НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені ІГОРЯ СІКОРСЬКОГО"

Факультет електроніки
(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем
(повна назва кафедри)

"На правах рукопису"
УДК 654.078

"До захисту допущено"

Завідувач кафедри

С.А. Найда
(ініціали, прізвище)

" 9 " грудня 2020 р.

Магістерська дисертація

зі спеціальності (спеціалізації) 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету речей
(код і назва)

на тему: "Особливості використання засобів інтернету речей у сферах критичного застосування"

Виконав: студент II курсу, групи ДВ-92мп
(шифр групи)

Макаренко Юлія Володимирівна
(прізвище, ім'я, по батькові) (підпис)

Керівник к.т.н., доц. Макаренко В.В.
(науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант
(назва розділу) (науковийступінь,вченезвання, прізвищетаініціали) (підпис)

Рецензент зав. відділом і-ту Кібернетики НАН України, професор, д.т.н., Романов В.А.
(науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент
(підпис)

Київ – 2020 року

Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"

Факультет Електроніки

Кафедра Акустичних та мультимедійних електронних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною (освітньо-науковою) програмою

Спеціальність 171 Електроніка (Електронні системи мультимедіа та засоби Інтернету речей)

ЗАТВЕРДЖУЮ
Завідувач кафедри
С.А Найда .
(ініціали, прізвище)
" 9 " грудня 2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Макаренко Юлії Володимирівні
(прізвище, ім'я, по батькові)

1 Тема роботи: Особливості використання засобів інтернету речей у сферах критичного застосування
керівник роботи Макаренко Володимир Васильович, к.т.н., доц,
затверджена наказом по університету від "05" листопада 2020 р. №3241-с

Термін подання студентом роботи 01 грудня 2020 року
2. Об'єкт дослідження Безпроводова сенсорна мережа на основі технології LoRa інтегрованої в системи IoT-моніторингу
3.Вихідні дані до роботи: Розробити систему контролю ключових параметрів інфраструктури на території НТУУ "КПІ ім. Ігоря Сікорського" на основі технології мережі LoRa з сенсорами для систем Інтернету речей
4.Перелік завдань, які потрібно розробити: Проаналізувати можливість впровадження системи моніторингу інфраструктури на основі систем Інтернету речей на території НТУУ "КПІ ім. Ігоря Сікорського", використовуючи технологію LoRa та запропонувати конфігурацію мережі.
5 Орієнтовний перелік публікацій: _____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Пошук інформаційних джерел за темою бакалаврської роботи	30.09.2020	Виконано
2	Дослідження можливостей безпроводових технологій для застосування в IoT системах	26.10.2020	Виконано
3	Дослідження структури та функціональних можливостей апаратних засобів для IoT систем	25.11.2020	Виконано
4	Укладання та оформлення пояснювальної записки	01.12.2020	Виконано
5	Підготовка та оформлення презентації для доповіді	05.12.2020	Виконано

Студентка _____ (підпис) Ю.В. Макаренко (ініціали, прізвище)

Керівник роботи _____ (підпис) В.В. Макаренко (ініціали, прізвище)

SUMMARY

This paper provides a comparative analysis of existing IoT system using LoRa technology on the territory of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". IoT projects, solutions and deployments need more than the connected physical objects and the data they ‘sense’ and capture. The physical ‘things’ and sensors/technologies in IoT devices, assets and things in IoT, consumer IoT, enterprise IoT also need technology to communicate about their internal state and external environment.

The structural and functional scheme of wireless sensor network on the basis of LoRaWAN technology, the plan of object and an arrangement of the equipment in the territory of the FEL case is designed.

LoRa is the new communication technology under the Low Power Wide Area Network (LPWAN). It emphasizes on the long-range communication with the high receiving sensitivity ability which allows it to work under the noise interference or noise floor effectively. The range of communication has become the critical part on most of the IoT system, especially in Wi- Fi and Bluetoothbased IoT system. With the emergence of LoRa technology, further improvements to applications of the Internet of Things (IoT) can be realized.

By using to provide the maximum coverage distance and increase the sensitivity of the connection on the FEL campus, an expansion factor of 12, a bandwidth of 125 kHz, an antenna in the 868 MHz band, and a transmitter power of 20 dBm are used. In practice, we will use Antares as a cloud service for data storage and display, for data analysis it is better to operate Node-red.

УДК 654.078

РЕФЕРАТ

Макаренко Ю.В. Особливості використання засобів інтернету речей речей у сферах критичного застосування: магістерська дис.: 171 Електроніка. Київ, КПІ ім. Ігоря Сікорського, 2020. 114 с.

Ключові слова: інтернет речей, iot, lora, комунікація, безпроводова сенсорна мережа, система моніторингу.

Актуальність дослідження. Зі зростанням кількісті підключеної техніки в Інтернеті зростає потреба у безпроводових сенсорних мережах, що доцільно використовувати у критичних сферах застосування. Це дозволяє вирішити проблеми передачі важливих даних або підтримки безпеки в приміщеннях для різних видів діяльності, як наслідок, підтримати безпечні умови роботи, де важливі наднадійні комунікації з малою затримкою.

Метою роботи є аналіз можливості впровадження Інтернету речей на територію НТУУ "КПІ ім. Ігоря Сікорського" ФЕЛ використовуючи технологію мережі LoRa, розробка архітектури системи підключення мережі LoRa та запропонування конфігурації мережі LoRa, розгорнутої у кампусі.

Об’єкт дослідження – безпроводова сенсорна мережа на основі технології LoRa інтегрованої в системи IoT-моніторингу.

Методи дослідження – теоретичний і практичний аналіз технології LoRa.

Наукова новизна одержаних результатів: запропонована БСМ у сферах критичного застосування з використанням технології LoRa

Практична значення одержаних результатів: спираючись на теоретичні результати, отримані у роботі, було запропоновано інтеграцію системи IoT-моніторингу на основі БСМ з використанням технології LoRa. Отримані результати досліджень можуть бути використані університетами та компаніями, які займаються моніторингом структури і навколишнього середовища, відстеження активів, а також моніторингом та оптимізацію процесів.

Апробація результатів дисертації: проектування безпроводової сенсорної мережі.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

BD	–	Big Data;
EDGE	–	Enhanced Data rates for GSM Evolution;
eMBB	–	enhanced Mobile Broadband;
GPRS	–	General Packet Radio Service;
GSM	–	Groupe Spécial Mobile;
IoT	–	Internet of Things;
LoRa	–	Long Range;
LPWA	–	Low-Power Wide-Area
LTE	–	Long-Term Evolution;
mMTC	–	massive Machine Type Communication;
OWA	–	Open Wireless Architecture;
SCADA	–	Supervisory Control And Data Acquisition;
SDWN	–	Software Defined Wireless Networking;
ULLRC	–	Ultra Low Latency Reliable Communication;
UMTS	–	Universal Mobile Telecommunications System;
WiMAX	–	Worldwide Interoperability for Microwave Access.

ВСТУП

"Інтернет речей" (Internet of Things – IoT) – це мережа фізичних об'єктів, які мають вбудовані технології, що дозволяють здійснювати взаємодію з зовнішнім середовищем, передавати відомості в своєму стані і сприймати дані ззовні [1].

Кількість підключених гаджетів до Інтернету досягло 26,6 млрд. штук, що в 3,5 разів перевищує число жителів нашої планети. Кожну секунду до Інтернету підключається 127 пристроїв, таких як побутова техніка для "розумних" будинків, датчики та інтелектуальні технології для промисловості. Китай, Північна Америка та Західна Європа складають 67% настановної IoT-бази.

Технології LPWA (Low-Power Wide-Area) обслуговують потреби ринку Інтернету Речей дешевими пристроями, які довго тримають батарею і дешевими мережами дальньої дії і при цьому підтримують величезну кількість з'єднань. Існує кілька варіантів для побудови LPWA мереж, але технології LoRaWAN показала найбільшу динаміку і отримує найбільшу частку ринку LPWA.

Тому у роботі розглядаються існуюча технологія LoRaWAN при побудові IoT-моніторингу та впровадження безпроводової сенсорної мережі на території НТУУ "КПІ ім. Ігоря Сікорського", використовуючи технологію мережі LoRa.

1 АНАЛІТИЧНИЙ ОГЛЯД

1.1 Що таке критичні сфери застосування

Критичні сфери застосування – це сфери, що взаємодіють з важливими функціями людини, що несуть наслідки фізичної загрози для життєдіяльності, такі як передача важливих даних або підтримка безпеки в приміщеннях для різних видів діяльності, як наслідок, підтримка безпечних умов роботи, де важливі наднадійні комунікації з малою затримкою.

Для продуктивного використання критично важливого Інтернету речей, система повинна відповідати параметрам: здатність працювати в суворих погодних умовах та у віддалених місцях, підтримка нових виробничих процесів, масштабованість для підтримки великомасштабних мереж з тисячами контролерів, роботів і машин, а також безпеки для захисту кінцевих пристроїв і мереж від загрози і нападу.

Одним із прикладів критично важливого IoT є управління роботизованими машинами і транспортними засобами, що працюють у вибухонебезпечних зонах промисловості. Це можуть бути такі технології, як робототехніка, 4K-телевізори і навіть віртуальна реальність (VR), всі з яких вимагають доставки великої кількості даних в режимі реального часу.

Критично важливий IoT включає меншу кількість кінцевих точок, які обробляють великі обсяги даних. З технічної точки зору, критично важливі програми IoT описуються як наднадійні комунікації з малою затримкою (Ultra-Reliable Low Latency Communication – URLLC). Він являє собою довгострокове бачення додатків і пристроїв з високою пропускною здатністю і малою затримкою, що виходить за рамки простого збору даних і охоплює більш складні сценарії.

Оскільки такі додатки, як безпека дорожнього руху, а також системи контролю та управління енергопостачанням, вимагають інформації, яка залежить від часу, і точного позиціонування, надійність і низька затримка важливі для життя.

Вони повинні працювати в обов'язковому порядку. Якщо з'єднання в критично важливій системі IoT обривається, то наслідки можуть бути фатальними.

Відмова в критично важливій системі Інтернету речей, на відміну від масового Інтернету речей, може привести до широко поширеним систематичним проблемам в розумному місті, бізнесі, інфраструктурі та несе загрозу безпосередньо людині.

Уявіть, що проблема з мережею виникає, наприклад, під час віддаленого хірургічного втручання або несправний датчик котла, що призводить до перегріву труб, все це приводить до загибелі людей.

Зв'язок атрибутів надійності, інформаційної та функціональної безпеки характеризується на рис. 1.1.

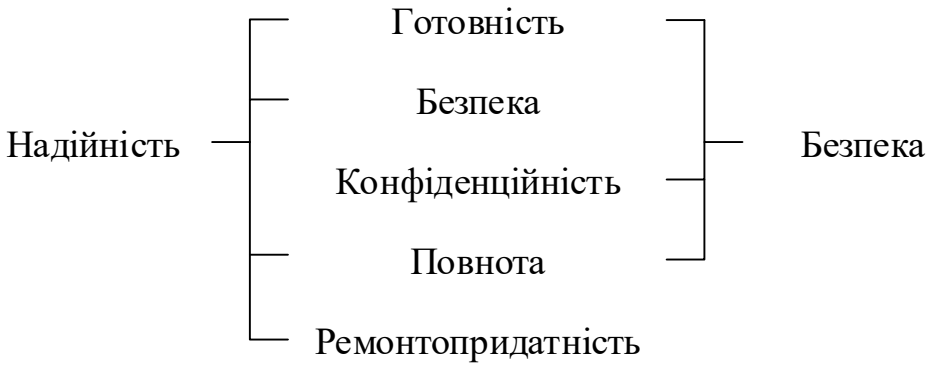

Рисунок 1.1 – Розподіл глобальних проектів за сферами застосування, заснованих на застосуванні технології Інтернету речей

За даними журналу IoT Analytics 2016 проекти, пов'язані з використанням технології Інтернету речей в 2016 році, розподілилися між різними сферами застосування відповідно на рис. 1.2. Ці дані отримані при оцінці 640 глобальних проектів в країнах Америки, Європи, Південно-Східної Азії, Близького Сходу та Австралії, що є свідченням появи нового класу так званих кібер-фізичних об'єктів. У таких об'єктах кошти забезпечення надійності, інформаційної та функціональної безпеки повинні бути об'єднані в єдину систему [2, 3].

"Розумні" міста застосовують систему критично важливою IoT забезпечення. Згідно з прогнозом IDC, до кінця 2020 року на облаштування смарт-міст буде витрачено 135 млрд. дол. Спочатку концепція "розумних" міст виникла в Європі. Першим містом з системою IoT в 2009 р, став Амстердам. США підхопили ініціативу в 2017 р. – першим американським смарт-містом став Коламбус (шт. Огайо). До 2020 р до ініціативи може приєднатися ще 100 міст, створених шляхом участі державних і приватних інвестицій.

Рисунок 1.2 – Розподіл глобальних проектів за сферами використання, заснованих на застосуванні технології Інтернету речей

У типовому "розумному" місті більшість завдань вирішується за допомогою мобільних додатків. Вони підказують як уникнути пробок, знайти місце для

парковки, попереджають про вибоїни на дорозі, інформують про заповнення сміттєвого контейнера і т. д. Базові IoT-пристрої роблять такі міста, як Нью-Йорк або Чикаго, більш життєздатними, що досягається за рахунок економії, поліпшення якості життя і розширення нових робочих місць.

Європейська влада планує перетворити вузи в "розумні" спільноти. 2020 рік стане роком, коли технологія смарт-міста буде тиражуватися в більш широких масштабах.

У 2020 році почнеться інтенсивний перехід від споживчого до промислового IoT (IIoT). Він буде застосовуватися в наступних областях: охорона здоров'я, роздрібна торгівля, сільське господарство та домашній побут.

Охорона здоров'я є найважливішою з критичних сфер використання IoT. Найімовірніше, основна частина інновацій в сфері IIoT торкнеться охорони здоров'я. IoT-пристрої дозволяють скоротити витрати на охорону здоров'я, підвищують рівень обслуговування пацієнтів, з їх допомогою можна впроваджувати нові методи профілактики і діагностики захворювань, а також покращувати ефективність лікування. Зокрема, вони допомагають лікарям стежити за станом здоров'я пацієнтів.

Медичні установи можуть за допомогою IoT контролювати роботу медичного обладнання та персоналу, а страхові компанії – виявляти випадки шахрайства.

Основне застосування IoT-пристроїв в охороні здоров'я:

- віддалений моніторинг – спеціальні телемедичні комп'ютерні системи або встановлене на мобільному пристрої ПО відправляють лікуючим лікарям згенеровані пацієнтом медичні дані (patient-generated health data, PGHD);
- носійні пристрої – пристрої, за допомогою яких відстежується стан і параметри життєдіяльності організму. Вони можуть інформувати членів сім'ї та лікарів про різкі зміни здоров'я пацієнта. Ці пристрої, призначені для контролю за артеріальним тиском і частотою серцевих скорочень,

можна також налаштувати таким чином, щоб вони здійснювали підрахунок калорій, виводили рекомендації лікаря, нагадували про прийом ліків тощо;

- моніторинг активів – оснащення медичного обладнання датчиками з підключенням до IoT-пристроїв.

За допомогою останніх медичні установи контролюють обладнання, таке як дефібрилятори, і можуть в режимі реального часу виявляти дефекти. Установи також можуть застосовувати цю технологію для оперативної розстановки персоналу.

Роздрібна торгівля. За даними журналу TotalRetail, до кінця цього року витрати на технології IoT в роздрібній торгівлі перевищать 35 млрд. дол. До IoT-інновацій в цій сфері належать такі:

- хвиля додатків і пристроїв нового покоління, з підтримкою штучного інтелекту, обробки великих даних і інших інноваційних технологій, таких як віртуальна/доповнена реальність (VR/AR) і блокчейн;
- покращений аналіз даних, використовуючи Edge Computing і 5G, які поліпшать швидкодію мережі й інші види зв'язку;
- SaaS стає нормою – все більше число сторонніх постачальників будуть розміщувати додатки і надавати їх клієнтам через Інтернет;
- розпізнавання голосу.

Як показують прогнози, в 2020 г. 50% інтернет-пошуку і управління IoT-пристроями буде здійснюватися за допомогою голосу. Технологія розпізнавання голосу вже широко використовується в смарт-динаміках (Apple HomePod).

