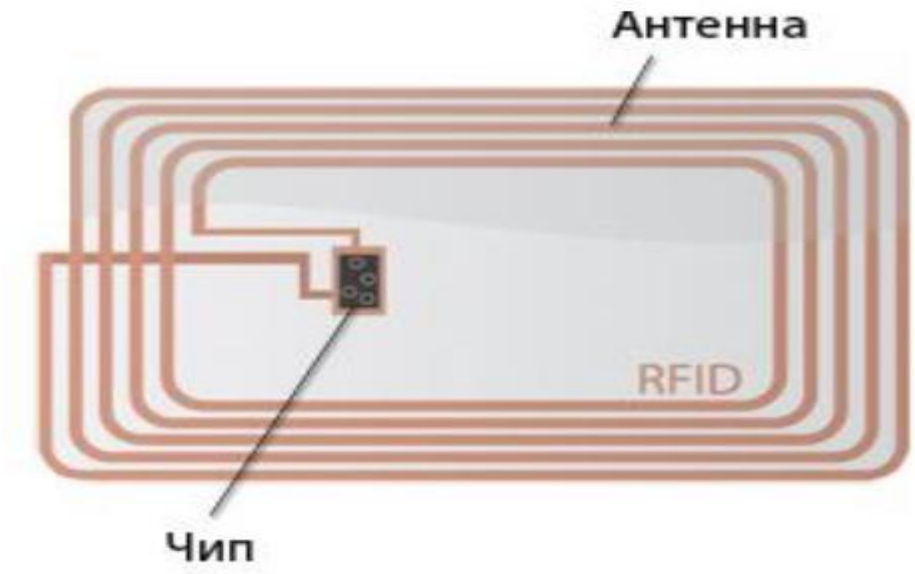

Рисунок 2.8 – Будова RFID-мітки

RFID-мітки застосовуються у різних галузях, включаючи управління товарними запасами та відстеження часу на спортивних змаганнях. Вони доповнюють систему штрих-кодів, надаючи можливість дистанційного зчитування. Мітки використовуються для маркування великої рогатої худоби з метою запису інформації про ветеринарний огляд. У транспортній галузі вони допомагають ідентифікувати автомобілі, навіть якщо вони рухаються на великій швидкості, а також використовуються авіалініями для ефективного відстеження

багажу. Крім того, технологія RFID вбудовується у біометричні паспорти та кредитні картки для безпечного доступу до захищених областей.

Деякі RFID-мітки можуть бути зчитані на відстані декількох метрів від пристрою зчитування навіть без прямої видимості. Більшість міток містять текстовий запис та штрих-код як додаткові дані для прямого зчитування у випадках, коли радіочастотна електроніка недоступна.

2.2.4 Bluetooth Low Energy

Bluetooth Low Energy (BLE) – це частина Bluetooth специфікації, яка була вперше представлена у версії Bluetooth 4.0 і продовжує свій розвиток з Bluetooth 5.0. Пристрої, які використовують BLE, відзначаються низьким енергоспоживанням порівняно з попередніми версіями Bluetooth. Це дозволяє багатьом пристроям працювати протягом довшого часу без заряджання на одній невеликій батарейці типу "таблетка". За допомогою BLE можна використовувати компактні датчики, які постійно працюють і взаємодіють з іншими пристроями, що розширює можливості IoT та мобільних додатків.

BLE має три основних рівні:

1. Додатковий рівень, він відповідає за реалізацію функціональності, корисної для кінцевого користувача. На цьому рівні розробляються програми та додатки, що використовують можливості Bluetooth Low Energy.

2. Основний пристрій, або хост. Цей рівень надає верхній шар стеку протоколів Bluetooth. Він відповідає за керування взаємодією між додатками та контролером Bluetooth.

3. Контролер. Контролер відповідає за нижні рівні стеку протоколів Bluetooth. Він забезпечує безперервну роботу пристроїв на фізичному рівні та здійснює обробку радіочастотних сигналів.

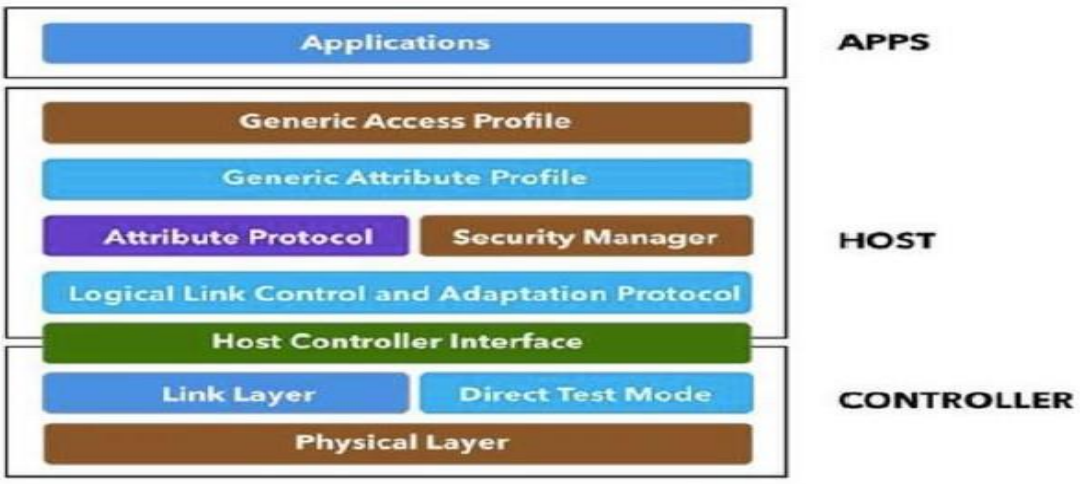

Рисунок 2.9 – Архітектура BLE

У стеку протоколів Bluetooth Low Energy (BLE) рівень додатків є найвищим. Рівень хосту включає такі підрівні:

– GAP (Generic Access Profile) – відповідає за налаштування з'єднання та забезпечення загального доступу до пристрою.

– GATT (Generic Attribute Profile) – визначає правила взаємодії та обміну даними між пристроями за допомогою атрибутів.

– ATT (Attribute Protocol) – забезпечує передачу даних між пристроями через атрибути.

– SM (Security Manager) – відповідає за управління безпекою та аутентифікацію пристроїв.

– L2CAP (Logical Link Control and Adaptation Protocol) – забезпечує логічний контроль з'єднання та адаптацію для різних типів даних.

– HCI (Host Controller Interface) – інтерфейс хост-контролера, що дозволяє взаємодіяти з контролером Bluetooth на стороні хосту.

На рівні контролера використовуються такі рівні:

– HCI (Host Controller Interface) – це інтерфейс між хостом і контролером Bluetooth, який дозволяє хосту керувати контролером.

– LL (Link Layer) – канальний рівень, що забезпечує управління з'єднаннями та передачу даних на фізичному рівні.

– PHY (Physical Layer) – фізичний рівень, який відповідає за обробку радіочастотних сигналів та їх перетворення в цифрові дані і навпаки.

Bluetooth Low Energy (BLE) призначений для пристроїв з обмеженими ресурсами, такими як невеликі мобільні пристрої, де важлива компактність та енергоефективність. У порівнянні з класичними Bluetooth рішеннями, BLE споживає на 10-20 разів менше енергії, що дозволяє працювати пристроям протягом тривалого часу без необхідності заряджання. Крім того, він здатний передавати дані швидше - на 50 і більше разів, та на більші відстані, до 100 метрів, що робить його ідеальним вибором для реалізації різноманітних IoT та мобільних додатків.

Поміж переліченими вище перевагами, BLE відзначається також високою безпечністю, надійністю та низькою затримкою при підключенні. Ще однією важливою особливістю цього стандарту є його адаптивність у налаштуванні частоти. BLE автоматично переналаштовує свою робочу частоту для уникнення помилок передачі сигналу. Ця здатність дозволяє швидко адаптуватися до змін у середовищі, вибираючи оптимальну частоту для мінімізації перешкод, уникнення переповнення та зниження інтерференції.