Сільське господарство. У 2050 році загальна чисельність населення Землі бути досягне 9,6 млрд. чоловік. До цього часу значення IoT досягне критичного рівня – технологія дозволить знизити витрати, принесе економію часу і дозволить прогодувати таку величезну кількість людей. Згідно з дослідженням Business Insider Intelligence, до кінця 2020 року кількість впроваджених в сільськогосподарській галузі IoT-пристроїв досягне 75 млн. Передові IoT-пристрої, які включають робототехніку, безпілотні транспортні засоби, автоматизоване

обладнання, засоби дозованого розпилення застосовуються в наступних областях сільського господарства:

1. "Точне" фермерське господарство. Пристрої IoT роблять методи ведення сільського господарства більш контрольованими і точними, особливо це стосується тваринництва і вирощування сільськогосподарських культур.

2. Моніторинг поголів'я домашньої худоби. Власники ферм використовують сенсорні додатки IoT для збору даних про місцезнаходження, безпеки та стан здоров'я домашньої худоби.

3. "Розумні" теплиці. Застосування віддаленого моніторингу для захисту цінних рослин від екстремальних коливань температури.

У новому році IoT-пристрої для будинку стануть більш "розумними" і попит на них виросте. До таких гаджетів можна віднести наступні:

1. "Розумні" дверні замки. За допомогою таких пристроїв двері можна відкривати/замикати віддалено. З'являться замки, які дозволять надавати одноразові коди на вхід для відвідувачів.

2. "Розумні" зубні щітки. Безакумуляторні зубні щітки нового покоління, оснащені датчиками, будуть повідомляти вам (і стоматологам) про стан здоров'я.

3. "Розумні" кухні – кухні, обладнані спеціальними датчиками, які, наприклад, будуть нагадувати про вимикання електроприладів. Це також може бути посуд, який вміє підраховувати калорії.

4. "Розумні" термостати – пристрої, які дозволяють віддалено включати або вимикати системи опалення та охолодження в будинках, що може значно знизити витрати на електроенергію.

5. Доставка вантажів за допомогою БПЛА. Безпілотники доставляють замовлення швидше і безпечніше, ніж людина.

Пристрої не тільки стануть більш функціональними і безпечними (наприклад, сушарки, які будуть попереджати про перевищення допустимої норми накопичення ворсу), але також економніше по частині споживання електроенергії,

що дозволить заощадити на комунальних витратах. За оцінками Statista, в 2020 р кількість підключених пристроїв у всьому світі виросте майже до 31 млрд. штук.

1.2 Канали зв’язку

Існує три варіанти передавання даних в системи автоматизованих будинків – дротове, безпроводове та комбіноване з'єднання.

Канали передавання даних комп'ютерних мереж – це комплекс пристроїв для обміну потоками інформації в обох напрямках. Він складається з обладнання і ліній. Канали поділяють на провідні, безпроводові та комбіновані. Вони з'єднують прилади, що уловлюють сигнали, з інформаційними вузлами. Комбіноване з’єднання об’єднує одночасне використання дротових та безпроводових систем.

Конкретний тип каналу корпоративного зв'язку створюється з урахуванням параметрів мережі та вимог. Безпроводовими технологіями називається ціла група технологій, об'єднана одним фактором: відсутністю необхідності підключення проводів для передавання інформації на відстань від одного пристрою до іншого. На цих технологіях тримається весь інтернет речей, навіть мінімальна домашня мережа не зможе сьогодні без них функціонувати.

Для проводової передавання даних використовують металеві кабелі і оптоволокно. Звичні кабелі активно заміняють на оптико-волоконні мережі. Оптоволоконна структура дозволяє передавати сигнали в рази швидше і точніше. Це відбувається за рахунок наявності елементів намагніченого кремнію, які оточені матеріалом заломлюючим світло. За ним проходять світлові коливання, в яких трансформовані електромагнітні хвилі. Оптоволоконне спорядження захищено, тому така лінія надійна.

Кабельні канали зв'язку. Кабельні лінії зв'язку мають досить складну структуру. Кабель складається з провідників, укладених в кілька шарів ізоляції. У комп'ютерних мережах використовуються три типи кабелів: вита пара, коаксіальний кабель, оптоволоконний кабель [4].

Вита пара (twisted pair) – кабель зв'язку, який представляє собою виту пару мідних проводів (або кілька пар проводів), укладених в екрановану оболонку. Пари проводів скручуються між собою з метою зменшення наведень. Вита пара є досить перешкодостійкою. Існує два типи цього кабелю: неекранована кручена пара UTP і екранована кручена пара STP. Характерним для цього кабелю є простота монтажу. Даний кабель є найдешевшим і поширеним видом зв'язку, який знайшов широке застосування в найпоширеніших локальних мережах з архітектурою Ethernet, побудованих по топології типу "зірка". Кабель підключається до мережевих пристроїв за допомогою з'єднувача RJ45. Кабель використовується для передавання даних на швидкості 10 Мбіт/с і 100 Мбіт/с. Вита пара зазвичай використовується для зв'язку на відстань не більше кількох сотень метрів. До недоліків кабелю "вита пара" можна віднести можливість простого несанкціонованого підключення до сеті.

Коаксіальний кабель (coaxial cable) – це кабель з центральним мідним дротом, який оточений шаром ізолюючого матеріалу для того, щоб відокремити центральний провідник від зовнішнього провідного екрану (мідного обплетіння або шар алюмінієвої фольги). Зовнішній провідний екран кабелю покривається ізоляцією. Існує два типи коаксіального кабелю: тонкий коаксіальний кабель діаметром 5 мм і товстий коаксіальний кабель діаметром 10 мм. У товстого коаксіального кабелю загасання менше, ніж у тонкого. Вартість коаксіального кабелю перевищує номінальну вартість витої пари і виконання монтажу мережі складніше. Коаксіальний кабель застосовується, наприклад, в локальних мережах з архітектурою Ethernet, побудованих по топології типу "загальна шина". Коаксіальний кабель більш перешкодозахищений, ніж кручена пара і знижує власне випромінювання. Пропускна здатність – 50…100 Мбіт/с. Допустима довжина лінії зв'язку – кілька кілометрів. Несанкціоноване підключення до коаксіального кабелю складніше, ніж до витої пари [5].

Оптоволоконний кабель (fiber optic) – це оптичне волокно на кремнієвій або пластмасовій основі, укладену в матеріал з низьким коефіцієнтом заломлення

світла, який закритий зовнішньою оболонкою. Оптоволокно передає сигнали тільки в одному напрямку, тому кабель складається з двох волокон. На передавальному кінці оптоволоконного кабелю потрібно перетворення електричного сигналу в світловий, а на приймальному кінці зворотне перетворення.

Основна перевага цього типу кабелю – надзвичайно високий рівень перешкодозахищеності і відсутність випромінювання. Несанкціоноване підключення дуже складне. Швидкість передавання даних 3 Гбіт/с.

Основні недоліки оптоволоконного кабелю – це складність його монтажу, невелика механічна міцність і чутливість до іонізуючих випромінювань [6].

Зв'язок по безпроводових каналах забезпечується кількома різними способами:

- стільникові радіоканали, сформовані системою стаціонарних приладів і мобільної апаратури. Дальність не обмежена певним відстанню, оскільки сигнали обробляються всюди, де є апаратура;
- електромагнітні канали (Wi-Fi хвилі);
- супутниковий зв'язок, забезпечений системою антен, які вловлюють сигнали і транслюють їх до наземних об'єктів прийому;
- мульти- з радіусом в 60 км;
- канали радіомовлення з дальністю сигналу не більше 50 км;
- Bluetooth – передача даних на короткій відстані в безкоштовному режимі.

Класифікуються безпроводові технології за різними характеристиками. Способи передавання інформації використовуються різні: від радіохвиль до оптичних і інфрачервоних випромінювачів.

Найпоширеніші різновиди безпроводових технологій по території охоплення сигналу:

- WPAN. Персональні мережі, Bluetooth, ZigBee;
- WLAN. Локальні мережі, Wi–Fi;
- WMAN. Мережі міського масштабу, WiMAX;
- WWAN. Сама глобальна різновид мереж, GPS, EDGE, HSPA і інші.

Безпроводові технології як середовище передавання даних використовують навколишній простір замість кабелю. При цьому вони забезпечують користувачеві значну мобільність, завдяки широкому радіусу дії. Вони активно розширюються, стабільність сигналу підвищується, швидкість передавання даних зростає, витрати знижуються.

Потреба в розвитку таких технологій, завдяки появі мобільних і переносних пристроїв, не знижується [7].

1.3 Технології безпроводового зв'язку для побудови сенсорних мереж

1.3.1 Технологія Bluetooth

Для побудови розгалуженої сенсорної мережі необхідно обрати найбільш ефективну технологію зв'язку. На сьогоднішній день частіше використовуються безпроводові технології. На цих технологіях тримається весь інтернет речей, навіть мінімальна домашня мережа не зможе сьогодні без них функціонувати.

Bluetooth – це безпроводова технологія для обміну даними на невеликих відстанях і спроба мінімізувати використання проводів, стандарт заснований на використанні власних протоколів. Використовує діапазон 2,4…2,4835 ГГц, має радіус дії, в середньому, близько 10 метрів. Остання версія Bluetooth може працювати на відстань до 100 метрів на відкритій місцевості і при відсутності радіоперешкод. Bluetooth-пристрої не потребують встановлення або налаштування. Робота такого пристрою дуже проста і не вимагає налаштування апаратної конфігурації.

Використовуючи спеціальну радіочастоту для передавання даних, вона створює мережу короткого діапазону. Вона дуже безпечна і може одночасно підключати до восьми пристроїв (елементів електронного обладнання). Bluetooth-адаптер можна підключати до таких елементів, як комп'ютери, цифрові камери, мобільні телефони та факси. Більшість сучасних ноутбуків мають вбудовану підтримку Bluetooth. Для ПК можно підключається до USB порту Bluetooth-

адаптером. Використовуючи дану технологію, можливо передавати дані зі швидкістю 1 Мбіт/с.

Назва "Bluetooth" відображає скандинавське походження цієї технології. Він названий на честь дакінського вікінгу 10-го століття, короля Харальда Блетанда Синьозубого (переклад на англійську мову як "Bluetooth"). Він об'єднав і контролював Данію і Норвегію, звідси і об'єднання пристроїв через Bluetooth. Легенда свідчить, що він любив їсти чорницю – настільки, що його зуби мали колір плоду, що породжувало його ім'я.

Bluetooth 5.0 є продовженням Low Energy (LE). Його швидкість складає 48 Мбіт/с (вдвічі більше, ніж у попередній версії). Він може бути підключений на відстань до 300 метрів (в 4 рази більше ніж попередня версія). Діапазон ISM становить 2,4…2,485 ГГц. Не має зворотної сумісності зі своїми попередніми версіями. Це вимагає нового обладнання, яке повинно бути сучасним.

Швидкість Bluetooth 5 швидше, ніж Bluetooth 4. 2 з форматом 2 Мбіт/с, що вдвічі більше швидкості Bluetooth 4, приблизно 1 Мбіт/с, що дозволяє Bluetooth 5 відповідати одній з вимог IoT. Це все завдяки пропускної здатності 5 Мбіт з Bluetooth 5 в порівнянні з 2,1 Мбіт/с Bluetooth 4. Підтримка пристроїв IoT Bluetooth 5 легко задовольняє вимоги різних пристроїв IoT з хорошим діапазоном і високою швидкістю передавання даних, в той час як Bluetooth 4 не може задовольняти всі вимоги пристроїв через його низьку швидкість і малого робочого діапазону. Це означає, що пристрої IoT будуть добре працювати з Bluetooth 5 і правильно використовувати всі його функції в великих і складних проектах.

1.3.2 Технологія Wi–Fi

Wi-Fi – це стандартний протокол безпроводового зв'язку, який дозволяє підключити пристрої без кабелів. Wi–Fi використовується для доступу до Інтернету на портативних пристроях, таких як смартфони, планшети або ноутбуки, Wi–Fi

використовується для підключення до маршрутизатора або іншої точки доступу, яка надає доступ до Інтернету.

Це технологія радіопередавання, яка побудована на наборі стандартів для забезпечення високої швидкості та безпеки зв'язку між широким спектром цифрових пристроїв, точками доступу та обладнанням. Це дає змогу пристроям, що підтримують Wi-Fi, отримувати доступ до Інтернету без необхідності використання обмежувальних дротів.

Термін "Wi-Fi" є маркетинговою назвою, що означає "безпроводову вірність" (wireless fidelity). Пишеться як wifi, Wifi, WIFI або WiFi, але жоден офіційно не затверджений Wi-Fi Alliance. Також використовується як синонім слова "безпроводовий" (wireless). Може працювати на коротких і великих відстанях, бути заблокований і захищений, або відкритий і вільний. Це неймовірно багатофункціональний і досить простий у використанні спосіб, який можна знайти у найпопулярніших споживчих пристроях. Wi-Fi є розповсюдженим і надзвичайно важливим для керування сучасним зв'язком.

Wi-Fi з самої появи став широко використовуватися для створення локальних мереж в будинках і офісах. Процес налаштування локальної мережі значно полегшується, якщо відпадає необхідність підключення LAN кабелів до системи. Wi-Fi використовує радіохвилі для передавання інформації на певних частотах, найчастіше на частотах 2,4 ГГц і 5 ГГц, хоча використовуються багато інших. Кожен діапазон частот має безліч каналів, на яких можуть працювати безпроводові пристрої, що допомагає поширювати навантаження, так що окремі пристрої не бачать своїх сигналів переповненими та не перериваються іншим трафіком, як це трапляється в зайнятих мережах.

Відстань, на якому може працювати Wi-Fi, охоплює приблизно 300 метрів від безпроводового вузла мережі на відкритій місцевості і 100 метрів в умовах приміщень. Потужність антени та частотна трансляція також можуть впливати на ефективний діапазон мережі. Більш високі частоти, такі як 5 ГГц і 60 ГГц, мають набагато коротші ефективні діапазони, ніж 2,4 ГГц.

1.3.3 Технологія Long-Range

LoRa (Long Range) – це технологія зв'язку в глобальній мережі з низьким енергоспоживанням. LoRaWAN – протокол рівня управління доступом до середовища (MAC), який побудований поверх фізичного рівня, і системна архітектура малопотужних глобальних мереж, а LoRa визначає фізичний рівень системи, топологія мережі на рис. 1.3. Протокол LoRaWAN визначає мережеву архітектуру, яка працює в неліцензованій смузі нижче 1000 МГц. LoRaWAN використовує шифрування AES-128 для забезпечення безпеки. Найчастіше використовуються три смуги частот: 433 МГц для Азії, 868 МГц для Європи і 915 МГц для Північної Америки [8].

Дана технологія забезпечує значну дальність зв'язку, в порівнянні з існуючими конкурентами. У LoRa модуляція заснована на технології розширення спектру SSM і варіації лінійної частотної модуляції CSS з інтегрованою прямою корекцією помилок FEC (скороч. Forward Error Correction). LoRa визначає PHY– рівень системи (фізичний).

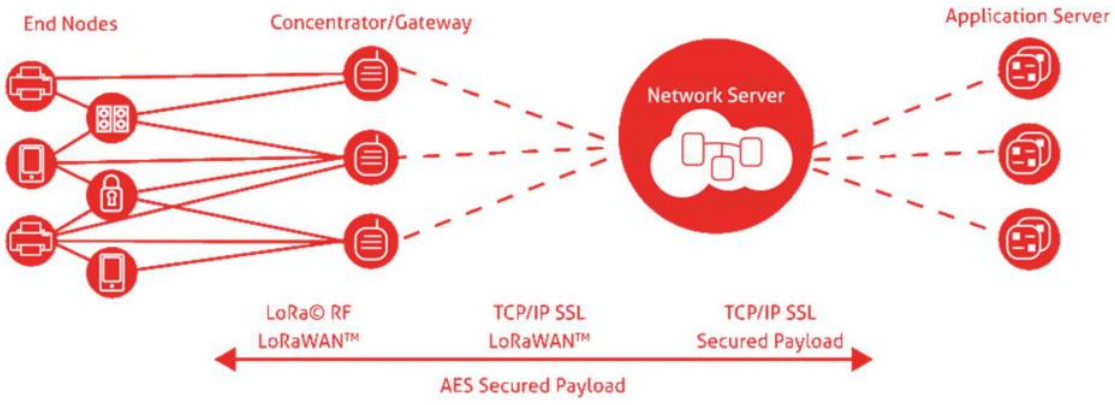

Рисунок 1.3 – Архітектура мережі LoRaWAN

LoRa пропонує привабливе поєднання великої дальності, низького енергоспоживання, глибокого покриття всередині приміщень і безпечної

передавання даних. LoRa працює в діапазоні частот <1 ГГц. Використовує технологію розширеного спектру, так що сусідні передавачі з меншою ймовірністю будуть заважати один одному, що збільшує пропускну здатність кожного шлюзу. Зв'язок з розширеним спектром також забезпечує "посилення кодування" в порівнянні з вузько лінійним зв'язком. Це призводить до каналу зв'язку, який може підтримувати зв'язок на великі відстані. Швидкості передавання даних LoRa варіюються від 0,3 Кбіт/с до 50 Кбіт/с і можуть підтримувати діапазон до 15 км.

LoRa дозволила демодулировати сигнали на рівні 20 дБ нижче рівня шумів, в той час як більшість систем з частотної маніпуляцією FSK працюють тільки з сигналами рівня не нижче 8…10 дБ рівня шумів.

LoRaWAN – це відкритий протокол для мереж, в яких:

- висока ємність (до 1 000 000 пристроїв в одній мережі);
- великий радіус дії (до 10…15 км на відкритій місцевості);
- низьке енергоспоживання.

LoRaWAN є протоколом (MAC-рівень) для мереж з високою ємністю, великим радіусом дії і низьким енергоспоживанням, встановленим організацією LoRa Alliance для мереж LPWAN.

1.3.4 Мережі мобільного зв'язку

Перше покоління мобільного зв’язку – 1G. У 80–х роках минулого століття з'явилися новаторські мережеві технології: поєднання NMT і TACS в Європі і AMPS в США. Декілька поколінь послуг мобільного зв'язку існували і раніше, трійка NMT, TACS і AMPS вважається першим поколінням безпроводової мережі, тому, що саме ці технології дозволили мобільним телефонам стати масовим продуктом. 1G – це чисто аналогові системи, придумані і спроектовані виключно для здійснення голосових викликів і деяких інших можливостей. Вже існували модеми, однак через те, що безпроводовий зв'язок більш схильний до спотворень і шумів, ніж звичайний дротовий зв'язок, швидкість передавання даних була дуже

низькою. Вартість хвилини розмови була настільки високою, що мобільний зв'язок могла дозволити собі тільки матеріально забезпечена людина [9].

Друге покоління мобільного зв’язку – 2G. На початку 1990–х років спостерігається підйом перших цифрових стільникових мереж, які мали ряд переваг в порівнянні з аналоговими системами, до яких можна віднести покращення якості звуку, підвищення продуктивності, більшу захищеність та GSM почав свій розвиток в Європі.

Друге покоління безпроводової мережі 2G вже мало підтримку передавання коротких текстових повідомлень (SMS), а також технологію передавання даних (CSD) [10], яка дозволяла передавати дані в цифровому вигляді. Все це дозволило збільшити швидкість передавання даних до 14,4 Кбіт/с, що можна порівняти зі швидкістю стаціонарних модемів в середині 1990–х років [9].

У 1997 році з'явився сервіс GPRS. З появою GPRS існуючі GSM–мережі почали підтримувати безперервну передачу даних. Можна було здійснювати передачу даних тільки тоді, коли це необхідно. GPRS міг працювати з більшою, ніж CSD, швидкістю – теоретично до 171,2 Кбіт/с, а оператори отримали можливість тарифікувати трафік, а не час на лінії.

Коли технологія GPRS вже була на ринку, Міжнародний союз електрозв'язку (ITU) опублікував новий стандарт – IMT-2000 що підтверджує специфікацію "справжнього" 3G. Ключовим моментом, в цій історії, було забезпечення швидкості передавання даних до 2 Мбіт/с для стаціонарних терміналів і 384 кбіт/с для безпроводових мереж, що було не під силу GPRS.

Нові стандарти 3G закликали забезпечити легку міграцію до безпроводових мереж другого покоління. Для здійснення даного заходу, був розроблений стандарт EDGE. За допомогою мобільного телефону, що підтримує EDGE, абоненти могли отримувати швидкість, в два рази перевищує GPRS.

Через деякий час, безпроводові мережі CDMA2000 отримали оновлення 1x EV–DO Rel.0. Оновлення дозволило збільшити вхідну швидкість до 2,4 Мбіт/с і вихідну швидкість до 153 кбіт/с.

Четверте покоління мобільного зв’язку – 4G, fourth generation або LTE (Long Term Evolution). Найпоширеніша в світі технологія безпроводової передавання даних. Стандарт виник в минулому десятиріччі, робота над його створенням розпочалася ще в 2004 році [11].

Формальною датою появи 4G став 2008 рік, коли Міжнародний союз електрозв’язку встановив для нього стандарти. Згідно з цими стандартами, швидкість зв’язку для рухомих об’єктів (смартфони, планшети) повинна становити не менше 100 Мбіт/с, а для статичних (точки доступу) – не менше 1 Гбіт/с. Перші комерційні запуски 4G–мереж почалися в 2009–2010 роках.

Специфікація встановлює швидкість вхідних даних в 1 Гбіт/с для стаціонарних терміналів і 100 Мбіт/с для мобільних апаратів.

Як показала практика, WiMAX і LTE зазнають невдачі в швидкості передавання даних. Теоретично значення швидкості знаходяться на рівні 40 Мбіт/с і 100 Мбіт/с, а практично, реальні швидкості комерційних мереж не перевищують 4 Мбіт с і 30 Мбіт/с відповідно. Даний факт не задовольняє високим вимогам IMT–Advanced. Оновлення стандартів до WiMAX Release 2 і LTE–Advanced обіцяє підтримку цих швидкостей, проте робота досі не завершена і реальних мереж, які їх використовують, як і раніше не існує [12].

Щоб розширити можливості LTE, запропоновано мережу п'ятого покоління (5G), яка зараз знаходиться в стадії дослідження та обговорення [13].

Стандарт мобільного зв'язку п'ятого покоління (5G) – це новий етап розвитку технологій, який покликаний розширити можливості доступу в Інтернет через мережі радіодоступу.

Завдання, які покликана вирішити технологія 5G:

- зростання мобільного трафіку;
- збільшення числа пристроїв, що підключаються до мережі;
- скорочення затримок для реалізації нових послуг;
- нестача частотного спектра.

Послуги в мережах 5G:

- надширокосмугові мобільний зв'язок (Extreme Mobile Broadband, eMBB) - реалізація ультрашірокополосной зв'язку з метою передавання "важкого" контенту;
- масова межмашинного зв'язок (Massive Machine-Type Communications, mMTC) - підтримка Інтернету речей (ультраузкополосная зв'язок);
- наднадійна межмашинного зв'язок з низькими затримками (Ultra-Reliable Low Latency communication, URLLC) – забезпечення особливого класу послуг з дуже низькими затримками.

В майбутньому до мережі буде підключено набагато більше пристроїв, більшість з яких будуть працювати за принципом "завжди онлайн". При цьому дуже важливим параметром буде їх низьке енергоспоживання.

Вимоги до мереж 5G:

- пропускна здатність мережі до 20 Гбіт/сек по лінії "вниз" (тобто до абонента); і до 10 Гбіт/с у зворотному напрямку;
- підтримка одночасного підключення до 1 млн. Пристроїв/км2;
- скорочення тривалості затримки на радіоінтерфейсу до 0,5 мс (для сервісів наднадійні міжмашинна зв'язку URLLC) і до 4 мс (для сервісів надширокосмугові мобільного зв'язку eMBB).

1.3.5 Технологія NB-IoT

Інноваційною технологією є рішення вузькосмугового Інтернету речей в мережі мобільного зв'язку (Narrow-Band IoT або NB-IoT). NB-IoT розроблена групою 3GPP на базі існуючих стандартів мобільного зв'язку. Існує два основні варіанти цієї специфікації: один випущений Nokia, Ericsson і Intel, а інший – Vodafone & Huawei. Це безпроводова вузькосмугова мережа – різновид глобальних мереж з низьким енергоспоживанням, яка в першу чергу призначена для додатків M2M. Стандарт NB-IoT відкриє компаніям, що спеціалізуються на наданні телекомунікаційних послуг, широкий спектр нових можливостей. Зокрема, істотно

збільшить прибутковість операторів від одного абонента (Average revenue per user, ARPU).

Фахівці вважають, що технологія NB-IoT отримає популярність серед операторів, тому що її обслуговування і експлуатація обійдеться їм дешевше, ніж у передових на сьогоднішній день мереж LTE і GSM. Це обумовлено її характеристиками. Стандарт NB-IoT є двосторонній зв'язок, що діє в частотному каналі шириною 200 кГц. Для того, щоб запустити мережу в експлуатацію, оператору всього лише необхідно встановити на базовій станції спеціальне програмне забезпечення. Це актуально, якщо розгортати IoT-мережу вже на існуючих частотах. Швидкість передавання даних в NB-IoT досягає 200 кбіт/с, що є достатнім для пристроїв, що періодично передають однотипні дані невеликого обсягу.

У свою чергу розробники обіцяють, що термін служби елемента живлення устаткування NB-IoT без підзарядки буде досягати 10 років. Очікується, що ціна терміналу NB-IoT складе $ 5.

Наступною найважливіших особливостей технології NB-IoT є можливість підключати до одної базової станції до 100 тисяч пристроїв NB-IoT. Це дозволяє отримати додаткову комерційну вигоду на основі застосування аналізу IoT-даних методами великих даних (Big Data). В рамках співпраці із суміжними галузями оператори, на додаток до продажу послуг зв'язку, отримують можливість продавати аналітичні дані третім особам.

Такі переваги стандарту NB-IoT дозволяють значно збільшити зону покриття, забезпечивши зв'язок у важкодоступних місцях і регіонах.

3GPP продумує модель функціонування мережі. Консорціум пропонує три варіанти розгортання NB-IoT мережі. Перший – це NB-IoT Guard Band, тобто для Narrowband IoT буде виділений окремий частотний спектр. Другий – це In Band, тобто технологія буде розміщена в захисному інтервалу частот мереж LTE. Третій – отримав назву Stand Alone. Відповідно до його концепції, NB-IoT і LTE працюють в одному частотному діапазоні. Таким чином, мережу NB-IoT можна розгорнути в

частотних діапазонах, в яких в даний час функціонує стандарт GSM, або в "захисних" інтервалах між мережами GSM і LTE.

1.4 Порівняння радіотехнологій IoT

Завдяки розвитку технологій, концепція IoT завойовує все більше місця в різних галузях: побутові прилади, гаджети, виробництво (IIoT), медицина, транспорт, логістика, системи безпеки, клімат-контроль і багато інших.

У "розумному будинку" поряд з комп'ютерами, мультимедійними системами та смарт-телевізорами буде використовуватися безліч пристроїв з локальним з'єднанням малого радіусу дії, включаючи пристрої для контролю за температурою, освітленням, замками і системою сигналізації. Переваги технологій "розумного будинку" будуть реалізовуватися в сферах опалення та захисту комерційних будівель, водовідведення, вуличного освітлення, енергозбереження та оптимізації вуличного руху за допомогою адаптивного управління обмеженням максимальної швидкості і роботи світлофорів [14].

Комунікація є однією з найважливіших частин будь-якого проекту IoT. Хоча існує безліч протоколів зв'язку, кожному з них не вистачає тих чи інших характеристик, що робить їх "не зовсім підходящими" для додатків IoT. Основними проблемами є енергоспоживання, радіус покриття і пропускна здатність. Порівняння технологій за радіусом дії та діапазоном робочих частот на рис. 1.4 та рис. 1.5.

Більшість комунікаційних радіотехнологій, таких як Zigbee, BLE, WiFi та інші, мають малу дальність дії, а інші, такі як 3G і LTE, споживають багато енергії, і дальність дії їх роботи не може бути гарантована, особливо в країнах, що розвиваються. Незважаючи на те, що ці протоколи і режими зв'язку працюють для певних проектів, вони мають велике обмеження, наприклад труднощі в розгортанні рішень IoT в областях без стільникового зв'язку (GPRS, EDGE, 3G, LTE/4G) і необхідність в придбанні дорогих ліцензій. Параметри технологій на табл. 1.1.

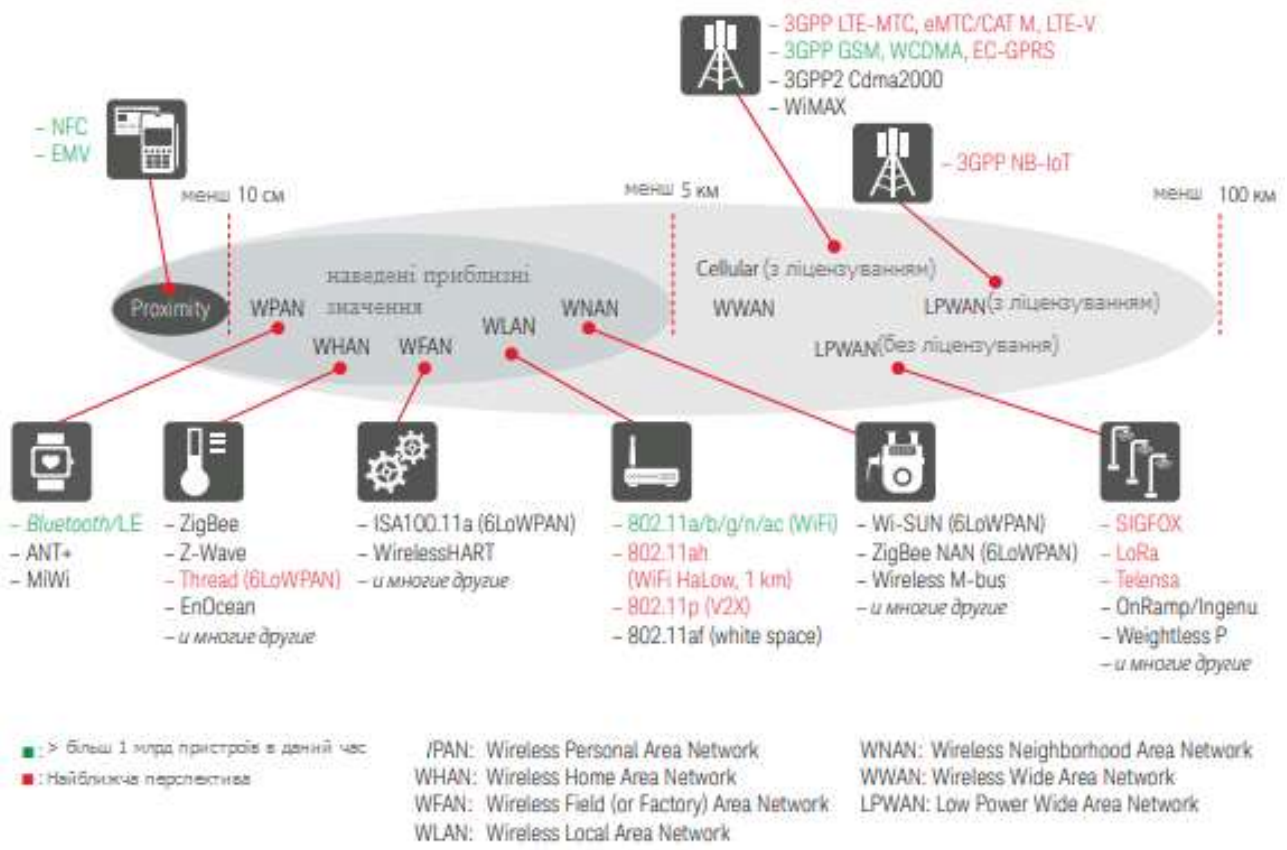

Рисунок 1.4 – Технології "розумного" будинку по радіусу дії

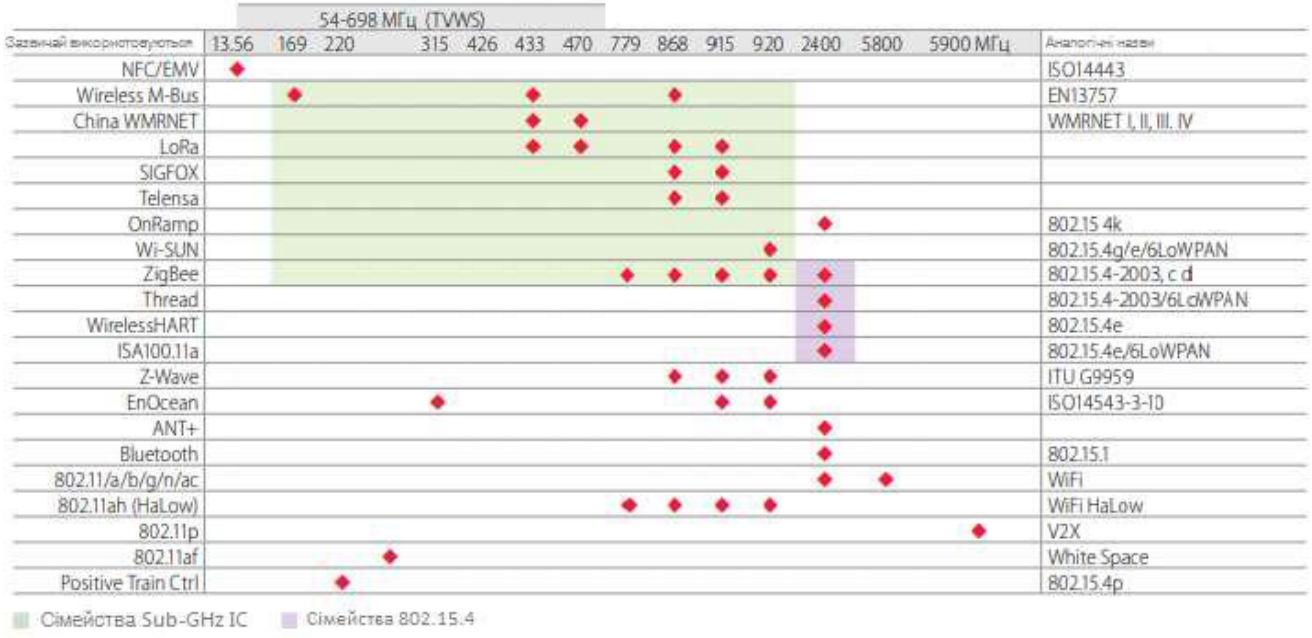

Рисунок 1.5 – Діапазони робочих частот технологій, відмінних від технологій мобільних пристроїв

Таблиця 1.1 – Параметри сучасних радіотехнологій для IoT.