Bluetooth 5.0 був спеціально розроблений з урахуванням потреб Інтернету речей (IoT), що свідчить про його амбіції у захопленні ринку пристроїв. У порівнянні з попередньою версією 4.0, Bluetooth 5.0 значно підвищив швидкість передачі даних, наближаючись до швидкостей, що характерні для технологій HSPA і LTE, при цьому енергоспоживання залишалося на попередньому рівні. Це особливо важливо для будівництва мереж IoT, де енергоефективність має велике значення. Наразі, хоча специфікація Bluetooth 5.0 ще не так поширена, як попередні версії, з часом це може змінитися. Bluetooth 5.0, як і попередні версії, забезпечує зворотну сумісність, що робить його привабливим вибором для розвитку мобільних технологій у майбутньому.

2.2.5 Wi-Fi HaLow

Wi-Fi HaLow, опублікований у 2017 році, є доповненням до стандарту бездротової мережі IEEE 802.11. Цей протокол використовує частоту 900 МГц, що не потребує ліцензування, для забезпечення розширеного діапазону Wi-Fi мереж порівняно зі звичайними мережами Wi-Fi, які працюють у діапазонах 2,4 ГГц і 5 ГГц. Однією з основних переваг Wi-Fi HaLow є його низьке енергоспоживання, що дозволяє створювати великі групи станцій або датчиків для підтримки концепції Інтернету речей (IoT). Цей протокол конкурує з Bluetooth за рахунок свого низького енергоспоживання, проте має додаткову перевагу у вищих швидкостях передачі даних і більшому діапазоні покриття.

Wi-Fi HaLow відкриває нові можливості для енергоефективного використання в різних сферах, включаючи розумний будинок, автомобільну індустрію, торгівлю, промисловість, сільське господарство і багато інших галузей. Цей протокол розширює Wi-Fi у діапазоні 900 МГц, що дозволяє підключати пристрої з низьким енергоспоживанням, такі як датчики і портативні комп'ютери. Крім того, Wi-Fi HaLow успадковує позитивні характеристики попередніх протоколів, такі як надійний захист інформації, широку сумісність обладнання та простоту встановлення.

Пристрої, що підтримують Wi-Fi HaLow, також зможуть працювати у діапазонах 2,4 та 5 ГГц, що відкриє шлях для їх інтеграції в існуючу екосистему, налічуючи більше 7 млрд пристроїв на сьогодні. Крім того, Wi-Fi HaLow буде підтримувати підключення по IP, що робить його сумісним з хмарами, що має велике значення для Інтернету речей. Додатково, цей протокол дозволить підключати до однієї точки доступу приблизно 1000 пристроїв, що робить його ідеальним рішенням для великих IoT мереж.

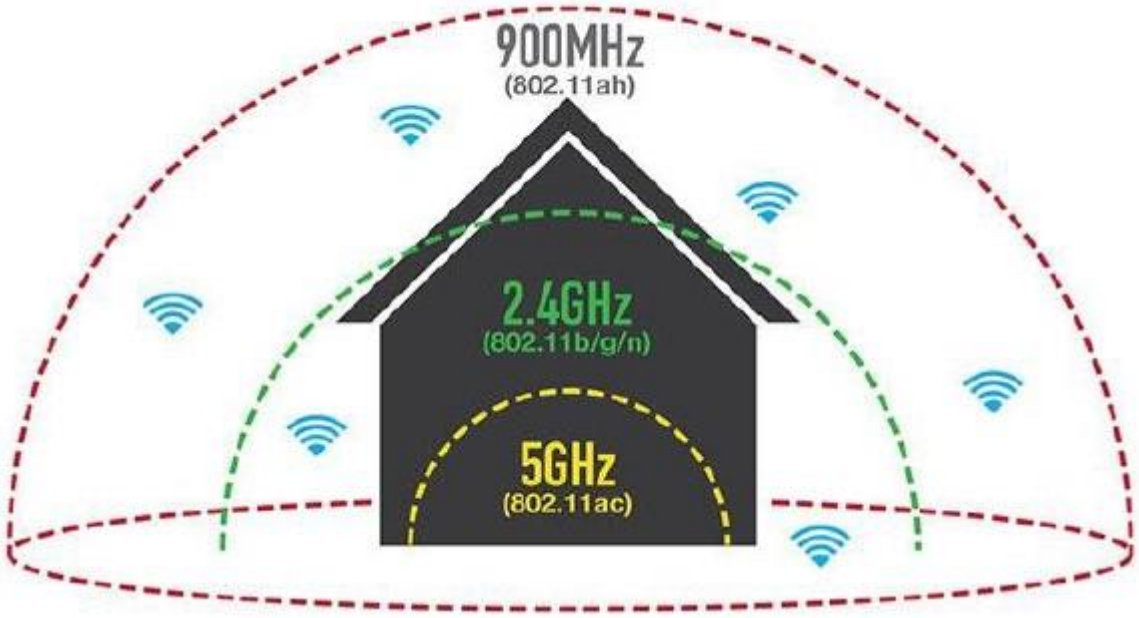

Рисунок 2.10 – Порівняльна хаоактерисика різних протоколів Wi-Fi за зоною покриття

Таблиця 2.2 – Відмінності у ключових технічних параметрах короткодіючих мереж

Характеристика	Sigfox	LoRa	NB-IoT
Частотний діапазон	868 МГц (Європа), 902 МГц (Північна Америка)	Залежно від регіону: 433 МГц, 868 МГц або 915 МГц	Різні діапазони, включаючи 700 МГц, 800 МГц, 900 МГц, 1800 МГц та 2100 МГц
Швидкість передачі даних	До 100 біт/с	До 27 Кбіт/с	До 250 Кбіт/с
Покриття	Широке покриття, охоплює великі території	Залежить від конфігурації, може мати дуже далеке покриття	Висока проникність, добре працює в затінених областях та всередині будівель

2.3 Різноманітні протоколи, призначені для обміну інформацією

2.3.1 Основні виклики, пов'язані з комунікацією в мережах IoT

Хоча окремі сенсорні вузли генерують обмежені обсяги інформації, основна ідея Інтернету речей полягає в обробці даних від багатьох таких вузлів. Це суттєво відрізняється від типових архітектур, таких як традиційні телефонні мережі або клієнт-серверні системи передачі даних.

Отже, ми стикаємося з новою моделлю архітектури: розподілена мережа, де інформація може створюватися і споживатися багатьма джерелами і одержувачами. Крім того, обсяг передаваного трафіку від сенсорного вузла може значно варіюватися. Традиційні протоколи передачі повідомлень не завжди адаптовані до таких умов.

2.3.2 Основна топологія, яка застосовується для передачі даних в мережі IoT

Подана у рис. 2.11 топологія відповідає концепції "видавець-підписник" (Publisher-Subscriber, або pub/sub), яка використовується для передачі повідомлень в Інтернеті речей. У цій схемі існує два ключових учасника: видавець, який є джерелом інформації, та передплатник, який отримує цю інформацію. Підписка - це операція, за допомогою якої передплатник отримує інформацію від конкретного видавця. Також в цій концепції важливо управляти збором інформації, встановлюючи параметри, такі як періодичність отримання даних та інші показники, залежно від конкретної реалізації.

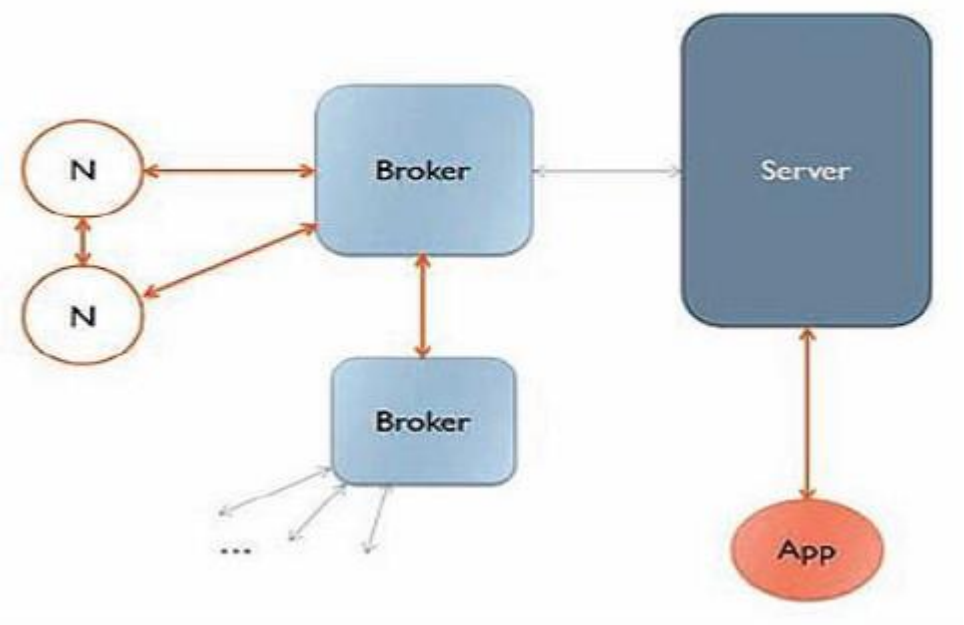

Рисунок 2.11 – Схема сполучень, що забезпечує обмін даними між вузлами в мережі IoT

У даному контексті розглядається ситуація, коли сенсорний вузол (Node) збирає дані від різних датчиків (наприклад, вологості повітря) та передає їх згідно з параметрами передплати або на запит, або автоматично через певний інтервал часу. Часто датчики є простими та надсилають дані про контрольовані параметри безперервно. Це призводить до потреби об'єднувати датчики в вузли, які оснащені мікроконтролерами для зчитування даних та їх відправки на сервер за визначеними алгоритмами. Для взаємодії клієнтів з системою також потрібна клієнтська програма (Application), що встановлюється на персональних пристроях для відображення даних з датчиків або вже оброблених на сервері, а також для управління системою.

У такій топології також може бути використаний брокер (Broker), який приймає дані від видавців та передає їх відповідним передплатникам. У складних системах брокер може також виконувати аналітичні операції та обробку даних, що надійшли на сервер. Брокер встановлює пріоритети для з'єднань та формує черги для передачі повідомлень, що дозволяє організовувати пересилання, зберігання та фільтрацію даних.

2.3.3 DDS

DDS (Data Distribution Service) – це протокол на рівні застосунків для машинного зв'язку в системах реального часу. Він ґрунтується на моделі "видавець-передплатник". Основна функція протоколу полягає в забезпеченні з'єднання між пристроями за допомогою шини обміну повідомленнями рис. 2.12. Протокол DDS може ефективно та синхронно передавати мільйони повідомлень в секунду.

Пристрої вимагають передачі даних з неймовірною швидкістю, вимірюваною в мікросекундах, що відрізняється від стандартних IT мереж. Звичайні TCP потоки не можуть відповідати таким вимогам, оскільки пристрої повинні встановлювати зв'язок шляхом складних маршрутів. DDS, натомість, забезпечує контроль якості обслуговування, багатоадресну передачу, надійність і широкий охоплюючий проміжок передачі. Ще однією перевагою DDS є можливість фільтрації та відбору даних за адресами призначення, а кількість одержувачів може досягати тисяч. DDS також надає спеціальні легковажні версії для компактних пристроїв, що працюють в обмежених умовах. Умови зіркоподібних мереж не підходять для використання даних від пристроїв, тому DDS використовує прямий шинний зв'язок між пристроями на базі реляційної моделі даних, що називається "шиною даних" (DataBus) - мережевий аналог бази даних.

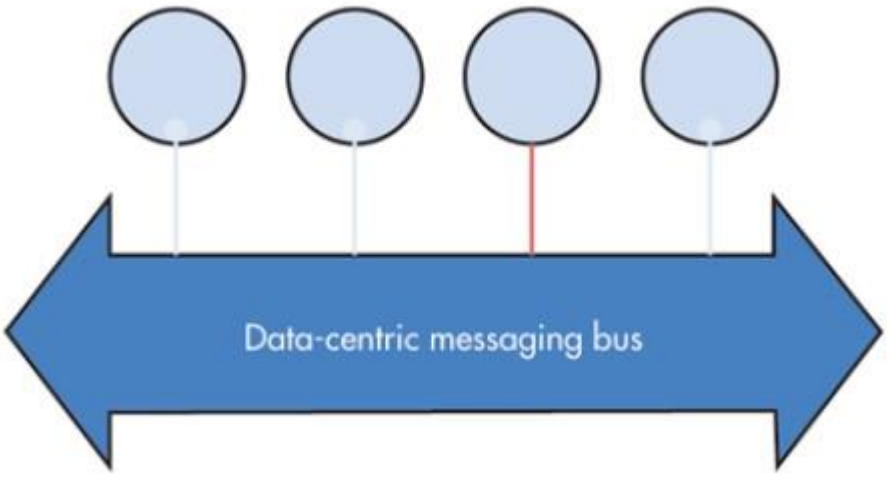

Рисунок 2.12 – Принцип з’єднання пристроїв за допомогою протоколу DDS в IoT

Аналогічно базі даних, яка керує доступом до збережених даних, шина даних управляє доступом та оновленнями даних для багатьох користувачів одночасно. Це важливо для високопродуктивних пристроїв, щоб вони могли працювати як єдина система. Високопродуктивні інтегровані системи використовують протокол DDS, оскільки він єдиний у своєму роді технології, яка поєднує гнучкість, надійність та швидкість, необхідні для розробки складних додатків реального часу. Серед таких додатків можна відзначити військові системи, вітроелектростанції, інтегровані системи лікарень, системи діагностичної візуалізації, системи супроводження ресурсів і автомобільні системи випробувань та забезпечення безпеки.

2.3.4 XMPP

XMPP (eXtensible Messaging and Presence Protocol) – це відкритий протокол, що базується на XML, і призначений для миттєвого обміну повідомленнями та інформацією про присутність в режимі, близькому до реального часу. Початково розроблений як легко розширюваний, XMPP крім передачі текстових повідомлень підтримує передачу голосу, відео та файлів через мережу.

У протоколі XMPP використовується текстовий формат XML для забезпечення природного зв'язку між людьми. Протокол працює через TCP або HTTP поверх TCP. Однією з переваг XMPP є метод адресування за допомогою ідентифікаторів Jabber ID, які включають в себе вузол, домен і, необов'язково, ресурс. Адреса має формат username@gmail.com, що допомагає об'єднувати користувачів у великому просторі Інтернету. XMPP підтримує різні комунікаційні моделі, такі як запит-відповідь, публікація, підписка та інші.

XMPP пропонує простий спосіб адресування пристроїв, що особливо зручно, коли дані передаються між віддаленими, часто незалежними точками, як у випадку зв'язку між двома абонентами. Незважаючи на те, що цей протокол не відзначається високою швидкістю, більшість реалізацій використовують методи опитування або перевірки доповнень тільки за потребою.

Однак XMPP має суттєві переваги, такі як безпека та масштабованість, тому він ідеально підходить для застосувань в невеликих мережах Інтернету речей.

2.3.5 CoAP

CoAP (Constrained Application Protocol) – це протокол передачі даних, розроблений для мереж та пристроїв з обмеженими ресурсами, таких як IoT пристрої та M2M додатки. Робоча група IETF-CORE створила його з метою забезпечення ефективної комунікації в обмежених умовах мережі. На відміну від HTTP, CoAP оптимізований для використання в пристроях з обмеженими ресурсами та використовує транспортний протокол UDP.

Протокол CoAP в основному використовує запити та відповіді, де GET (отримання інформації про ресурс), PUT (запис нових даних у ресурс), POST (зміна стану ресурсу) та DELETE (видалення ресурсу) є основними операціями. Клієнти (користувацькі програми) використовують ці повідомлення для керування та спостереження за ресурсами. При запиті встановлюється прапор спостереження, що дозволяє серверам надсилати оновлення стану ресурсу після початкового запиту. Це забезпечує можливість організації потокової передачі змін стану датчиків та інших ресурсів.