Технологія	Стандарт зв'язку	Частота	Швидкість передавання даних	Топологія мережі	Кільк. учас. мережі	Дальність	Потуж-ність	Спосіб застосування
LoRaWan	Власний	433 МГц, 868 МГц, 915 МГц.	RX 290 бит/с TX 50 Кбит/с	Зірка	Дуже велике	5-15 Км	Середня	Мобільний/ Локальний
LTE-M	3GPP	700 МГц… 2,2 ГГц. 452,5… 467,5 МГц.	1 Мбит/с	Зірка	Дуже велике	5 км	Висока	Мобільний/ Локальний
Sigfox	Власний	868 МГц, 915 МГц, 921 МГц.	0,1 Кбит/с	Зірка	Дуже велике	10-50 км	Середня	Мобільний/ Локальний
NB-IoT	3GPP	700 МГц… 2,2 ГГц, 452,5… 467,5 МГц.	~200 Кбитс/с	Зірка	Дуже велике	5 км	Висока	Мобільний/ Локальний
NFC	ISO 13157	13,56 МГц.	424 Кбит/с	P2P	2	1…10 см	Низька	Локальний
BLE	Bluetooth SIG	2,4 ГГц.	125Кбит/с… 2Мбит/с	P2P, broad	20	40…1000 м	Низька	Локальний
Wi-Fi	802.11	2,4/5,0 ГГц.	до 150 Мбит/с	Звезда	100	40…100 м	Середня	Локальний
Z-Wave	Власний	868…926 МГц.	100 Кбит/с	Mesh	232	40…100 м	Середня	Локальний
ZigBee	IEEE 802.15.4	2,4 Г	250 Кбит/с	Mesh	250+	40…100 м	Середня	Локальний

Таким чином, з огляду на майбутнє IoT і підключення всіх видів "речей", розташованих у всіх місцях, виникла потреба в комунікаційному середовищі, спеціально розробленому для IoT, яке підтримує його вимоги, зокрема, щодо малої потужності і значно великої дальності, дешевого, безпечного і простого в розгортанні.

Розглянемо детально характеристики двох більш схожих сучасних LPWAN-стандартів – LoRaWAN і NB-IoT.

LoRaWAN – це LPWAN система з відкритою архітектурою, розроблена і стандартизована некомерційною асоціацією компаній LoRa Alliance, яка налічує понад 500 учасників. LoRa це технологія модуляції, що застосовується на

фізичному рівні, що дозволяє здійснювати далекі енергоефективні передавання даних з використанням CSS (Chirp Spread Spectrum) модуляції, яка поширює вузькосмугові сигнали по розширеному каналу, ніж забезпечує високу стійкість і низькі рівні відношення сигнал/шум.

NB-IoT зі свого боку, працює в ліцензованому діапазоні і подібно LTE використовує багатостанційний доступ з частотним поділом каналів (FDMA) в висхідній лінії зв'язку, ортогональний FDMA (OFDMA) в низхідній лінії зв'язку і QPSK (Quadrature Phase Shift Keying) модуляцію.

Обидві технології можуть конкурувати в якості обслуговування, як показано на табл. 1.2 та рис. 1.6.

І LoRaWAN, і NB-IoT пристрої споживають менше енергії, коли переходять в сплячий режим. Але під час роботи в якості синхронного протоколу NB-IoT споживає значно більше енергії, ніж LoRaWAN, який є асинхронним протоколом, і при вимірах з однаковою пропускною спроможністю NB-IoT споживає більш високий піковий струм, необхідний для модуляції OFDM/FDMA.

Характеристики обох технологій важливі при реалізації багатьох практичних рішень, які вимагають високої проникаючої здатності всередині приміщень і роки автономної роботи.

Фактором, що впливає на відносну вартість і продуктивність LoRaWAN і NB-IoT, є краща проникаюча здатність LoRaWAN в приміщеннях. Максимальна втрата зв'язку (MCL) для висхідній і низхідній лінії LoRaWAN становить 165 дБ; значення MCL для NB-IoT може становити від 145 дБ до 169 дБ для висхідній лінії зв'язку і 151 дБ для низхідній лінії зв'язку в залежності від класу пристрою.

Більш низькі показники енергетичного потенціалу лінії зв'язку у NB-IoT призводять до зменшення терміну служби батареї. Для охоплення Амстердама, площа становить 219 кв. км., треба було встановити 10 базових станцій мережі LoRaWAN.

Вартість кожної станції склала лише $ 1,2 тис.

Таблиця 1.2 –Параметри LoRaWAN і NB-IoT

Параметри	LoRaWAN	NB-IoT
Смуга частот	125 кГц	180 кГц
MCL	165 дБ	164 дБ
Термін служби батареї	15+ лет	10+ лет
Піковий струм	32 мА	120 мА
Ток в сплячому режимі	1 мкА	5 мкА
Пропускна здатність каналу	50 Кб/с	60 Кб/с
Затримка	Залежить від класу	Меньше 10 с
Безпека	AES 128 бит	3GPP 128-256 бит
Геолокація	Так, метод TDOA	Так, метод 3GPP Rel 14
Ефективність витрат	Висока	Середня

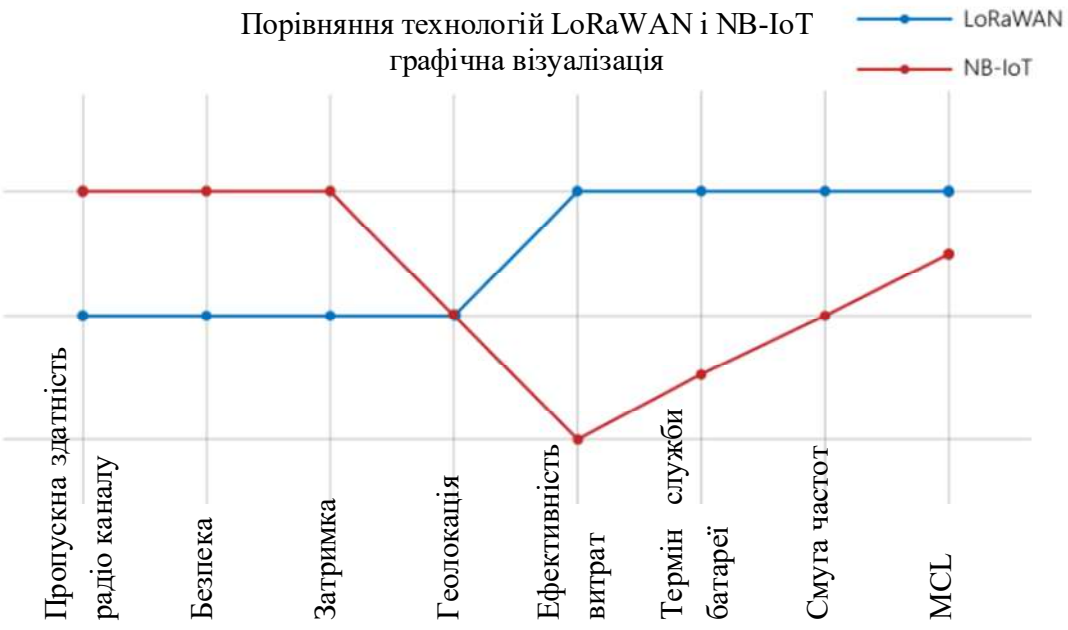

Рисунок 1.6 – Графічна візуалізація порівняння технологій

Корпоративним клієнтам, які бажають розгорнути гібридну мережу з використанням як приватної, так і загальнодоступною мережевої інфраструктури, найкраще використовувати LoRaWAN, таблиця 1.3. З приватними LoRaWAN

мережами підприємства не обмежені діловими і фінансовими причинами при передавання даних. При можливості, доступ до корпоративної мережі може бути доповнений загальнодоступною мережею LoRaWAN.

Підключення NB-IoT в даний час пропонується в зонах, де вже є покриття стільникового зв'язку, але в порівнянні з LoRaWAN витрати на розгортання вищі, оскільки розгортання приватної мережі потребують придбання або оренди спектра РЧ у операторів мереж.

Таблиця 1.3 – Характеристики LoRaWAN і NB-IoT

Характе-ристики	LoRaWAN	NB-IoT
Простота розгортання	Не є стільниковим стандартом. Для роботи не потрібно отримання ліцензій на використання частот.	Стандарт стільникового зв'язку, тому для роботи базових станцій необхідно отримати ліцензію.
Синхронізація	Асинхронна відправка даних тільки тоді, коли ці дані є. Поки пристрій нічого не передає, він "спить", економлячи енергію. Відправка даних за розкладом або поза залежністю від часу.	Пристрої повинні "прокидатися" і синхронізуватися з мережею.
Час автономної роботи	В архітектурі LoRa синхронізація з мережею не потрібна. В асинхронних діапазонах, тільки природа кінцевих додатків визначає, як довго пристрій може "спати". Автономність LoRaWAN-пристроїв в три-п'ять разів вище, ніж у девайсів, які працюють в інших LPWAN.	Пристрої синхронізуються з мережею відносно часто. Це витрачає батарею.
Швидкість передавання даних	Середня швидкість передавання даних від 300 біт/с до 50 Кбіт/с. Для більшості випадків використання пристроїв, достатньо швидкості передавання даних в 11 Кбіт/с.	Середня швидкість передавання даних 200 Кбіт/с. NB-IoT – це більш ефективний протокол IoT для "швидких" додатків.
Пропускна смуга	125 кГц	180 кГц

Характе-ристики	LoRaWAN	NB-IoT
Покриття мережі	LoRaWAN не покладається на мобільні дані і її покриття залишається відносно стійким незалежно від умов місцевості.	NB-IoT найкраще працює в складних міських районах. Продуктивність мережі буде надлишковою в приміських або сільських районах.
Випадки застосування	Підходить для додатків і пристроїв, які невибагливі до швидкостей передавання даних і кількості даних, що відправляються. Пристрої повинні забезпечувати тривалий термін служби батареї при мінімальних витратах на технічне обслуговування.	Підходить для додатків, вимогливим до часу затримки (воно повинно бути мінімальним) і регулярного прийому і відправлення повідомлень.
Сценарії розгортання	Використовується операторами, які працюють в сфері мобільного зв'язку, та приватними підприємствами в їх власних мережах, наприклад, для реалізації проектів "розумна фабрика", і одночасно використовувати громадську мережу для роботи поза об'єктом.	NB-IoT можуть розвивати тільки мобільні компанії з ім'ям. Використання NB-IoT обмежена тільки публічними моделями.
Коефіцієнт витрат	Загальна вартість модулів LoRaWAN становить приблизно в $ 8…$ 10.	Загальна вартість модулів становить $ 20…$ 40.
Екосистема	Послуги зв'язку доступні в 40 країнах світу і 250 містах. LoRaWAN вже прийнятий в якості стандарту мережі IoT в багатьох країнах. В LoRa Alliance входить більше 500 компаній.	За даними GSMA, в квітні 2017 року світі тестувалися 40 NB-IoT мереж і тільки чотири мережі почали повноцінну роботу.

Мережі LoRaWAN і NB-IoT почали розгортатися відносно недавно, але вже спостерігається їх швидке зростання в глобальному масштабі. LoRaWAN і NB-IoT масово застосовується у IoT внаслідок переваг: більш низькі витрати на пристрої, мережева інфраструктура та доступ до мережі; висока проникаюча здатність

всередині будівлі; і низьке енергоспоживання. LoRaWAN в найближчій перспективі має явну перевагу перед NB-IoT, зі своєю розвиненою системою постачальників, сертифікованими IoT пристроями та комплексними рішеннями, які вже сьогодні готові до впровадження.

1.5 Сенсори контролю параметрів критично важливих систем

Успішне просування на світовий ринок промислового Інтернету речей пов'язано з швидким розвитком безпроводових сенсорних мереж, які об'єднують безліч промислових сенсорів в єдину систему. Промислові мережі відрізняються від звичайних комерційних систем, перш за все, високою надійністю і безпекою.

Систему IoT-моніторингу вживають для вирішення різного роду проблем. Найчастіше інститути впроваджують безпроводову сенсорну мережу через наявність транспорту або оранжерей. Різкі зміни погодних умов, техногенні катастрофи, вірусні та бактеріальні захворювання тропічних і субтропічний рослин привели до необхідності розробки і створення сенсорів для експрес-діагностики стану рослин в реальному часі і визначення впливу на рослинний покрив кліматичних факторів, вірусних і бактеріальних навантажень, а також стресових факторів природного і техногенного походження. Отримання оперативної і об'єктивної інформації про стан рослин дозволяє своєчасно виробити заходи щодо захисту рослин. Це дасть змогу зменшити матеріальні витрати по догляду, зберегти зелені насадження від можливих втрат, а також сприяти захисту від вірусної і бактерійної інфекції.

У найближчі роки безліч найрізноманітніших датчиків в додатках IoT повинні будуть виходити в ефір лише періодично і тільки для того, щоб відправити накопичену інформацію про витрати води, газу, електрики, температуру повітря, вологість ґрунту, вміст шкідливих домішок і т. д. Такі інтелектуальні датчики повинні володіти специфічними властивостями, з яких, перш за все, необхідно відзначити мінімальне енергоспоживання і вартість. Ці пристрої з автономним

батарейним харчуванням повинні забезпечувати роботу без заміни батареї протягом декількох років. В англомовній літературі даний тип пристроїв, що забезпечує мале енергоспоживання і широке територіальне охоплення, отримав назву LPWA – low power wide area. Технології ліцензованих діапазонів IoT, призначені для пристроїв LPWA eC-GSM-IoT, eMTC і NB-IoT.

Типова безпроводова сенсорна мережа, рис. 1.7, яка на нижньому рівні включає безпроводові інтелектуальні сенсори, координатор і концентратор. Дані безпроводової мережі надходять в мобільну безпілотну платформу, а далі в віддалений комп'ютер, або обробляються хмарними технологіями [15].

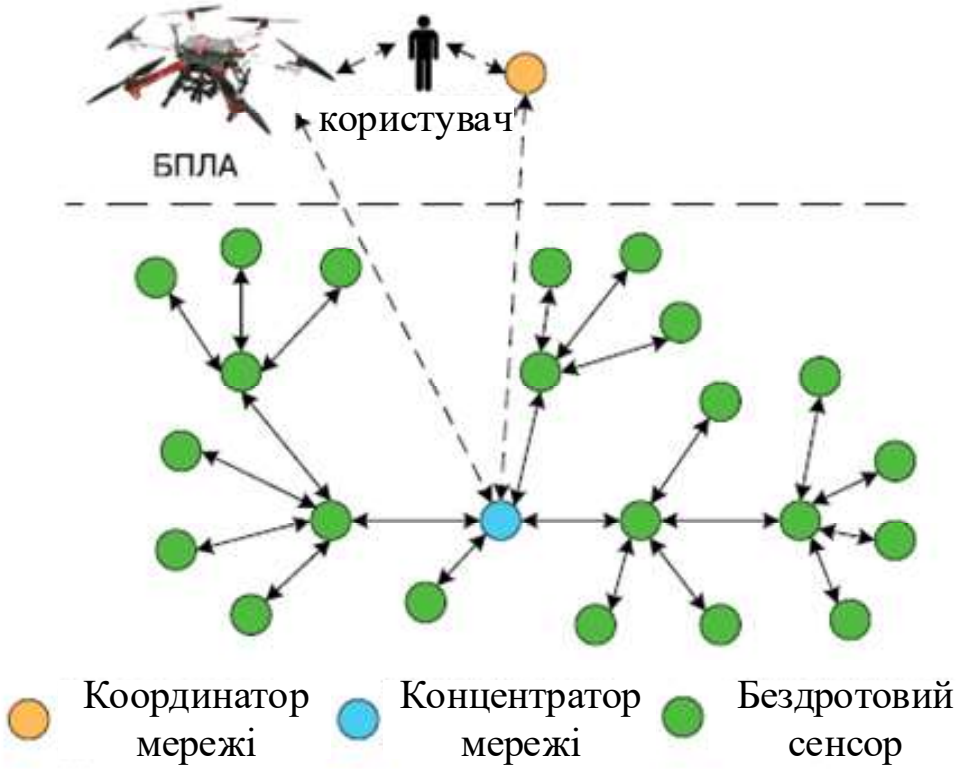

Рисунок 1.7 – Структурна організація безпроводових сенсорних мереж

До інтелектуальних безпроводових сенсорів ставлять такі вимоги:

- можливість роботи в польових умовах експлуатації;
- тривалий час роботи без заміни або підзарядки акумулятора;
- невисока вартість;

- невеликі маса і габарити;
- можливість самокалібрування основних вузлів;
- висока надійність;
- оптимальне співвідношення дальності передавання даних до споживаної енергії;
- можливість заміни або підзарядки акумулятора в польових умовах.