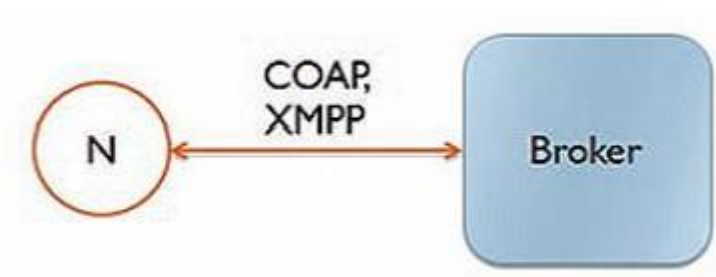

Рисунок 2.13 – Мережевий сегмент, де використовуються протоколи CoAP та XMPP

На ділянці мережі між сенсорними вузлами та брокером для забезпечення їх зв'язку та обміну даними найчастіше використовуються протоколи XMPP та CoAP. XMPP застосовується для реєстрації, конфігурації вузлів та обміну

повідомленнями, особливо в системах освітлення, клімат-контролю та в невеликих персональних мережах. З іншого боку, CoAP ідеально підходить для пристроїв з обмеженими ресурсами та мереж з низьким енергоспоживанням, таких як системи датчиків у розумних будинках. Ці протоколи забезпечують ефективну комунікацію та обмін даними в мережах Інтернету речей.

2.3.6 MQTT

MQTT (Message Queue Telemetry Transport) – це протокол обміну даними, спеціально створений для передачі даних на віддалених локаціях з обмеженими ресурсами, де важливі низька потреба в пропускній здатності та ефективне використання мережевих ресурсів. Він є легким, компактним і відкритим протоколом, ідеально підходить для застосування в системах машинного навчання та мережах машинного-машина (M2M). Крім того, існує варіант протоколу MQTT-SN (MQTT для мереж датчиків), раніше відомий як MQTT-S, який спеціально призначений для вбудованих бездротових пристроїв без підтримки TCP/IP мереж.

На рис. 2.14 показана загальна структура повідомлень протоколу MQTT. Кожне повідомлення має наступні складові:

Заголовок фіксованої довжини MQTT, який містить основну інформацію про повідомлення.

Заголовок змінної довжини, який може змінюватися в залежності від типу повідомлення та містить додаткові метадані.

Поле корисного навантаження змінної довжини, яке містить саму інформацію, яку передає повідомлення.

У заголовку фіксованої довжини протоколу MQTT включені наступні поля:

– Тип повідомлення (Message Type) – вказує на тип повідомлення, наприклад, публікація (Publish), підписка (Subscribe) або відключення (Disconnect).

– Прапор дублювання (DUP) – показує, чи є повідомлення дублікатом.

– Рівень якості обслуговування (QoS Level) – визначає, як брокер має обробляти повідомлення, наприклад, чи має він підтверджувати його отримання та доставку.

– Прапор збереження (Retain) – вказує, чи має брокер зберегти останнє отримане повідомлення з цим тематичним відомостями для нових підписок.

– Залишкова довжина (Remaining Length) – визначає довжину залишкової частини повідомлення після заголовка фіксованої довжини.

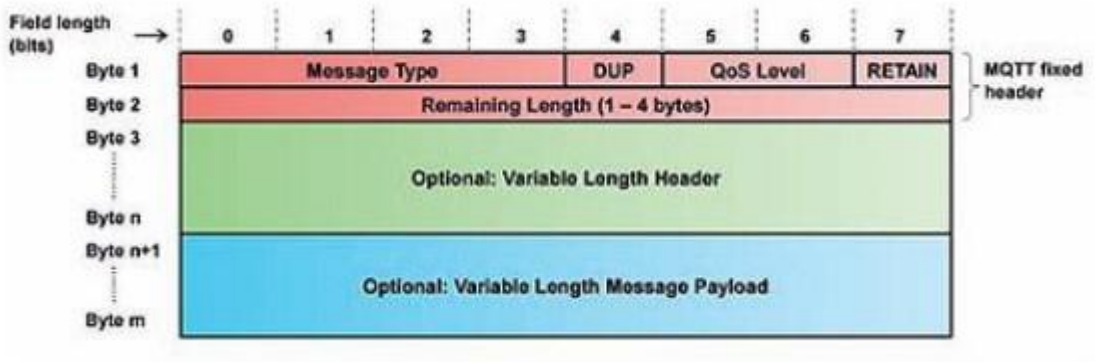

Рисунок 2.14 – Загальний формат повідомлення протоколу MQTT

Процес роботи протоколу MQTT можна спростити таким чином:

– Видавець передає повідомлення з певними даними (наприклад, вимірювання вологості з датчиків) на брокера, вказуючи тему (Topic), до якої відносяться ці дані (наприклад, "вологість").

– Брокер аналізує, які з передплатників мають підписку на певні теми, такі як "вологість".

– Підписникам, які підписані на тему "вологість", брокером буде відправлено повідомлення з інформацією від датчиків вологості.

Таким чином, різноманітні підписники можуть підписатися на цікаві для них теми і отримувати необхідну інформацію безпосередньо від видавця, який публікує цю інформацію. На рис. 2.15 представлена схема передачі інформації, відома як "видавець-підписник".

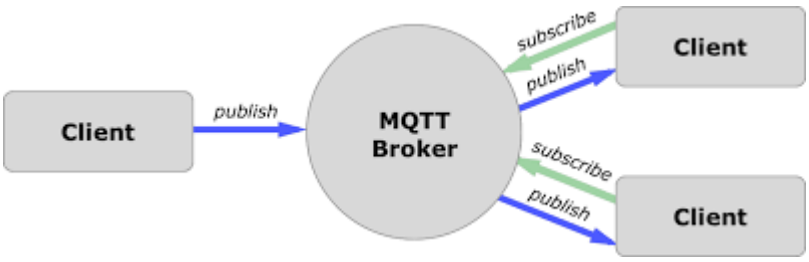

Рисунок 2.15 – Принцип роботи протоколу MQTT

2.3.7 STOMP

STOMP (Simple Text Oriented Message Protocol) – це простий протокол обміну повідомленнями, який дозволяє легко взаємодіяти з багатьма мовами програмування, платформами та брокерами повідомлень. Він відповідає шаблону "видавець-підписник" і забезпечує зв'язок з брокером за допомогою таких повідомлень, як SEND (надіслати), SUBSCRIBE (підписатися), UNSUBSCRIBE (відписатися), BEGIN (почати), ABORT (відмінити), ACK (підтвердити), NACK (відмовити в підтвердженні), DISCONNECT (відключитися), використовуючи метод "запит-відповідь".

Цей протокол широко використовується в ситуаціях, де необхідно просте і ефективне обмін повідомленнями в мережах з різноманітним обладнанням та платформами.

Використовуючи транспорт TCP, протокол є простим текстовим інтерфейсом, який дозволяє клієнтам STOMP взаємодіяти з будь-яким брокером повідомлень, який підтримує цей протокол. Це розв'язання сприяє ефективній комунікації між програмним забезпеченням, написаним на різних мовах програмування, та мережевими сервісами.

Завдяки великій кількості сумісних клієнтських бібліотек, цей протокол стає привабливим вибором для розробників, які шукають універсальне та надійне рішення для обміну повідомленнями між різними платформами та середовищами програмування.

Важливо зазначити, що для забезпечення функціонування брокера в мережі Інтернету речей можна використовувати обидва протоколи: MQTT і STOMP. Протокол STOMP орієнтований на взаємодію брокера з сервером, тоді як

протокол MQTT забезпечує "наскрізний" зв'язок як від брокера до сенсорних вузлів, так і від брокера до сервера.

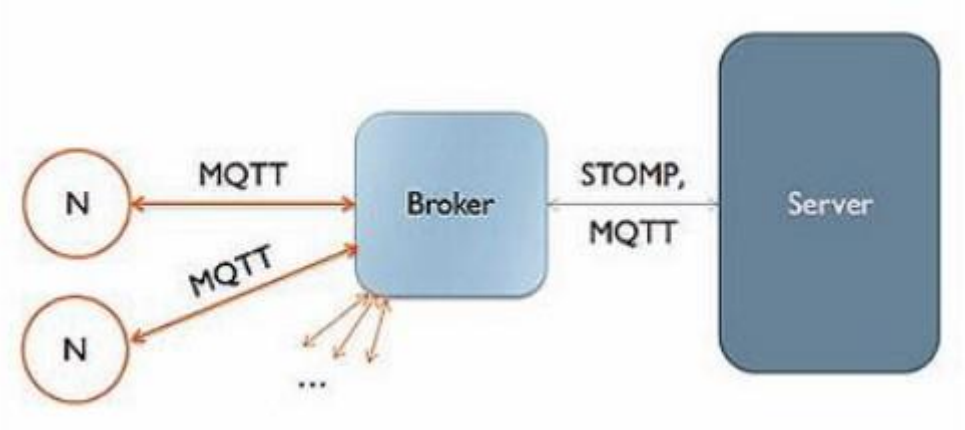

Рисунок 2.16 – Сегмент мережі де використовується протокол MQTT та STOMP

2.3.8 SOAP

SOAP (Simple Object Access Protocol) – це протокол обміну повідомленнями, який використовує формат XML для передачі структурованих та довільних даних в розподіленому обчислювальному середовищі. SOAP використовує модель з'єднання, що гарантує надійну передачу повідомлень від відправника до одержувача, з можливістю використання проміжних посередників, які можуть обробляти або додавати до повідомлень додаткову інформацію.

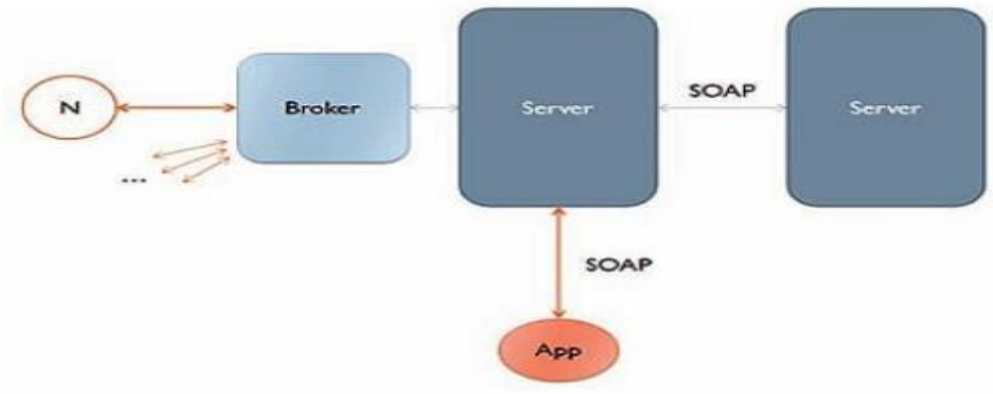

Рисунок 2.17– Сегмент мережі де використовується протокол SOAP

SOAP підтримує два механізми доступу: SOAP MESSAGE та SOAP RPC.

SOAP MESSAGE – це протокол, який дозволяє відправляти та обробляти SOAP повідомлення, використовуючи об'єкт Message. Він призначений для асинхронних комунікацій і може мати як негайну, так і відкладену відповідь на запит.

SOAP RPC є простим протоколом "запит-відповідь", який ґрунтується на об'єкті Call. Цей механізм використовується для синхронного віддаленого виклику процедур за допомогою XML.

Завдяки різним типам повідомлень (GET, SOAP ACTION–RESPONSE, SOAP ACTION), які можуть бути використані в протоколі "запит-відповідь", SOAP може взаємодіяти з будь-яким протоколом прикладного рівня, таким як FTP, HTTPS або SMTP.

Таблиця 2.3 – Порівняння розглянутих протоколів

Протокол	Транспорт	Призначення	Особливості
DDS	UDP	Для мереж, що потребують розподіленого навантаження	Реалізує прямий шинний зв’язок між пристроями на базі реляційної моделі даних. Підтримує збереження історії та механізми контролю життєдіяльності.
Продовження таблиці 3.3XMPP	TCP	Для адресації в невеликій персональній мережі	Використовує XML-потоки та XML-строфи для швидкого асинхронного обміну. Використовує схему адресації JID для ідентифікації користувачів.
CoAP	UDP	Для мереж з обмеженими ресурсами, низьким електроспоживанням	Представляє двійкову версію протоколу HTTP, спрощену для транспортування даних по лініям з обмеженою пропускною здатністю.
MQTT	TCP	Для завантажених	Підтримує різні класи якості

		мереж з великою кількістю пристроїв та брокером	обслуговування QoS (1-3) та механізми черг повідомлень.
STOMP	TCP	Для мереж з можливістю використання декількох комбінацій різних протоколів через брокера	Взаємодіє з більшістю мов, платформ та брокерами, забезпечуючи простий протокол передачі повідомлень.
SOAP	TCP	Для розподіленої обчислювальної мережі	Підтримує два механізми доступу: SOAP RPC та SOAP Message.

Таблиця 2.4 – Операції, що виконуються аналізованими протоколами

Операції	Відмінні особливості
DDS	Процедури отримання та відправки даних. Підтримує прямий шинний зв’язок, зберігання історії та механізми контролю життєдіяльності.
XMPP	Процедури запиту інформації/вимог, отримання даних, встановлення нових значень або заміщення існуючих. Використовує XML-потоки та схему адресації JID.
CoAP	Процедури запису та отримання необхідних конкретних параметрів. Представляє двійкову версію протоколу HTTP, призначену для мереж з обмеженою пропускною здатністю.
MQTT	Процедури обробки публікацій/підписки. Підтримує різні класи якості обслуговування QoS (1-3) та механізми черг повідомлень.

3 ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ ІОТ В УКРАЇНІ

3.1 Стан технологій передачі даних в Україні, досягнення та перспективи

Українські телекомунікаційні компанії активно впроваджують технології передачі даних в мережі Інтернету речей (IoT). Наразі в країні найбільш поширеними є дві основні технології для передачі даних на великі відстані: LoRaWAN та NB-IoT.

Основна відмінність між ними полягає в тому, що LoRaWAN працює в неліцензованому діапазоні частот, тоді як мережа NB-IoT працює в ліцензованому діапазоні на частотах, що використовуються мережами 4G. Для операторів зв'язку перевагою вибору мереж NB-IoT є можливість використання наявної інфраструктури мережі.

Обидві технології мають свої переваги та обмеження, та вибір між ними залежить від конкретних вимог і потреб проекту IoT.

Наразі Lifecell вирішила розвивати мережу IoT шляхом будівництва нової інфраструктури, використовуючи технологію LoRaWAN. Компанія обгрунтувала свій вибір тим, що LoRaWAN, як технологія, працює на низьких частотах, надаючи можливість забезпечувати більше покриття, ніж NB-IoT, що працює на вищих частотах (1800 МГц). Для реалізації цього плану, оператор обрав частоту 868 МГц. Такий вибір технології дозволить підтримувати зв'язок між пристроями на відстані до 15 км, з мінімальним енергоспоживанням.

Наразі Lifecell спільно з IoT Ukraine встановили понад 80 базових станцій. У Києві, Львові та Кропивницькому, вже запущено доступ до Інтернету речей для трьох обласних центрів України. Ці базові станції покривають 90% територій цих міст і успішно підключили перших клієнтів.

У процесі впровадження цього проекту були протестовані онлайн-рішення для "розумних" міст, моніторингу навколишнього середовища, логістичних сервісів, систем "розумного" будинку та інших інноваційних напрямків.

Послуги технологій Інтернету речей (IoT) стають все більш популярними серед компаній, які зацікавлені в різноманітних сферах діяльності, включаючи облік витрат на водопостачання, газ та електроенергію, розумне освітлення, стеження, моніторинг відкриття дверей, а також контроль вологості та температури в приміщеннях. Наразі більше, ніж 10 бізнес-компаній різних секторів вже активно використовують послуги IoT.

У лютому 2019 року Vodafone Україна оголосила про успішне завершення тестування технології NB-IoT в найбільших містах України. Пристрої NB-IoT можуть обмінюватися даними на частоті 1800 МГц. Ця технологія забезпечує стабільний доступ до мережі навіть у важкодоступних місцях, таких як шахти ліфтів та підвали.