При віддаленому від ядра вимірювальної системи сенсорі, включеному в міст, слід використовувати вимірювальні підсилювачі, які дозволяють послабити рівень перешкод і шумів в лініях зв'язку.

Приклад сенсору контролю параметрів критично важливих систем: електрохімічний газовий сенсор. Популярність електрохімічних газових сенсорів можна пояснити високою лінійністю, низьким споживанням і високою роздільною здатністю. Більш того, після калібрування ці сенсори демонструють високу селективність, повторюваність і точність. Важливе промислове застосування електрохімічних газових сенсорів – це виявлення токсичних газів і, як наслідок, підтримку безпечних умов роботи для співробітників гірничодобувної, хімічної, біогазової, харчової та фармацевтичної промисловості [16].

Незважаючи на постійне вдосконалення технології електрохімічних сенсорів, вони, як правило, мають обмежений термін служби – зазвичай від шести місяців до одного року. Виробники цих сенсорів вказують на те, що їх чутливість може погіршуватися на 20% протягом року. Крім того, в ряді випадків при наявності суміші різних газів сенсори можуть мати невисоку селективність. Параметри сенсорів залежать від температури і вологості навколишнього середовища.

Технічні проблеми, на які повинні звернути увагу розробники, полягають у наступному:

- в забезпеченні необхідної повторюваності за рахунок калібрування сенсорів в процесі виробництва;
- в забезпеченні необхідної електромагнітної сумісності;
- у збільшенні терміну служби;

- в застосуванні автоматичної самодіагностики працездатності сенсорів.

Складність вимірювального каналу, який включає АЦП, підсилювачі та інші вузли, призводить до збільшення споживання, розмірів друкованої плати і ускладненні закінченого виробу в цілому.

Незважаючи на велику увагу, яку приділяє безпеці сенсорних вузлів при прийомі і передавання даних, не слід нехтувати забезпеченням безпеки сенсорних вузлів. Часто атакам піддаються кінцеві точки мережі або сенсорні вузли. Такі вузли потребують підвищеного захисту. Тому пристрої захисту в промислових системах Інтернету речей, як правило, вбудовуються в кінцеві сенсорні вузли, що робить їх незалежними від ступеня захисту сенсорних мереж в цілому. Особливо це важливо для віддалених від шлюзу сенсорних вузлів.

Сенсорні вузли повинні бути надійно захищені від кібератак. Повинний бути гарантований захист сенсорних вузлів і даних, які в них зберігаються, вхідних і вихідних даних, одержаних по каналах зв'язку, повинна бути передбачена можливість виявлення спроб таких кібератак з подальшим інформуванням користувача. Всі ці можливості повинні бути забезпечені на ранній стадії проектування сенсорних мереж. Не існує універсального підходу до вирішення проблеми захисту сенсорних мереж і її вузлів від різного роду атак. Однак розроблені загальні підходи дозволяють використовувати ті чи інші методи в кожному конкретному випадку для зниження уразливості мережевих рішень для конкретного застосування.

Про можливість відновлення мережі після компрометації. В якості аналогії можна вказати на застосовуваний в медицині метод стерилізації інструментів після їх інфікування, що дозволяє повторно їх використовувати. Однак, якщо інфікована сенсорна мережа, то така можливість відновлення початкового стану мережі, як інструментів в медицині, на жаль, відсутня. Наприклад, інфікований вірусом процесор мережевого вузла може вести себе по-різному, і передбачити його поведінку неможливо. Є тільки один шлях очистити систему від зараженого вірусом ПО. Необхідно переписати дані з незалежної пам'яті у зовнішній

накопичувач, перевірити їх на предмет відсутності вірусу і переписати їх назад у вбудовану в вузол пам'ять, якщо вірус не був виявлений. Однак слід звернути увагу на те, що часто мережеві вузли спроектовані так, що виконати таку операцію неможливо. Єдино, що можна зробити, це використовувати в вузлах сенсорної мережі незалежну пам'ять, призначену тільки для читання (пам'ять типу ROM), з електромеханічним мультиплексором. Це унеможливлює інфікування такої пам'яті за допомогою віддаленого хакерського пристрою. Таку можливість мають користувачі, які мають безпосередній доступ до віддалених мережевих вузлів. Можна модифікувати систему брандмауера, в цьому випадку в ROM-пам'яті дані оновлюються через електромеханічний мультиплексор.

1.6 Принципи побудови систем збору та контролю даних

Поява процесорів з низьким енергоспоживанням, інтелектуальних безпроводових мереж і сенсорів в поєднанні з Big Data Analytics (засобами обробки великих даних) привело до швидкого розвитку IIoT. Нова технологія збору і обробки даних дозволяє розміщувати безліч сенсорів в будь-якій точці промислового виробництва: і не тільки там, де є відповідна інфраструктура, а й там, де є цінна інформація, яку треба зібрати і обробити для успішної взаємодії Інтернету речей.

Концепція оснащення машин, насосів, трубопроводів і залізничних вагонів та іншого обладнання сенсорами не нова для промисловості. Спеціалізовані сенсори і мережі давно застосовуються в різних галузях промисловості – від нафтопереробних заводів до виробничих ліній. У недавньому минулому ці системи працювали як автономні мережі, підтримуючи високий рівень надійності і безпеки виробничого процесу. Такі ж високі вимоги до надійності і безпеки пред'являються до технологій промислового Інтернету речей, зокрема, до об'єднаних в мережу численних сенсорів, забезпечуючи їх надійну роботу в жорстких умовах експлуатації, типових для промислового застосування

Безпроводові мережі в системах Інтернету речей можуть використовувати ліцензовані частотні діапазони в рамках стільникового зв'язку. Але в такій мережі застосовуються пристрої з великим енергоспоживанням. У більшості випадків промислові системи Інтернету речей цілком можуть працювати в неліцензованому ISM-діапазоні частот, тобто в смузі частот, відведених для промислової, наукової і медичної радіослужби (918 МГц, 2450 МГц, 5800 МГц, 22500 МГц).

Вимоги до функціональної безпеки систем збору і обробки даних постійно посилюються. Це відноситься не тільки до систем, призначених для застосування в атомних станціях, але до систем, що застосовуються в медичній, автомобільної, авіаційної промисловості. До систем на основі Інтернету речей, таких як "розумне" місто, "розумна" вулиця, "розумні" апартаменти, теж застосовуються високі вимоги до забезпечення функціональної безпеки [17].

Одним із загальних принципів проектування надійної мережі є апаратна надмірність, при якій механізми аварійного відключення при збоях і відмовах дозволяють відновити систему без втрати даних. У безпроводової сенсорної мережі є дві основні можливості використання надмірності. По-перше, це просторова надмірність, при якій у кожного основного безпроводового вузла є як мінімум два резервних, з якими він може обмінюватися даними, а схема маршрутизації дозволяє ретранслювати дані на будь-який резервний вузол, при цьому дані обов'язково доставляються в кінцевий пункт призначення.

Правильно організована стільникова (коміркова) мережа, в якій кожен вузол може обмінюватися даними з двома (або більше) сусідніми вузлами, має більш високу надійність, ніж двоточкова мережа, так як дозволяє автоматично відправляти дані за альтернативним маршрутом, якщо основний маршрут недоступний. Другий рівень надмірності мережі забезпечується використанням декількох каналів, рознесених в радіочастотному спектрі. В цьому випадку пари вузлів можуть перемикати канали при кожній передавання даних, тим самим запобігаючи відмови, що виникають в тимчасовій області в будь-якому конкретному каналі. Таким чином, забезпечення надійності такої мережі тісно

пов'язане ще з використаним інтелектуальним програмним забезпеченням, призначеним для управління роботою мережі. Це ПО динамічно оптимізує топологію мережі, безперервно відстежуючи якість каналу зв'язку, щоб максимізувати пропускну здатність в умовах дії перешкод і інших факторів, що впливають.

Безпека – ще одна важлива властивість промислових безпроводових сенсорних мереж. Основою безпеки БСМ є її конфіденційність, тобто дані, що передаються по мережі, не повинні бути прочитані ким-небудь, крім можливого одержувача. Тому безпека мережі характеризується цілісністю, коли кожне одержане повідомлення підтверджується тим, що воно було відправлено без додавання, видалення або зміни вмісту, і справжністю, коли в повідомленні міститься підтвердження, що воно було отримано з даного джерела. Перевірка мережі на автентичність також захищає повідомлення від помилкових даних. Технології забезпечення безпеки, які повинні бути вбудовані в БСМ, включають шифрування (наприклад, відповідно до стандарту шифрування AES128) і надійні ключі, генератори випадкових чисел для запобігання активних атак, перевірку цілісності повідомлення (Message Integrity Checks - MIC) для кожного з них і списки контролю доступу (Access Control Lists - ACL) для дозволу або заборони доступу до певних вузлів мережі. Ці технології забезпечення безпеки БСМ можуть бути легко включені в багато пристроїв, що використовуються в сучасних мережах. На практиці іноді користуються спрощеними засобами підтримки безпеки БСМ. Наприклад, підключення захищеного вузла мережі до "небезпечного" шлюзу підвищує уразливість мережі і це необхідно враховувати при її проектуванні.

Промисловий Інтернет речей не завжди розгортають мережеві фахівці. У ряді промислових виробництв обладнання та послуги Інтернету речей об'єднують з раніше використовуваними застарілими системами і обладнанням.

Інтелектуалізація сучасних БСМ повинна забезпечувати простоту використання промислового Інтернету речей. Мережі повинні швидко самоорганізовуватися і не вимагати зупинки на відновлення, автоматично

виправляючи або змінюючи маршрути при втраті зв'язку, мати можливості самоконтролю і самодіагностики при збоях і відмовах, а в ідеалі практично не вимагати обслуговування.

Крім того, БСМ і системи на їх основі повинні забезпечувати глобальне розгортання, орієнтоване на роботу з віддаленими користувачами. Це зазначено у вимогах, пропонованих до мережі міжнародними галузевими стандартами радіозв'язку, такими, наприклад, як IEEE 802.15.4e TSCH.

Попередня обробка інформації включає в себе: схему узгодження з датчиком (джерелом сигналу), гальванічну ізоляцію, аналогову переробку, аналого-цифрове перетворення, цифрову обробку сигналу.

Накопичення даних в більшості випадків реалізується у вигляді буферизації даних перед передачею в будь-який інтерфейс. На прикладі ПК, це може бути як внутрішній інтерфейс (PCI, PCI Express), так і зовнішній (USB, Ethernet, RS-485, RS-232).

У систему збору даних також включають і керуючі засоби: лінії цифрового вводу-виводу, цифро-аналогові перетворювачі. Таким чином, система збору даних охоплює відразу кілька рівнів програмних і апаратних засобів.

Фундаментальний принцип побудови систем збору даних – це модульність, що забезпечує гнучкість при побудові систем. Це можуть бути як окремі модулі, так і модулі, об'єднані в блок (крейт).

Параметри сучасних систем збору даних постійно удосконалюються. Зростає їх швидкість перетворення, зменшується рівень шуму, знижується ступінь нелінійних спотворень. Однак, поліпшення цих параметрів найчастіше вимагає збільшення споживної потужності, що в багатьох випадках обмежується конкретним застосуванням систем збору даних, зокрема, використанням автономного живлення, відсутністю можливості відведення додаткового тепла, внаслідок чого зростає температурний дрейф лінійних вузлів і т.д. Одним із шляхів вирішення цієї проблеми є застосування методу динамічного регулювання потужності споживання. У найпростішому випадку метод полягає в перекладі з

активного в сплячий режим електронних компонентів, які в певний інтервал часу не беруть участі в процесі збору даних. На рис. 1.8 приведена схема типового поразрядного АЦП з драйвером, як базового елементу системи збору даних. Його продуктивність пов'язана з потужністю споживання, якою можна керувати в процесі роботи системи. У мікросхемах драйверів АЦП, як правило, є спеціальні виводи, що дозволяють відключати їх від джерела живлення в період між циклами перетворення, що дає можливість істотно знизити середнє значення струму споживання.

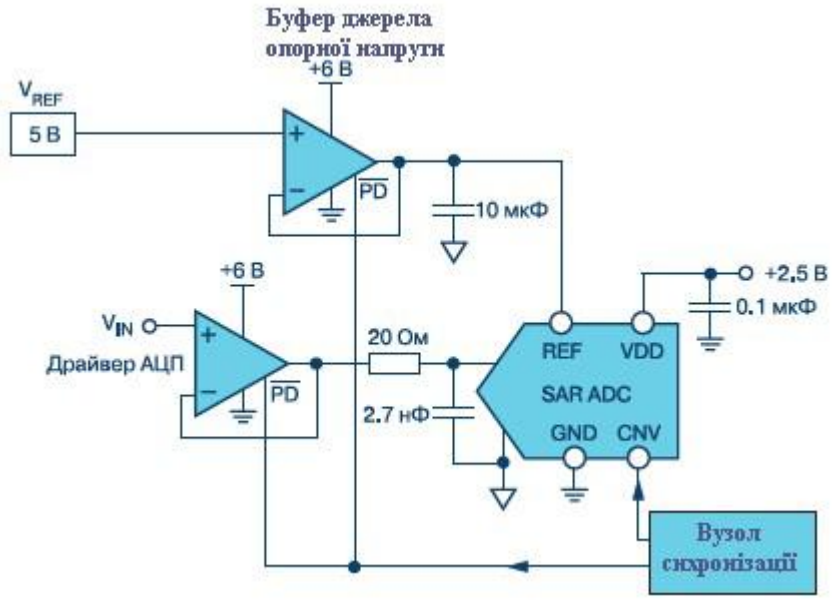

Рисунок 1.8 – Функціональна схема системи збору даних на основі поразрядного АЦП

На рис. 1.9 показані традиційна система збору та обробки даних, яка включає досить багато зовнішніх компонентів, що обрамляють АЦП попереднього покоління, і нова система, в якій практично всі компоненти включені до складу мікросхеми перетворювача [18]. Слід зазначити, що сучасні системи збору і обробки даних в разі збою або відмови, можуть стати причиною виходу з ладу складного обладнання. Наприклад в системах, які підтримують на заданому рівні (з похибкою 5%) тиск в газовому резервуарі, завжди є ймовірність того, що на

виході АЦП можуть з'явитися помилкові дані, і контролер не зможе відрегулювати відхилення внутрішнього тиску від зовнішнього, що може привести до вибуху резервуара і, як наслідок, до людських жертв.