Розгортання технології NB-IoT на базі мережі LTE забезпечує високий стандарт безпеки для користувачів та партнерів. Зокрема, вона використовує шифрування та автентифікацію на базі SIM-карти, що забезпечує високий рівень захисту даних. Ця можливість недоступна для інших технологій, таких як LoRa.

Крім того, NB-IoT дозволяє оптимізувати енергозбереження, що дозволяє пристроям працювати на одній батареї до 10 років. При цьому, мережа NB-IoT має вищу ємність порівняно з голосовою мережею, що дозволяє легко масштабувати мережу за потреби.

3.2 Майбутність технологій передачі даних в Україні

Наразі найбільш очікуваною та перспективною технологією, яка стимулює розвиток IoT в Україні та в усьому світі, є технологія 5G.

Головною перевагою 5G є підтримка ширшого діапазону частот, що призводить до значного збільшення швидкості передачі даних. Швидкість передачі даних у мережах 5G може перевищувати 10 Гбіт/с, що в десятки разів

перевищує показники 4G. Це дозволить значно покращити якість і швидкість передачі даних для різних сфер застосування, включаючи IoT.

Ще однією важливою особливістю 5G є мінімальна затримка та безперебійність. Порівняно з мережею 4G, затримка зменшилася у 10 разів: якщо раніше вона становила 10 мілісекунд, то тепер в мережі 5G вона складає всього 1 мілісекунду. Це дозволяє передавати дані практично в реальному часі, що відкриває широкі можливості для розвитку інтерактивних інтернет-застосунків та розваг.

Стандарт 5G передбачає наступні характеристики:

– пікова швидкість завантаження даних на одну базову станцію до 20 Гб/с.;

– швидкість завантаження даних до 100 Мб/с і вивантаження до 50 Мб/с для кожного абонента;

– можливість руху абонентських пристроїв зі швидкістю до 500 км/г між базовими станціями;

– здатність пристроїв переключатися між режимом заощадження енергії та робочим режимом за 10 мс.

– затримки до 4 мс за сприятливих умов, і до 1 мс для спеціалізованих з'єднань;

– поліпшена ефективність використання радіочастотного спектру;

– можливість передачі даних зі швидкістю 1 Гб/с одночасно для багатьох користувачів на одному поверсі будівлі;

– здатність працювати з до 1 млн пристроїв на 1 км.

Завдяки впровадженню технології 5G очікується значний прогрес у вдосконаленні та впровадженні нових технологій у різних аспектах нашого життя. Це охоплює такі сфери як медицина, технології, розумний будинок, розумне місто та розваги. Давайте розглянемо ці сфери детальніше.

3.2.1 Медична галузь

Після впровадження технології 5G можливим стане проведення віддалених хірургічних операцій, де хірург може керувати роботизованим обладнанням на

великій відстані від пацієнта. Це відкриє нові можливості для проведення складних медичних процедур у віддалених районах або навіть під час екстрених ситуацій. Крім того, завдяки використанню технології 5G, хірург може отримувати реальний час відображення візуальних та тактильних даних під час операції, що підвищить точність та безпеку процедури.

Володіючи спеціальним обладнанням, лікар зможете керувати необхідними інструментами та бути онлайн під час операцій. Завдяки технології 5G ви також зможете оперативно реагувати на погіршення стану здоров'я через спеціальні датчики або звичайні смарт-годинники. Наприклад, це допоможе у вирішенні таких проблем, як захист від падінь, який вже випробувала компанія Apple у моделі Apple Watch 4, проте без підтримки 5G ця функція ще не готова до реального використання.

Додатково, завдяки високим швидкостям 5G стане можливим швидке декодування ДНК. Навіть зараз ця процедура виконується, але вона потребує великих обсягів даних: інформація про геном однієї людини може займати до 140 гігабайт, і відправлення цих даних може зайняти лише одну-дві хвилини.

У випадку аварії або серцевого нападу ваш лікар швидко отримає інформацію та відправить карету швидкої допомоги, завдяки датчикам, розташованим у вашому пристрої. Це дозволить медичному персоналу точно визначити ваше місце знаходження та швидко надати допомогу.

3.2.2 Безпілотні авто та квадрокоптери

У майбутньому технологія 5G може значно знизити ймовірність ДТП та сприяти розвитку безпілотних автомобілів. Завдяки швидкому та надійному зв'язку 5G, автомобілі зможуть швидше та точніше реагувати на зміни дорожньої ситуації, уникати транспортних пригод та обходити переповнені дороги. Це може призвести до зменшення заторів та покращення загальної безпеки на дорогах.

Безпілотні автомобілі в майбутньому будуть інтегруватися з камерами, світлофорами та іншими дорожніми системами для миттєвого отримання та

аналізу інформації про стан доріг та дорожніх умов. Вони зможуть автоматично реагувати на зміни погоди та інші фактори, що впливають на безпеку на дорозі.

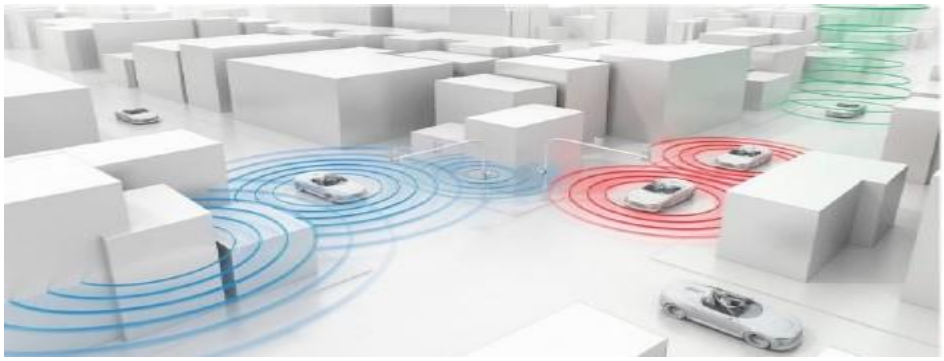

Рисунок 3.3 – Принцип роботи безпілотних транспортних засобів

Максимальна дальність польоту квадрокоптерів збільшиться, і буде обмежуватися виключно потужністю акумулятора. Управління дронами буде можливе в режимі реального часу з віддалених місць. Дрони будуть активно обмінюватися інформацією між собою, що сприятиме автоматизації їх масового використання без прямого втручання людини.

Рисунок 3.4 Квадрокоптери в розумних містах

У майбутньому квадрокоптери можна буде використовувати для пошуку людей, які заблукали в важкодоступних місцях. У разі потреби вони зможуть оперативно доставити необхідні медикаменти та речі, доки рятувальники дістануться до потерпілих.

4 ТЕХНІКО – ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

4.1 Розрахунок капітальних витрат на розробку

Капітальні витрати на розробку становлять:

$$К=К1+К2 \quad (4.1)$$

де: К1– витрати на розробку, грн.;

К2– витрати на налагодження і дослідну експлуатацію програмного засобу на ПК, грн.;

4.2 Складові структури витрат на розробку

Складові структури витрат на розробку та реалізацію розробки розраховуються за формулою:

$$К1=Зз+Нз+Ві, \quad (4.2)$$

де: Зз – загальна зарплата розробників, грн;

Нз – нарахування на зарплату, грн;

Ві – інші витрати, грн;

Для проведення розрахунків зарплати (Зз) необхідно визначити спеціальність робітників, чисельність робітників і трудомісткість цих робіт. Для розробки проектного рішення потрібно чотири спеціалісти розробники:

– Керівник проекту(К);

–Студент-дипломник(СД);

– Консультант з економічне ї частини(КЕ);

– Консультант з охорони праці(КОП);

Згідно з штатним розписом сума витрат на оплату праці робітників, з 01.01.2025р. складає:

– Керівник (викладач вищої категорії) – 107,93 грн/год;

– Консультант з економічної частини (викладач вищої категорії) – 107,93 грн/год;

– Консультант з охорони праці(викладач першої категорії) 93,70 грн/год;

– Час витрачений керівником – tk = 14 годин.

– Час витрачений консультантом з охорони праці – tko= 1 година.

– Час витрачений консультантом з економічної частини–tke = 1 година.

– Час витрачений студентом дипломником tc = 3×50= 150 годин.

Витрати на оплату праці керівника проекту:

Ск = 14 роб.год.× 107,93 грн.год.=1511,02 грн.

Витрати на оплату праці консультанта з економічної частини:

Ске = 1 роб.год.×107,93грн.год.= 107,93 грн.

Витрати на оплату праці консультанта з охорони праці :

Ско = 1 роб.год×93,70грн.год.= 93,70грн.

Денна оплата студента дипломника :

1510/173=8,73 грн.

1510 – стипендія

173 – місячний фонд робочого часу, годин.

Витрати на оплату праці студента дипломника

Сс = 8,73×150= 1310 грн.

Витрати на оплату праці робітників проектустановлять

Зз= Ск+Ске+Ско+Сс= 1511,02 +107,93 +93,70 +1310= 3022,65 грн.

Нарахування на зарплату визначаються в розмірі 22% від фонду оплати праці

Нз = Зз×22% = (3022,65 ×22)/100 = 664,98 грн.

де 22 – норматив нарахування на зарплату, %

Інші витрати Ві відображають витрати які, не враховані в попередніх статтях витрат. Ці витрати розраховуються згідно структури витрат(5%)

Ві = 0.05×(Зз+Нз)= 0.05×(3022,65 +664,98)=1843,93 грн.

К1 = Зз+Нз+Ві= 3022,65 +664,98 +1843,93 =5578,56 грн.

4.3 Витрати на відлагодження розробки

Витрати на від лагодження та дослідну експлуатацію розробки

$$К2 = Sм\text{-}г. \times t \quad (4.3)$$

де Sм-г. – вартість однієї машино-години роботи конкретно ПК, грн./год.;

t–машинний час, витрачений на накладку та дослідну експлуатацію програмного засобу, год.

Вартісь 1 машинно-години роботи ПК розраховуємо за складовими витрат на таку роботу:

$$Sм\text{-}г =(А+Ен)/Фд \quad (4.4)$$

де А – амортизація використаного ПК, грн;

Ен – вартість електроенергії, яку споживає ПК, грн.;

Фд – дійсний час від лагодження програми, год.;

Розрахунок складових вартості 1 машино-години роботи ПК:

а) амортизація ПК становить

А= (Кт×На)/100 = (670,31 ×15%)/100= 100,55 грн.

Де Кт – вартість використання ПК, грн..

На – норма амортизації (На=15%)

Кт = (Кс×Тексп)/Твик = (14625×2,2)/48= 670,31 грн.

де Кс – вартість компютероної системи,грн.

Тексп – період експлуатації системи 2.2 місяців(50 робочих днів)

Твик – термін корисного використання 4 роки (48 місяців):

Кс= Ркомп×Р$ = 500×41,00=14625 грн.

де Ркомп –вартість комп'ютерної системи у доларах США;

Р$ – курс долара США по курсу НБУ на момент купівлі системи.

б) вартість використання електроенергії розраховується за формулою:

Ен = (Р×Тф)×Фд×Квик=(0,25 ×5,60)×150×0,8=154,8грн.

де Р – потужність обчислювальної системи, кВт (Р=0,25)

Квик – коефіцієнт використання ПК

Тф – ціна за 1кВт/год.,грн..(Тф = 5,16 грн.)

Фд – дійсний час від лагодження програми

Фд = пр.д.×Тсер= 50р.дн.×3год. = 150год.

Де пр.д. – кількість робочих днів ПК

Тсер = 3 год – середній щоденний час роботи ПК

Отже вартість 1 машино-години роботи і від лагодження на ПК становить

Sм-г=(100,55+154,8)/150= 1,70 грн.

Таким чином сумарні витрати на від лагодження і дослідну експлуатацію проектного рішення становлять:

К2=Sм-г×Фд= 1.70×150=255 грн.

Отже, капітальні витрати на розробку проектного рішення за формулою становлять:

К=К1+К2 = 5578,56 + 255 = 5833,56 грн.

Загальний кошторис витрат на розробку проектного рішення приведений в таблиці 4.1

Таблиця 4.1 – Кошторис витрат на розробку проектного рішення

Складові елементи витрат	Умовне позначення	Сума витрат, грн
Витрати на оплату праці	Зз	3022,65
Нарахування на зарплату	Нз	664,98
Інші витрати	Ві	1843,93
Разом	К1	5578,56
Витрати на відлагодження	К2	255
Разом К=К1+К2	К	5833,56

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЕДІЯЛЬНОСТІ

5.1 Загальні положення

Визначення поняття охорони праці дається в ст. 1 Закону України від 14 жовтня 1992 р. «Про охорону праці». Охорона праці – це система правових, соціально-економічних, організаційно-технічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. В поняття охорони праці входять і всі ті заходи, що спеціально призначені для створення особливих полегшених умов праці для жінок і неповнолітніх, а також працівників зі зниженою працездатністю. Охорону праці і здоров'я громадян віднесено до пріоритетних напрямків соціальної політики України. Так, Конституція України одним з основних соціальних прав громадян визначає право кожного на належні, безпечні й здорові умови праці, встановлює, що використання праці жінок і неповнолітніх на небезпечних для їхнього здоров'я роботах забороняється. Завдання охорони праці:

– проектування підприємств, технологічних процесів і конструювання обладнання з обов'язковим виконанням вимог охорони праці;

– знаходження оптимальних співвідношень між різними факторами виробничого середовища, що дозволяє забезпечити мінімум несприятливого впливу їх на здоров'я працівників;

– розробка конкретних заходів щодо покращення умов праці та забезпечення її безпеки на основі застосування у виробництві новітніх досягнень науки і техніки;

– застосування раціональних засобів захисту працівників від впливу несприятливих факторів виробничого середовища, а також втілення організаційних заходів, які нейтралізують або послаблюють ступінь їх впливу на організм людини;

– розробка та застосування методів і засобів оцінки ефективності заходів з охорони праці, що плануються і здійснюються.

5.2 Організація охорони праці на підприємстві

На сучасному етапі науково-технічного розвитку нашої держави питання охорони праці на підприємствах є одним із найактуальніших.

Належна організація охорони праці, яка відповідає вимогам нормативно-правових актів, є основним заходом профілактики та запобігання виробничому травматизму й професійній захворюваності. Крім того, кожним трудовим договором передбачаються зобов’язання роботодавця щодо забезпечення найманих працівників безпечними умовами праці.

Законодавство України покладає на всіх роботодавців обов'язок щодо забезпечення безпечних і нешкідливих умов праці. Витрати на охорону праці на підприємстві згідно зі ст. 19 Закону повинні становити не менше 0,5% від фонду оплати праці за попередній рік, а за невиконання законодавства про охорону праці до підприємства можуть бути застосовані санкції аж до заборони його експлуатації.

Для того щоб не поставити під загрозу існування підприємства, роботодавцю необхідно:

– створити службу охорони праці.

Згідно зі ст. 15 Закону така служба обов'язково повинна бути створена на підприємстві з кількістю працюючих 50 і більше осіб відповідно до Типового положення про службу охорони праці, затвердженого наказом Держкомітету з нагляду за охороною праці від 15.11.2004 № 255. На підставі цього документа також має бути розроблено Положення про службу охорони праці цього підприємства, визначено структуру такої служби, її чисельність, основні завдання, функції та права її працівників. На підприємствах із кількістю працівників менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку.

– Розробити та затвердити на підприємстві положення, інструкції та інші акти з охорони праці.

Обов'язок роботодавця стосовно розробки та затвердження документів, які повинні встановлювати правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майдан-чиках і робочих місцях, передбачений ст. 13 Закону про охорону праці.

– Організувати проведення інструктажів з питань охорони праці.

Перед початком роботи нового працівника роботодавець згідно зі ст. 29 КЗпП зобов'язаний проінформувати його під розпис про умови праці, наявні на його робочому місці, у тому числі про всі небезпечні чи шкідливі виробничі фактори, які ще не усунуто, та про можливі наслідки їх впливу на здоров'я працівника, а також про можливі пільги та компенсації за роботу в таких умовах.