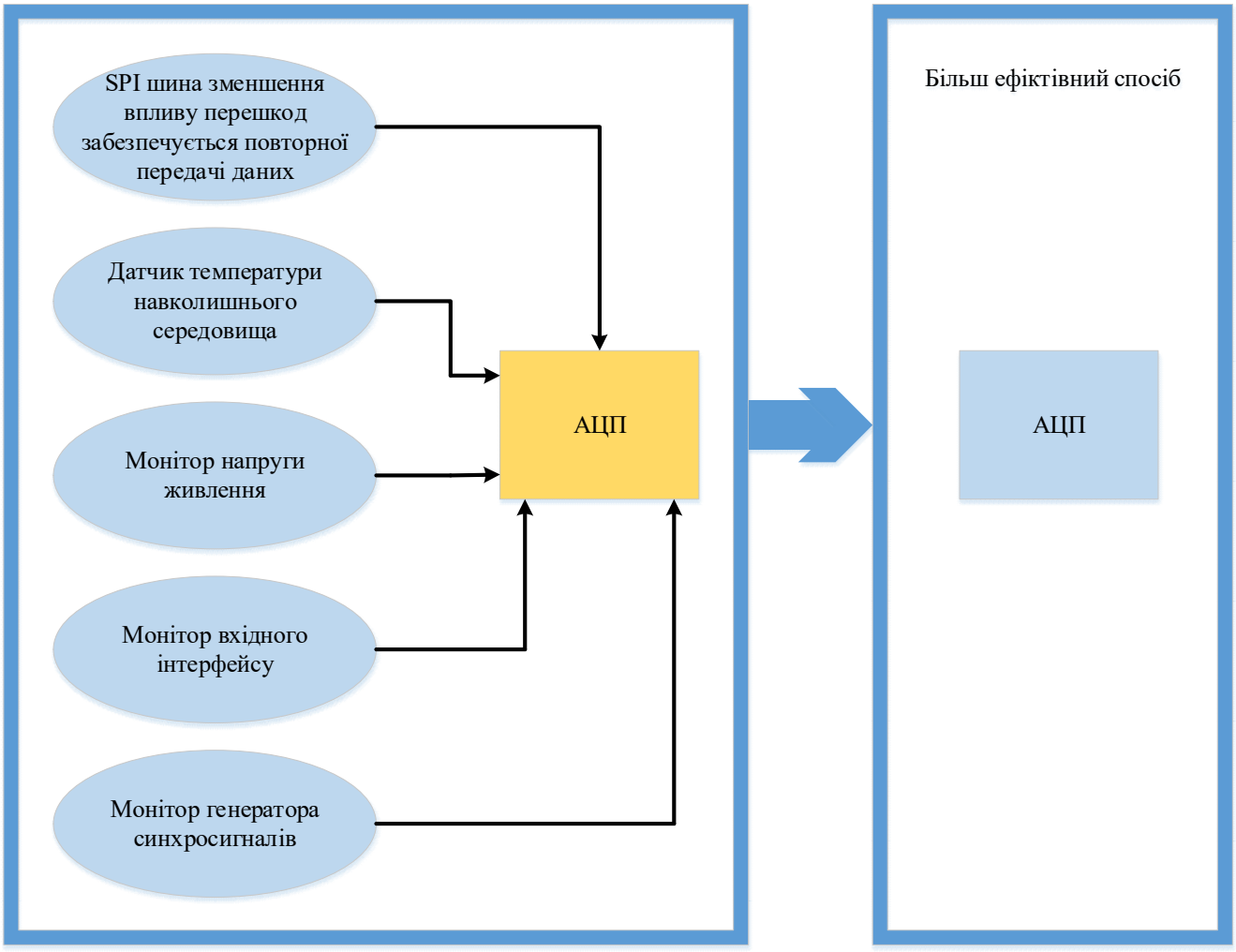

Рисунок 1.9 – Система з функціями діагностики традиційна (зліва) і нова (справа)

Причин виникнення помилок у роботі:

- на виході джерела живлення напруга нижче заданого;
- пошкоджений датчик тиску або підсилювач на вході АЦП;
- збої або відмови в цифровому вузлі АЦП приводять до спотворення вихідного коду даних;
- спотворення коду в лінії зв'язку між АЦП і контролером;

- вихід температури навколишнього середовища за межі діапазону робочих температур ІМС АЦП.

Згідно із сучасними вимогами, системи управління складними об'єктами підвищеної небезпеки повинні мати високу функціональну безпеку. Функціональна безпека є системною властивістю, проте забезпечення її починається на рівні мікроелектронної елементної бази. Самодіагностика і самоконтроль закладаються у вигляді додаткових вузлів безпосередньо в кристали АЦП і мікроконтролерів.

Безпека БСМ включає три наступних аспекти: конфіденційність, цілісність і автентичність або достовірність. Під конфіденційністю мається на увазі те, що дані не виходять за межі відомої інфраструктури Інтернету речей або були заблоковані зовнішніми по відношенню цієї інфраструктури пристроями. Під цілісністю даних мають на увазі те, що вони не змінюються при передавання, тобто до них не додається додаткова інформація, і вони не модифікуються в процесі передавання. Під автентичністю мається на увазі те, що дані надходять від ексклюзивних джерел. Якщо захищений сенсорний вузол пов'язаний з незахищеним шлюзом, виникає небезпека несанкціонованого доступу до БСМ. Безпека роботи мережі підтримується поліпшеним стандартом шифрування даних AES-128, якщо мережа відповідає стандарту IEEE 802.15.4, і стандарту шифрування даних AES-128/256 для мережі в стандарті IEEE 802.11. В рамках стандарту шифрування даних використовується криптографічний генератор псевдовипадкових чисел з розрядністю не менше 128 двійкових розрядів і список контролю доступу (ACL), які дозволяють забезпечити необхідний рівень захисту БСМ.

Основні вимоги до функціональної безпеки безпроводових сенсорних мереж регламентуються серією стандартів МЕК 61508 і МЕК 61511. Головною особливістю цих стандартів є ризик-орієнтований підхід.

Промислові мережі повинні працювати безперервно протягом багатьох років, тому незалежно від того, наскільки надійна мережа, в ній так чи інакше можуть виникати збої і відмови. На якість роботи мережі в процесі її експлуатації можуть впливати різні чинники навколишнього середовища. Раннє і належне оповіщення

про проблеми в роботі БСС є важливим аспектом будь-якої промислової мережі, а здатність швидко діагностувати і усувати неполадки є основою високоякісного обслуговування. Сучасна система управління промислової БСМ має як мінімум забезпечувати доступ до такої інформації:

- якості зв'язку за рівнем переданих сигналів;
- відсотку успішно прийнятих-переданих пакетів;
- кількості вузлів без альтернативних маршрутів приймання передавання даних;
- станом вузла і рівнем батарейного живлення.

В правильно спроектованих промислових БСМ ці проблеми вирішуються автоматично. Дані перенаправляються по альтернативних маршрутах при погіршенні якості зв'язку, безперервно оновлюється топологія мережі для забезпечення надійного підключення вузлів.

Промислові мережі повинні використовувати інтелектуальні вузли та функції управління мережею, в тому числі її безпекою, максимально використовуючи інформаційні та об'єктні технології компанії, в якій вони застосовуються. Мережі повинні бути легко налаштованим для адаптації до конкретних вимог додатків.

Беручи до уваги високі вимоги до енергоспоживання для забезпечення тривалого терміну служби батареї, слід використовувати можливості самоорганізації мережі з метою мінімізації енергоспоживання в процесі обміну даними.

Висновки до розділу

Безпроводові сенсорні мережі є основою технології Інтернету речей, на базі яких створюються пристрої та системи нового покоління для застосування в різних областях людської діяльності.

Для забезпечення умов роботи та підтримки безпеки в приміщеннях різних видів діяльності необхідно впроваджувати безпроводові сенсорні мережі.

Широке застосування технології Інтернету речей тісно пов'язане із забезпеченням функціональної та інформаційної безпеки безпроводових сенсорних мереж.

Надійність БСМ залежить від безлічі факторів, включаючи параметри її компонентів і параметри середовища, в якій мережі експлуатується. Таким чином, надійність мережі залежить як від формату, швидкості передавання даних, надійності апаратних засобів, так і від зовнішніх факторів: електромагнітних завад, характеру місцевості, на якому розповсюджуються радіохвилі, дальності передавання, організації роботи мережі в умовах дії активних і пасивних перешкод і багатьох інших факторів, які слід враховувати при проектуванні і експлуатації БСМ.

Проаналізувавши параметри технологій Інтернету речей, найбільш оптимальним і збалансованим рішенням для БСМ може бути використання технології LoRaWan. Тому що це запатентована технологія безпроводового зв'язку, яка поєднує в собі наднизьке споживання енергії і ефективний дальній зв'язок. При цьому потрібно враховувати, що дальність дії сильно залежить від навколишнього середовища і можливих перешкод (LOS або N-LOS).

2 РОЗРОБКА СТРУКТУРНОЇ ТА ФУНКЦІОНАЛЬНОЇ СХЕМ СИСТЕМИ

2.1 Обґрунтування вибору технології безпроводового зв'язку

Для ефективного розв'язку завдань, пов'язаних з енергоспоживанням використаємо технологію мережі LoraWAN.

M2M та IoT стали основною метою розгортання LoRa через специфікації зв'язку на великі відстані і з низьким енергоспоживанням. Крім того, алгоритм адаптивної швидкості передавання даних технології LoRa допомагає максимізувати час автономної роботи вузла і ємність мережі.

Wi-Fi і Bluetooth вже є визнаними безпроводовими технологіями для локальної мережі (LAN). Завдяки популярності і простоті використання протоколу, ці безпроводові технології домінують на ринку IoT, але у технології є недолік – проблема у галузі передавання. Для областей застосування IoT, таких як інтелектуальна система позиціонування і інтелектуальне сільське господарство, потрібні енергоефективні сенсорні вузли, які можуть зв'язуватися на великій відстані. У недавніх дослідженнях провели тестування дальності зв'язку в приміщенні на основі технологій Wi-Fi і LoRa відповідно [19, 20]. Зона покриття системи позиціонування на основі Wi-Fi становить 2 метри [19], а LoRa дозволяє досягти максимальної зони охоплення 200 метрів і 28,8 метра з високою точністю результату позиціонування [20]. Результати показують слабкість технології Wi-Fi в системі позиціонування в порівнянні з технологією LoRa. Дальність зв'язку системи Bluetooth складає 15 м (без розширення діапазону), а для Wi-Fi – 60 м [21].

Впровадження рішення з використанням технології Wi-Fi або Bluetooth потребує більш високих витрат для побудови мережі телекомунікації, для якої потрібен додатковий розширювач діапазону. Це мотивує розвиток багатьох технологій малопотужних глобальних мереж, таких як LoRa, для виконання таких вимог як низькі витрати при побудові мережі та використання без ретрансляторів.

Ґрунтуючись на дослідженні [22], основним цільовим застосуванням технології LoRa є інтелектуальні пристрої, які працюють автономно і не вимагають

постійного зв'язку. Використовуючи один приймач в мережі LoRa, можна обробляти безліч вузлів в декількох місцях в межах області, на відміну від системи на основі Wi-Fi, яка повинна мати багато точок доступу для збільшення зони покриття. Поєднання технологій LoRa і Wi-Fi знижує вартість розгортання системи IoT. У порівнянні з рішенням IoT на основі Wi-Fi або Bluetooth, яке має невеликий діапазон передавання даних і пропускну здатність (без додавання розширювача або ретранслятора діапазону), ця технологія здатна забезпечити максимальну ефективність передавання даних при збереженні низьких витрат на роботу. Модуляція LoRa відбувається на фізичному рівні, який використовує власну модуляцію Chirp Spread Spectrum, отриману зі схеми модуляції з розширеним спектром, цей тип модуляції працює з сигналами що мають рівень нижче рівня шуму. Це робить його більш стійким до впливу завад [23].

Концепція модуляції з розширеним спектром полягає в перетворенні одного біта інформації в інший ряд бітів і поширення його на весь спектр. Іншими словами, сигнал або інформація поширюється по широкосмугової мережі. Модуляція з розширеним спектром – це стара методика модуляції, розроблена в 1940 році, яка спочатку використовувалася для військового зв'язку. Система LoRa характеризується п'ятьма основними параметрами:

- носійна частота;
- потужність передавача;
- коефіцієнт розширення (SF);
- ширина смуги (BW);
- коефіцієнт коду (CR).

Метод модуляції, що використовується в LoRa, робить його стійким до канального шуму, оскільки вся виділена смуга пропускання використовується для широкомовної передавання сигналу (інформації або даних), безпеку системи LoRa може бути гарантована, оскільки передача поширюється псевдовипадковою послідовністю символів. Отже, сам метод модуляції забезпечує базову безпеку для

системи LoRa [24]. Проникнення сигналу LoRa дозволяє забезпечити достатню дальність зв'язку в приміщеннях [25].

Існує безліч рішень, заснованих на технологіях LoRa. По суті, ця технологія використовується в додатках, націлених на низьке енергоспоживання, низьку швидкість передавання даних і передавання даних на великі відстані [26].

Таким чином, мережа LoRa є підходящою альтернативою, коли, наприклад, мережа Wi-Fi не покриває потрібну відстань.

У системі LoRa використовується носійні частоти: 433, 868 і 915 МГц [27]. Потужність передавача і коефіцієнт підсилення антени вибираються на підставі обмеження EIRP, табл. 2.1.

Таблиця 2.1 – Максимальна потужність в частотних діапазонах

Частотні діапазони	Максимальна потужність
433 МГц	100 мВт EIRP
868 МГц	100 мВт EIRP
915 МГц	100 мВт EIRP

Потужність і послаблення антени повинні вибиратися відповідним чином, щоб уникнути перевищення встановленого обмеження EIRP. Для України максимальна потужність 100 мВт EIRP.

Пристрої LoRaWAN поділяються на три робочих класи, описаних в специфікаціях протоколу [27]:

1. Клас А: пристрої можуть відправляти передавання по висхідній лінії зв'язку. За цими передачами слідують два коротких вікна прийому низхідних ліній. Будь-яка інша передача по низхідній лінії від сервера повинна чекати наступної передавання по висхідній лінії від пристрою.

2. Клас B: в цьому режимі пристрій відкриває додаткові вікна прийому в запланований час. Пристрій синхронізує свій внутрішній годинник, використовуючи маяки, які випромінює шлюзом, щоб сервер знав, коли заплановані вікна.

3. Клас C: Пристрій LoRaWAN має майже безперервні вікна прийому. Для передавання по низхідній лінії зв'язку від мережевого сервера не потрібно ніякої передавання по висхідній лінії зв'язку або синхронізації годин.

Технологія модуляції LoRa (Long Range) являє собою метод модуляції, який забезпечує значно більшу дальність зв'язку (зону покриття), ніж інші конкуруючі з ним способи. Метод ґрунтується на технології модуляції з розширеним спектром і варіації лінійної частотної модуляції (Chirp Spread Spectrum, CSS) з інтегрованою прямий корекцією помилок (Forward Error Correction, FEC). Технологія LoRa значно підвищує чутливість приймача і, аналогічно іншим методам модуляції з розширеним спектром, використовує всю ширину смуги пропускання каналу для передавання сигналу. Технологія LoRa дозволяє здійснювати демодуляцію сигналів з рівнями на 19,5 дБ нижче рівня шумів, притому що для правильної демодуляції більшості систем з частотної маніпуляцією (Frequency Shift Keying, FSK) потрібна потужність сигналу як мінімум на 8-10 дБ вище рівня шуму.

2.2 Аналіз об’єкту для впровадження системи

Розглянемо національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" (КПІ ім. Ігоря Сікорського), як об'єкт для впровадження безпроводової сенсорної мережі LoRaWAN.

НТУУ "КПІ ім. Ігоря Сікорського" вважається найбільшим навчальним закладом в Україні. В університеті працюють 18 факультеті та 9 навчально-наукових інститутів. У ньому навчається 25 тисяч студентів, аспірантів і докторантів. Має у кампусі центр культури та мистецтв, спортивний комплекс, поліклініку.

Будівлі інститутів, факультетів НТУУ "КПІ ім. Ігоря Сікорського" та університетські гуртожитки розташовані на площі близько 1,2 км^2 [28].

IoT доцільно розміщувати на території університетів в першу чергу для вирішення різного роду проблем. У випадку з НТУУ "КПІ ім. Ігоря Сікорського", на території кампусу немає ні транспорту, ні оранжерей, де потрібно відстежувати вологість, ph–ґрунту та час поливу, але гострою проблемою є температура повітря в лекційних приміщеннях, за нею потрібно стежити в холодну пору року, тому що великі приміщення іноді не достатньо опалюються, і пари відміняються за значеннями термометрів в лекційних приміщеннях, також критично важливо розмістити сенсорні датчики виявлення пожежі.

В рамках прийнятих стандартів відзначається, що головною ознакою загоряння, за яким можна своєчасно визначити наявність проблеми і прийняти оперативні заходи для її усунення, є дим. Відомо, що на самому початку пожежі, в переважній більшості випадків, відбувається тління будь-якого матеріалу, що завжди супроводжується різними ступенями задимлення. І тільки після цього з'являються осередки загоряння, які виділяють тепло, і дозволяють за допомогою теплових датчиків відреагувати на небезпеку. Пожежі набагато простіше запобігти ще на початковій стадії – з появою диму, який, небезпечний для життя. На основі цього, можна зробити висновок, що димові пожежні датчики – це найбільш ефективний засіб захисту від лиха. В Україні димові датчики поки не отримали такого широкого розповсюдження, як в західних країнах. Використовуються, головним чином, датчики теплові. І саме тому за кількістю пожеж наша країна істотно випереджає інші.