– Забезпечити навчання і перевірку знань з питань охорони праці.

Згідно зі ст. 18 Закону працівники, зайняті на роботах з підвищеною небезпекою або там, де є потреба у професійному доборі, проходять спеціальне навчання і перевірку знань відповідних нормативно-правових актів з охорони праці. Таке навчання з питань охорони праці може проводитись як безпосередньо на підприємстві, так і навчальним центром.

– Подбати про проведення медичних оглядів.

Згідно зі ст. 169 КЗпП роботодавець зобов'язаний за свої кошти організувати проведення попереднього (при прийнятті на роботу) та періодичних (протягом трудової діяльності) медоглядів працівників, зайнятих на важких роботах, роботах із шкідливими чи небезпечними умовами праці або таких, де є потреба у професійному доборі. Також він зобов'язаний проводити щорічний обов'язковий медогляд осіб віком до 21 року.

– Забезпечити працівників засобами індивідуального захисту.

На роботах із шкідливими й небезпечними умовами праці, а також на роботах, пов'язаних із забрудненням або несприятливими температурними умовами, працівникам згідно зі ст. 164 КЗпП необхідно безкоштовно видавати спеціальний одяг, взуття та інші ЗІЗ.

– Провести атестацію робочих місць.

На підприємствах, де технологічний процес, використовуване обладнання, сировина, матеріали є потенційними джерелами шкідливих і небезпечних виробничих факторів, які можуть негативно впливати на стан здоров'я працюючих, повинна проводитись атестація робочих місць за умовами праці. Така атестація повинна проводитися атестаційною комісією, склад і повноваження якої визначаються наказом по підприємству в строки, передбачені колективним договором, але не рідше одного разу на 5 років. Порядок проведення такої атестації передбачений постановою КМУ від 01.08.1992 № 442. Відомості про результати атестації заносяться в картку умов праці.

– Налагодити облік нещасних випадків.

Згідно зі ст. 22 Закону «Про охорону праці» роботодавець зобов'язаний організувати розслідування та вести облік нещасних випадків, професійних захворювань і аварій у порядку, встановленому постановою КМУ від 30.11.2011 № 1232. За результатами такого розслідування роботодавець повинен складати акт за формою Н-5 (якщо нещасний випадок визнано таким, що не пов'язаний з виробництвом) або Н-1 (якщо він визнаний пов'язаним з виробництвом). Один із примірників повинен видатися потерпілому або іншій зацікавленій особі не пізніше трьох днів з моменту закінчення розслідування.

5.3 Заходи безпеки на робочому місці

Конструкція робочого місця, його розміри та взаємне розташування його елементів повинні відповідати антропометричним, фізіологічним І психофізіологічним характеристикам людини, а також характеру роботи.

Організація робочих місць повинна забезпечувати стійке положення та вільність рухів працівника, безпеку виконання трудових операції виключати або допускати лише в деяких випадках роботу в незручну позиціях, котрі зумовлюють підвищену втомлюваність.

Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого; всі необхідні для роботи предмети повинні знаходитись поряд з працівником, але не заважати йому;

– ті предмети, котрими користуються частіше, розташовуються ближче, ніж ті предмети, котрими користуються рідше;

– предмети, котрі беруть лівою рукою, повинні знаходитись зліва а ті предмети, котрі беруть правою рукою, повинні знаходитись справа;

– якщо використовують обидві руки, то місце розташування інструментів вибирається з врахуванням зручності захоплювання його двома руками;

– небезпечніше, з точки зору можливості травмування обладнання повинне розташовуватись вище, ніж менш небезпечне. Однак слід враховувати, що важкі предмети під час роботи зручніше опускати, ніж піднімати.

5.4 Санітарно-гігієнічні вимоги

Санітарно-гігієнічні вимоги до умов праці під час виконання роботи мають відповідати визначеним нормативам:

– параметри мікроклімату у приміщенні забезпечували комфортне самопочуття організму. Параметри мікроклімату закритих приміщень унормовані за санітарні норми ДСН 3.3.6.042-99.

– освітлення приміщень та робочих місць забезпечене відповідно до встановлених вимог. Відносно вікна робоче місце розміщено так, що природне світло збоку, переважно з лівого та забезпечувало коефіцієнт природної освітленості не нижче 1,5 %. Освітленість за штучного освітлення в площині робочої поверхні становила 300 – 500 Лк. Відношення яскравості робочих поверхонь було 3:1, а яскравість робочих поверхонь і стін (іншого обладнання) – 5:1. Використана система вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

– Дотримані вимоги до рівнів шуму та вібрації. Було дотримано допустимих рівнів звукового тиску в октавних смугах частот, еквівалентні рівні звуку на робочих місцях встановлені санітарними нормами виробничого 17 шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99.

– Надходження свіжого повітря регульоване, виходячи із відповідних нормативних.

– Передбачений захист від шуму та вібрацій.

Дотримані заходи особистої гігієни на робочому місці (підтримання чистоти, миття рук тощо). Заходи особистої гігієни на робочому місці передбачають щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому місці тільки необхідних для роботи засобів. На робочому місці необхідно дотримуватись вимог правил внутрішнього трудового розпорядку.

ВИСНОВКИ

У роботі було детально розглянуто основні аспекти Інтернету речей (IoT) та технології передачі даних, що лежать в основі цієї концепції. Була розглянута архітектура IoT, включаючи рівні датчиків, мережевого, обробки даних та прикладного рівня, а також її переваги та недоліки.

Окрему увагу було приділено технологіям передачі даних на довгі та короткі відстані, таким як LoRaWAN, SigFox, NB-IoT, Z-Wave, RFID, Bluetooth Low Energy та інші. Проведено порівняльний аналіз їх характеристик, таких як дальність передачі, швидкість, безпека та інші.

Крім того, досліджено топологію мереж для передачі повідомлень в IoT та проведено порівняльний аналіз протоколів передачі повідомлень.

На основі досліджень стану технологій передачі даних на довгі відстані в Україні були виявлені перспективи розвитку IoT, зокрема на базі технології 5G. Розглянуті можливості застосування технології 5G у сферах медицини, автономних автомобілів, квадрокоптерів та розумних будинків свідчать про потенційні можливості її впливу на різні галузі життя.

Отже, можна зробити висновок, що IoT та технології передачі даних відкривають широкі перспективи для розвитку різноманітних галузей, а впровадження технології 5G може виявитися кроком до нових технологічних можливостей та інновацій у сучасному світі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Інтернет речей: чи зможе смартфон управляти бізнесом // електрон. текст. дані URL: http://persona.pumb.ua/ua/club/digest/detail.php?CODE=internet-veshchey-smozhet-li-smartfon-upravlyat-biznesom
2. МСЭ-Т Y.2060 // електрон. текст. дані URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I
3. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications // електрон. текст. дані URL: https://arxiv.org/pdf/1802.02041.pdf
4. IoT Explained – How Does an IoT System Actually Work? // електрон. текст. дані URL: https://medium.com/iotforall/iot-explained-how-does-an-iot-system- actually-work-e90e2c435fe7
5. The advantages and disadvantages of Internet Of Things // електрон. текст. дані URL: https://e27.co/advantages-disadvantages-internet-things-20160615/
6. The advantages and disadvantages of Internet Of Things (IoT) // електрон. текст. дані URL: https://www.linkedin.com/pulse/advantages-disadvantages-internet- things-iot-tommy-quek
7. MAC Layer Protocols for Internet of Things: A Survey // електрон. текст. дані URL: https://www.mdpi.com/1999-5903/11/1/16/htm
8. Sigfox Technology // електрон. текст. дані URL: https://www.betasolutions.co.nz/Blog/17/Sigfox-Technology-Review
9. Z-Wave // електрон. текст. дані URL: https://ru.wikipedia.org/wiki/Z-Wave
10. Z-Wave Technical Basics // електрон. текст. дані URL: https://www.domotiga.nl/attachments/download/1075/Z Wave%20Technical%20Basics-small.pdf

КОПІЇ ОБОВ’ЯЗКОВИХ КРЕСЛЕНЬ