Додатково IoT використаємо для моніторингу стану таких рівнів якості повітря, як температура, вологість повітря, CO і CO2. У системи застосуємо LPWAN модулі LoRa 868 МГц потужністю 20 дБм для передавання даних і для користування на практиці Antares, як хмарний сервіс для зберігання даних, для відображення на Android, а для аналізу даних краще експлуатувати Node-red.

Для покриття території кампусу НТУУ "КПІ ім. Ігоря Сікорського" (у даному випадку у кампусі центральної частини) доцільно використати шлюзи LoRa у кожному корпусі, або один на два поряд розташованих корпуси, як у корпусах 13-16 (рис. 2.1), тому що мережа буде розгортатися в середовищі зі склом, бетоном і металом та з високим рівнем щільності завад між шляхами розповсюдження сигналу. Так як у корпусах 13-16 схожа архітектура, близьке розміщення один до одного та однакова площа будівлі – доцільно використовувати один шлюз на два поряд розташованих корпуси, при такому розміщенні шлюз здатен забезпечити максимальну ефективність передавання даних при збереженні низьких витрат на роботу. Такий самий підхід підключення вузлів до шлюзу іншої будівлі застосовано у корпусах 5 і 35, 20 і 21, 22 і 23, тому для покриття території загальна кількість шлюзів дорівнює 20. На рис. 2.2 наведено конфігурацію мережі LoRa, розгорнутої у кампусі НТУУ "КПІ ім. Ігоря Сікорського".

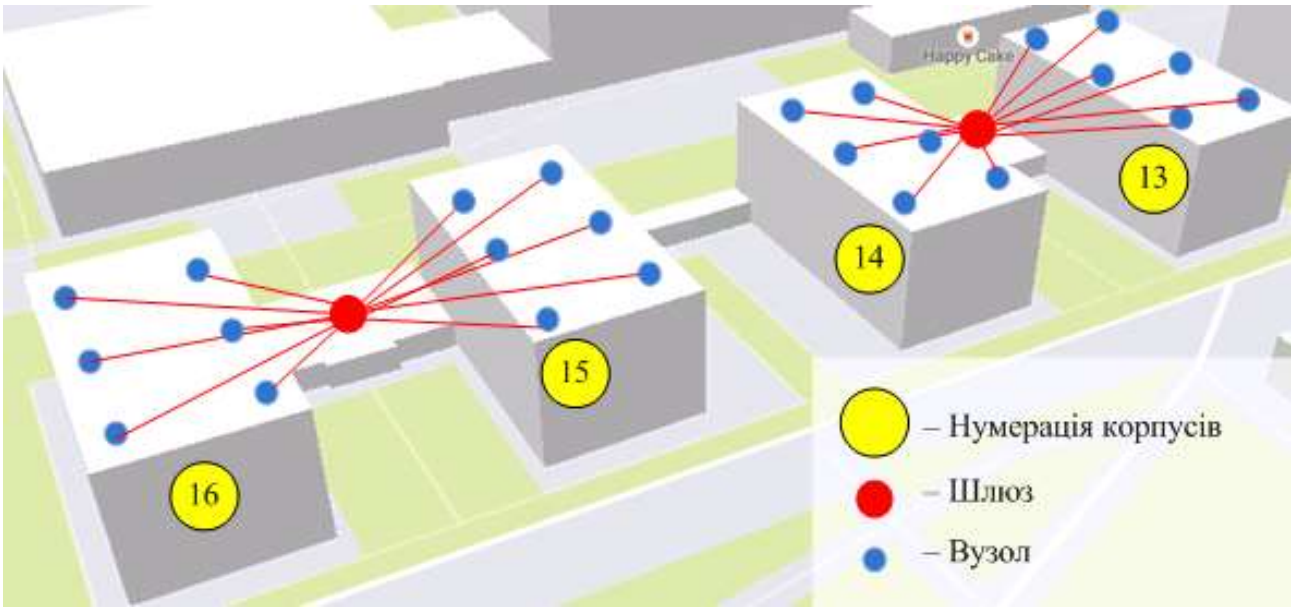

Рисунок 2.1 – Розташування шлюзів і вузлів у корпусах 13-16

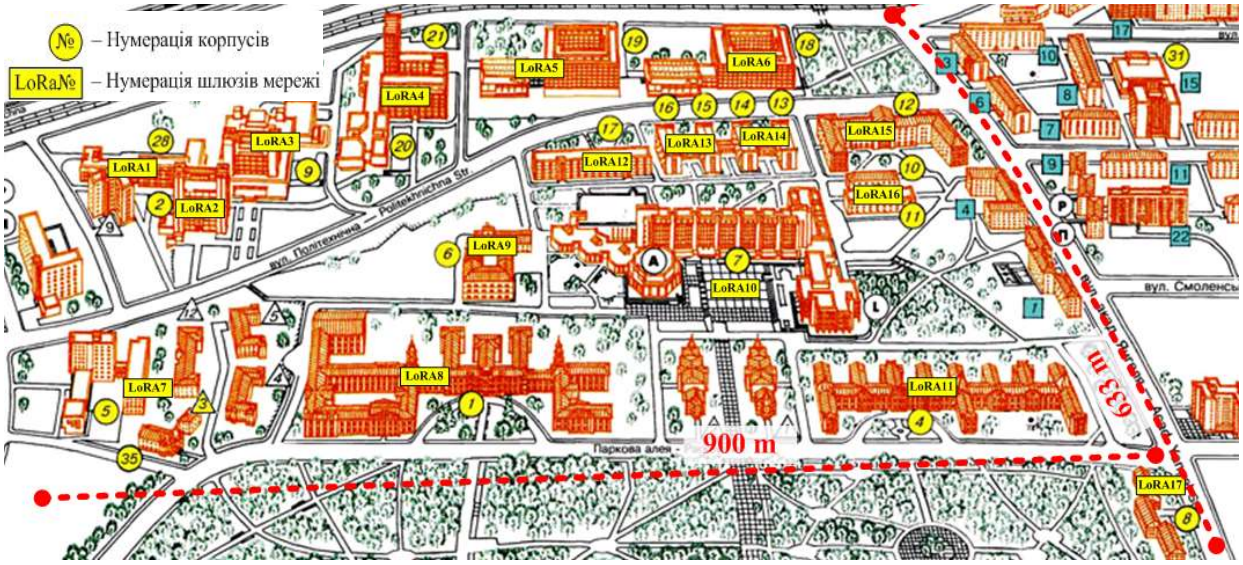

Рисунок 2.2 – Конфігурація мережі LoRa, розгорнутої у кампусі КПІ

Проходження сигналу через перешкоди на шляху передавання зменшує його потужність. Коли потужність сигналу від передавача нижче максимальної чутливості приймача, шлюз LoRa не може виявити і прийняти сигнал. Отже, кращій LoRa-зв'язок забезпечується при прямій видимості, наприклад, розташовуючи шлюз або вузол LoRa поруч з вікном замість кімнати (по можливості).

НТУУ "КПІ ім. Ігоря Сікорського" займає територію близько 120 гектарів, тому спочатку доцільно проаналізувати IoT систему з одним шлюзом LoRa на одному факультеті, наприклад ФЕЛ, а потім з отриманою практично інформацією, після тестування, розташовувати на всієї території НТУУ "КПІ ім. Ігоря Сікорського".

У будівлі факультету електроніки 5 поверхів. Архітектура розташування приміщень на всіх поверхах однакова, крім першого, через головний вхід (рис. 2.3).

Для ефективного покриття безпроводової сенсорної мережі шлюз LoRa потрібно розмістити всередині будівлі на середньому поверсі. Групи датчиків розподілити рівномірно по аудиторіях, так щоб датчики диму діяли ефективно, а датчики стану навколишнього середовища не зачіпали студенти.

Підходяще місце для установки детектора диму – це стеля в кімнаті або коридорі, поруч з входом до приміщення. Якщо встановити на стелю неможливо, детектор можна прикріпити до стіни, але максимально близько до стелі.

Є ряд місць, де краще не встановлювати детектор диму, тому що він може часто давати неправдиві тривоги:

1. Місця, де виділяється пар, наприклад в душовій та ванній кімнаті або на кухні.

2. У безпосередній близькості від вентиляційних отворів, нагрівальних пристроїв або радіатора опалення. У таких місцях конвекція повітря може запобігти потраплянню диму на детектор.

3. У гаражі, де вихлопні гази можуть викликати помилкову тривогу.

4. Близько до лампам. Детектор диму може швидко забруднитися пилом в результаті кругообігу повітря через тепло, що йде від лампи. Детектор диму повинен бути встановлений на відстані не менше 30 см від лампи.

Світлозвукові сирени для оповіщення пожежі встановити на видимих місцях коридору в центральній частині і в кожному крилі будівлі, тобто по три сирени на поверх.

Таблиця 2.2 – Радіуси дії для різних типів забудови

Тип забудови	Відкритий простір	Приміщення	Підвальне приміщення
Сільська місцевість	10 км	4,6 км	3,3 км
Передмістя	4,0 км	2,0 км	1,3 км
Місто	2,5 км	1,0 км	0,7 км
Мегаполіс	2,0 км	0,6 км	0,3 км

Узагальнений досвід польових випробувань представлений в таблиці 2.2, де показані приблизні радіуси дії (в км) БС LoRa (шлюзів) для різних типів забудови,

при висоті підвісу 30 м, Омні антени (ДН 360 град.) і коефіцієнтом підсилення антени 3 дБі.

На підставі результатів, отриманих в [29], максимальна відстань мережі зв'язку LoRa становить 330 метрів, SNR становить – 16,75 дБ, а RSSI – 130 дБм для внутрішньої установки шлюзу LoRa в приміщенні зі склом, бетоном і металом. Крім того, зі збільшенням відстані від шлюзу якість сигналу також може змінюватись. За результатами тестування на відстані більше 120 метрів від шлюзу система зв'язку починає працювати нижче рівня шуму (від'ємне значення SNR). Це в основному викликано підвищеними завадами і втратами всередині і зовні приміщень. Загалом, коли вузол LoRa відправляє повідомлення в шлюз LoRa, потужність випромінюваного сигналу, значно зменшується зі збільшенням відстані. Коли потужність сигналу від відправника нижче максимальної чутливості приймача, шлюз LoRa не може виявити і прийняти сигнал. Отже, кращій LoRa-зв'язок може досягатися при прямій видимості, наприклад, розташовуючи шлюз LoRa поруч з вікном замість замкнутої кімнати.

Таким чином, шлюз LoRa потрібно розмістити всередині будівлі на третьому поверсі біля вікна (для майбутнього розширення мережі), а вузол LoRa (відправник) у приміщеннях, які потрібно контролювати, рис.2.4. Під час збору даних вузол LoRa повинен по необхідності відправляти повідомлення на шлюз LoRa, а шлюз LoRa відправляє на вузол LoRa повідомлення з підтвердженням, яке вказує на успішне з'єднання. Така робота пристроїв відноситься до Класу А. Доцільно використовувати коефіцієнт розширення 12 і ширину смуги 125 кГц, що може забезпечити максимальну відстань покриття і підвищити чутливість зв'язку [30, 31].

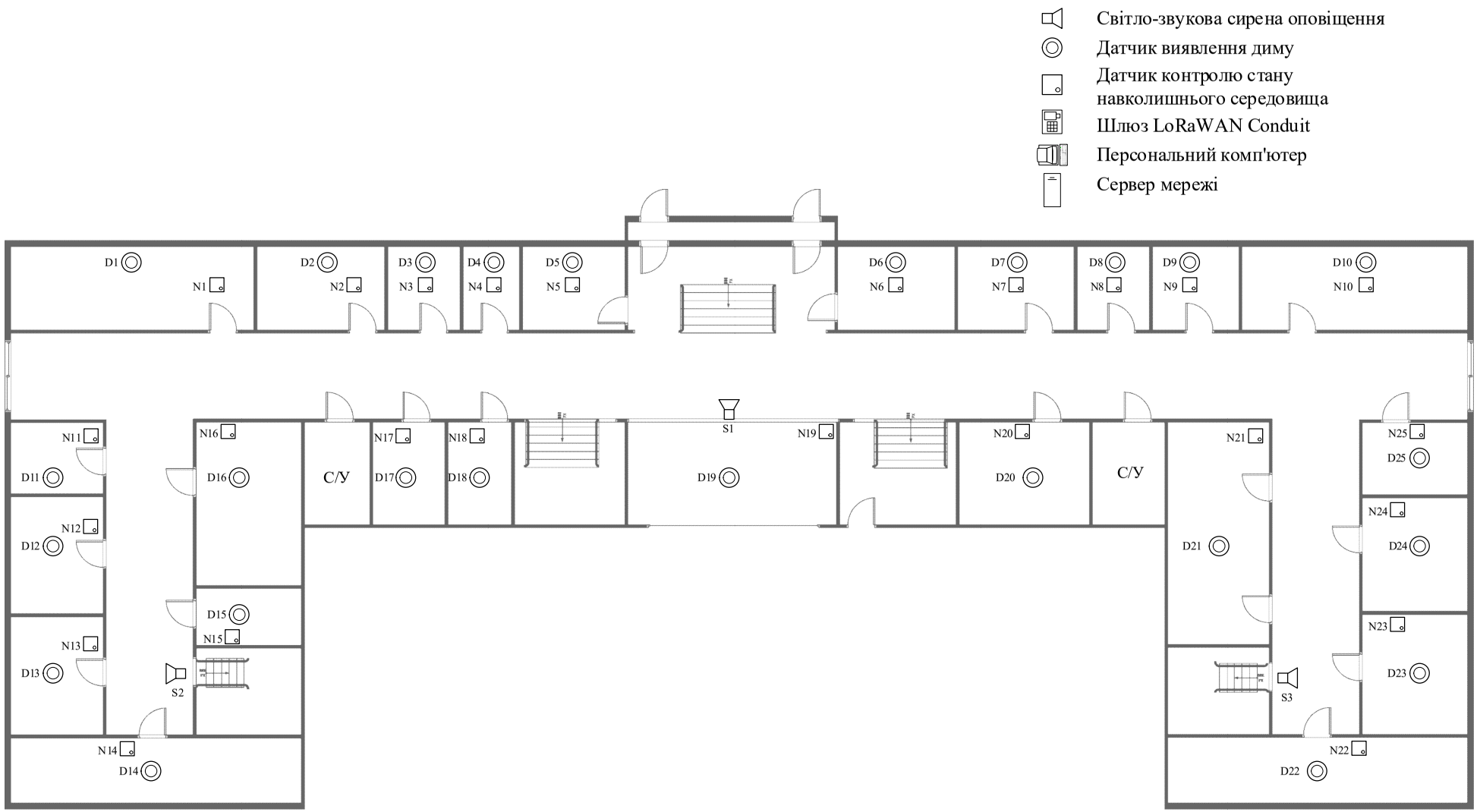

Рисунок 2.3 – План першого поверху об'єкту та розташування обладнання безпровідної сенсорної мережі

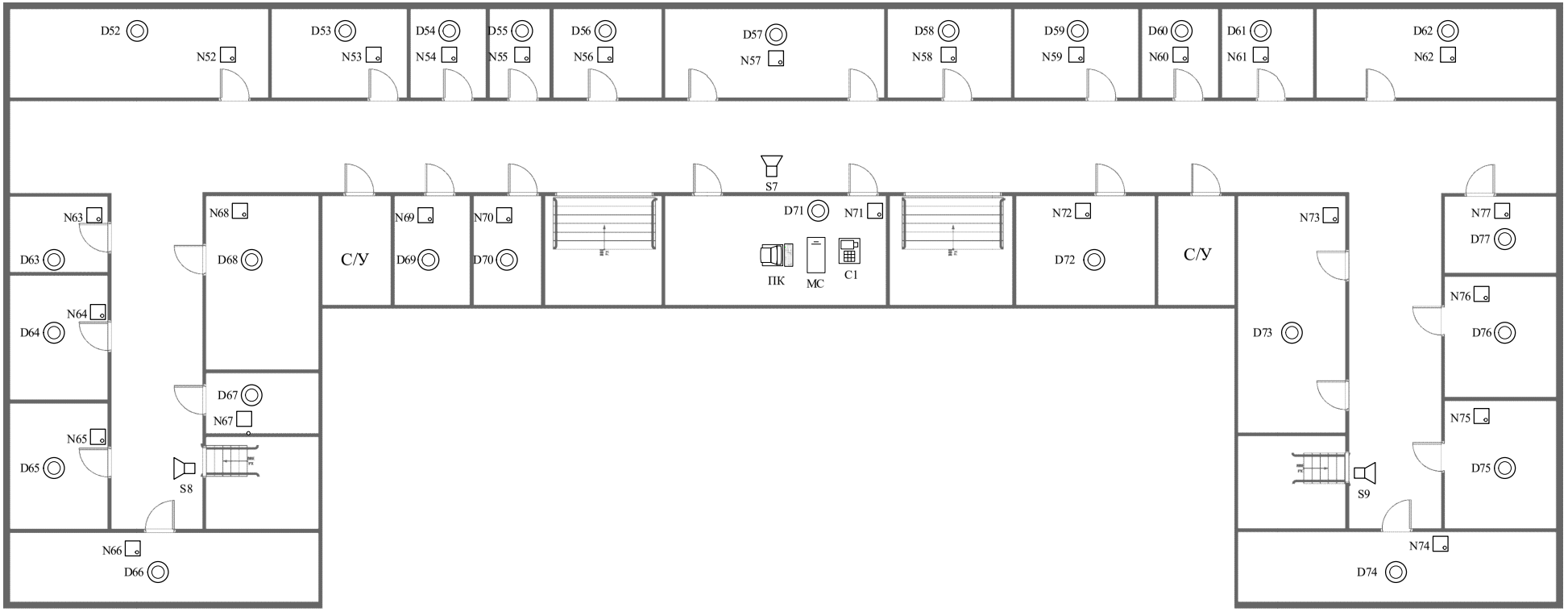

Рисунок 2.4 – План третього поверху об'єкту та розташування обладнання безпровідної сенсорної мережі

2.3 Структурна схема системи збору та контролю даних

Архітектура LoRaWAN була розроблена з метою полегшити виявлення мобільних об'єктів для відстеження активів підприємств, що є одним з найбільш швидко зростаючих додатків на рівні Інтернету речей. Протокол LoRaWAN розроблявся для використання в загальнонаціональних мережах великих операторів зв'язку. З цією метою організація LoRa Alliance стандартизував свій протокол LoRaWAN з урахуванням сумісності і взаємодії з усіма основними світовими операторами зв'язку.

На рисунку 2.5 показано структурну схему безпроводової сенсорної мережі. Виходячи з малюнка, кінцеві пристрої LoRa зв'язуються з шлюзом LoRa в зіркоподібну топологію з використанням модуляції LoRa.

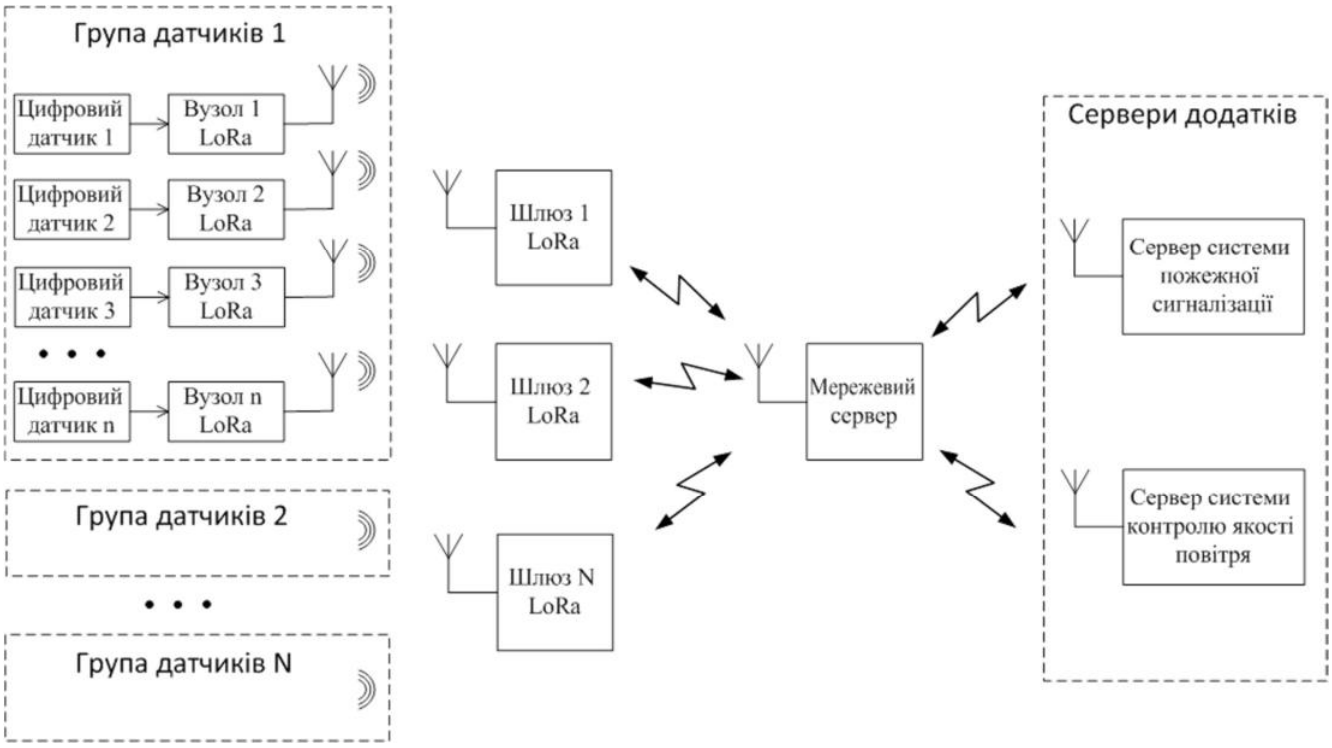

Рисунок 2.5 – Структурна схема системи контролю критичних параметрів підключення мережі LoRa

Кінцеві пристрої – призначені для здійснення керуючих або вимірювальних функцій. Містять набір необхідних датчиків і керуючих елементів. Вони розташовуються віддалено і мають батарейне харчування, можуть бути налаштовані для зв'язку з шлюзом LoRa, що підходить для вирішення проблем з великою кількістю підключень.

Шлюз – пристрій, що приймає дані від кінцевих пристроїв за допомогою радіоканалу і передає їх в транзитну мережу. В якості транзитної мережі можуть виступати Ethernet, WiFi або мережі рухомого радіотелефонного зв'язку. Шлюз і кінцеві пристрої утворюють мережеву топологію типу зірка. Зазвичай даний пристрій містить багатоканальні приймачі для обробки сигналів в декількох каналах одночасно або навіть, кількох сигналів в одному каналі. Відповідно, кілька таких пристроїв забезпечує зону радіопокриття мережі і прозору двосторонню передачу даних між кінцевими пристроями і сервером.

Мережевий сервер – призначений для управління мережею: завданням розкладу, адаптацією швидкості, зберіганням і обробкою отриманих даних.

Сервер додатків – може віддалено контролювати роботу кінцевих пристроїв і збирати необхідні дані з них.

На рис. 2.6 показаний веб-інтерфейс мережі LoRa. Це панель з програми Node-Red, яка відображає інформацію, отриману від кінцевих пристроїв LoRa, таку як SNR, RSSI і дані датчиків.

Рисунок 2.6 – Графічний інтерфейс користувача (GUI) системи LoRa з використанням Node-Red

Шлюзи підключаються до мережевого сервера через стандартні IP-з'єднання, а кінцеві пристрої використовують одно-стрибковий безпроводовий зв'язок до одного або кількох шлюзів. Всі кінцеві точки зв'язку, як правило, є двонаправленими, але вони також підтримують функціонування в режимі, що забезпечує можливість здійснення групового оновлення програмного забезпечення через стільникову мережу або передачу інших масових повідомлень, що дозволяє скоротити активний час на їх передачу. В залежності від бажаної канальної ємності і місць установки, доступні різні версії.

Пропускна здатність шлюзу LoRa, в першу чергу, є наслідком того числа пакетів, які можуть бути отримані в даний момент часу. Один шлюз SX1301 з вісьмома каналами, використовуючи протокол LoRaWAN, здатний отримати близько 1,5 млн пакетів в день. Таким чином, якщо додаток відправляє один пакет

на годину, то один шлюз SX1301 може обслуговувати близько 62 500 кінцевих пристроїв.

Модем LoRa на суміщеному GMSK-каналі має можливість зменшення перешкод до 19,5 дБ (за рахунок Гаусової фільтрації). Він може приймати і демодулювати сигнали на 19,5 дБ нижче рівня перешкод або шумів. Цей імунітет до перешкод дозволяє використовувати просту і недорогу систему з LoRa-модуляцією в тих місцях, де є важка спектральна обстановка, або в гібридних мережах зв'язку. У цих випадках використання технології LoRa дозволяє розширити діапазон покриття зв'язку, в той час як інші варіанти модуляції виявляються безсилими.

Шлюзи можуть встановлюватися всередині приміщень або на вишках. Специфікація дає значення вихідної потужності в +20 дБм безпосередньо на виході мікросхеми. Смуговий фільтр і високочастотний ключ, як і всі радіочастотні елементи, характеризуються певними втратами. Після узгодження антени і фільтрації типова потужність в антені складе +19 дБм.

Не зважаючи на дешевизну абонентських пристроїв мереж IIoT LPWAN, а також низьку абонентську плату і невисоку вартість захисту переданих даних, в мережах LoRaWAN використовуються одні з найдосконаліших алгоритмів авторизації пристроїв і захисту інформації користувачів.

Захист даних в будь-якій мережі "Інтернету речей", незалежно від конкретного стандарту чи технології, повинна відповідати таким критеріям:

- End-to-end-конфіденційність даних користувача на рівні додатку;
- взаємна ідентифікація абонентського пристрою і мережі;
- перевірка цілісності даних при передавання на радіоінтерфейсу;
- конфіденційність сигнальної інформації (керуючих команд);
- безпечне зберігання ідентифікаторів абонентського пристрою і його повноважень;
- оперативне усунення знайдених вразливостей в ПО компонентів мережі та абонентських терміналів;

- можливість використання вітчизняних ЗКЗІ (засобів криптографічного захисту інформації) для критичної інформаційної інфраструктури (КВІ).

Слід також наголосити на необхідності захисту від атак серверів (операторських, керуючих мережею, клієнтських, на яких запускаються додатки обробки даних користувача).

Для забезпечення захисту інформації, що передається та перевірки цілісності даних при передавання їх радіоінтерфейсу в мережі IoT LoRaWAN передбачена багаторівнева система безпеки (рис. 2.7).

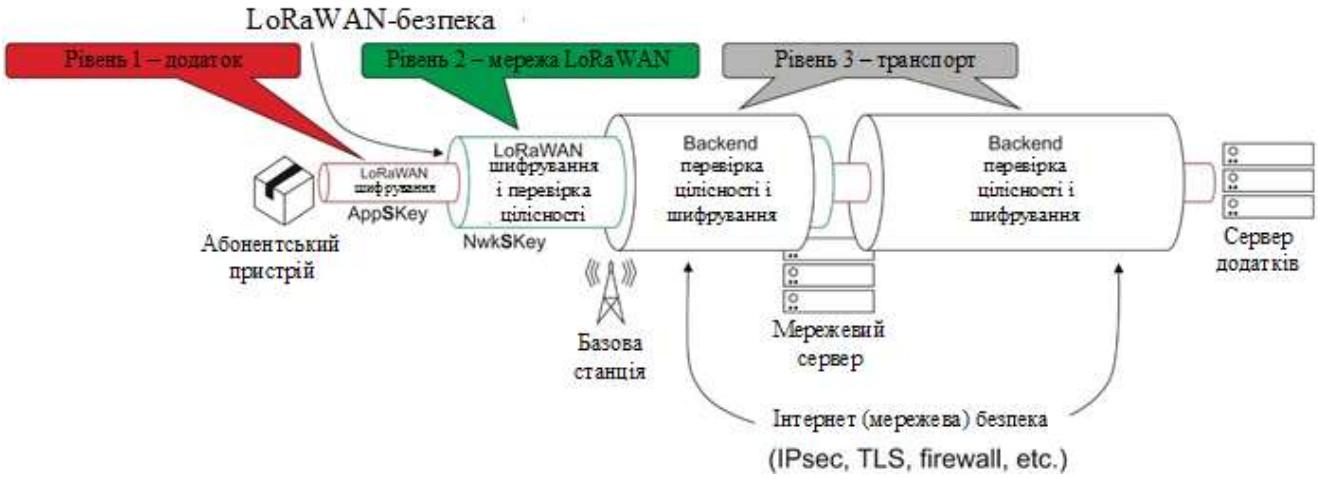

Рисунок 2.7 – Загальна схема безпеки даних в мережі LoRaWAN

1-й рівень. AES-шифрування на рівні додатку (end-to-end, тобто між абонентським терміналом і сервером додатків) за допомогою 128-бітного змінного сесійного ключа Application session key (AppSKey). Даний ключ шифрування зберігається в абонентському терміналі і на сервері додатків і недоступний оператора мобільного зв'язку (доступ до AppSKey є тільки у клієнта - власника сервера додатків). Формування сесійного ключа AppSKey відбувається паралельно в абонентському терміналі і на стороні мережі під час процедури активації терміналу – через ефір AppSKey не передається.

2-й рівень. AES-шифрування і перевірка цілісності повідомлень на мережевому рівні (між абонентським терміналом і сервером) за допомогою 128-

бітного змінного сесійного ключа Network session key (NwkSKey). Даний рівень шифрування призначений для захисту переданих сигнальних команд на MAC-рівні, а також для обчислення MIC (Message IntegrityCode) з метою перевірки цілісності даних, що передаються по радіоінтерфейсу. NwkSKeyухраніться в абонентському терміналі і на мережевому сервері і недоступний клієнту (доступ до NwkSKeyесть тільки у оператора мережі – власника мережевого сервера). Формування сесійного ключа NwkSKey також відбувається паралельно в абонентському терміналі і на стороні мережі під час процедури активації терміналу – через ефір NwkSKey не передається.

3-й рівень. Стандартні методи аутентифікації і шифрування інтернет-протоколу (IPsec, TLS і т. П.) При передавання даних по транспортній мережі між вузлами мережі (базова станція, мережевий сервер, join-сервер, сервер додатків).

За командою додатки або мережевого сервера в будь-який момент можливий перехід на нову сесію з генерацією нового комплекту ключів шифрування, що робить марними старі ключі шифрування. Також є можливість установки періодичної генерації нового комплекту ключів NwkSKey і AppSKey.

2.5 Функціональна схема системи збору та контролю даних

Для застосування Інтернету речей точне розміщення сенсора або контрольної точки має вирішальне значення. Безпроводова технологія має багато переваг перед дротовою технологією, але підключити проводові сенсори до обладнання моніторингу під час експлуатації неможливо, а дані, отримані безпроводовим сенсором в процесі експлуатації, дозволяють прогнозувати технічний стан критично важливого обладнання, і, як наслідок, уникнути небажаних і дорогих простоїв.

Живлення безпроводового вузла може здійснюватися безпосередньо від мережі живлення або від вбудованих акумуляторів. Але для БСМ система живлення повинна бути змішаною. Щоб забезпечити гнучке і економічне

розгортання БСМ, кожен вузол мережі повинен мати можливість роботи від автономного живлення протягом як мінімум п'яти років, що забезпечує максимальну гнучкість промислового Інтернету речей.

Промислові мережі для моніторингу та управління є критично важливими для багатьох галузей промислового виробництва. Вони впливають на базову вартість виробів, що випускаються, тому своєчасність отримання і передавання даних в цих мережах мають важливе значення.

Промислові мережі повинні працювати безперервно протягом багатьох років, тому незалежно від того, наскільки надійна мережа, в ній так чи інакше можуть виникати збої і відмови. На якість роботи мережі в процесі її експлуатації можуть впливати різні чинники навколишнього середовища. Раннє і належне оповіщення про проблеми в роботі БСМ є важливим аспектом будь-якої промислової мережі, а здатність швидко діагностувати і усувати неполадки є основою високоякісного обслуговування. Не всі безпроводові сенсорні мережі створені з урахуванням перерахованих факторів.

Беручи до уваги високі вимоги до енергоспоживання для забезпечення тривалого терміну служби батареї, слід використовувати можливості самоорганізації мережі з метою мінімізації енергоспоживання в процесі обміну даними. Функціональна схема системи збору та контролю даних безпроводової сенсорної мережі з одним шлюзом на рис. 2.8.

Всі кінцеві пристрої LoRa та шлюз LoRa будуть живитися від джерела постійного струму, а при автономному режимі від літієвих акумуляторів. Як тільки спрацює пожежний датчик, замкнеться лінія живлення 12 В і на вхід управління ключа SW1 буде подано нульове напруга. Ключ замкнеться, напруга від джерела живлення 12 В буде подано на сирени і вони почнуть видавати звук.

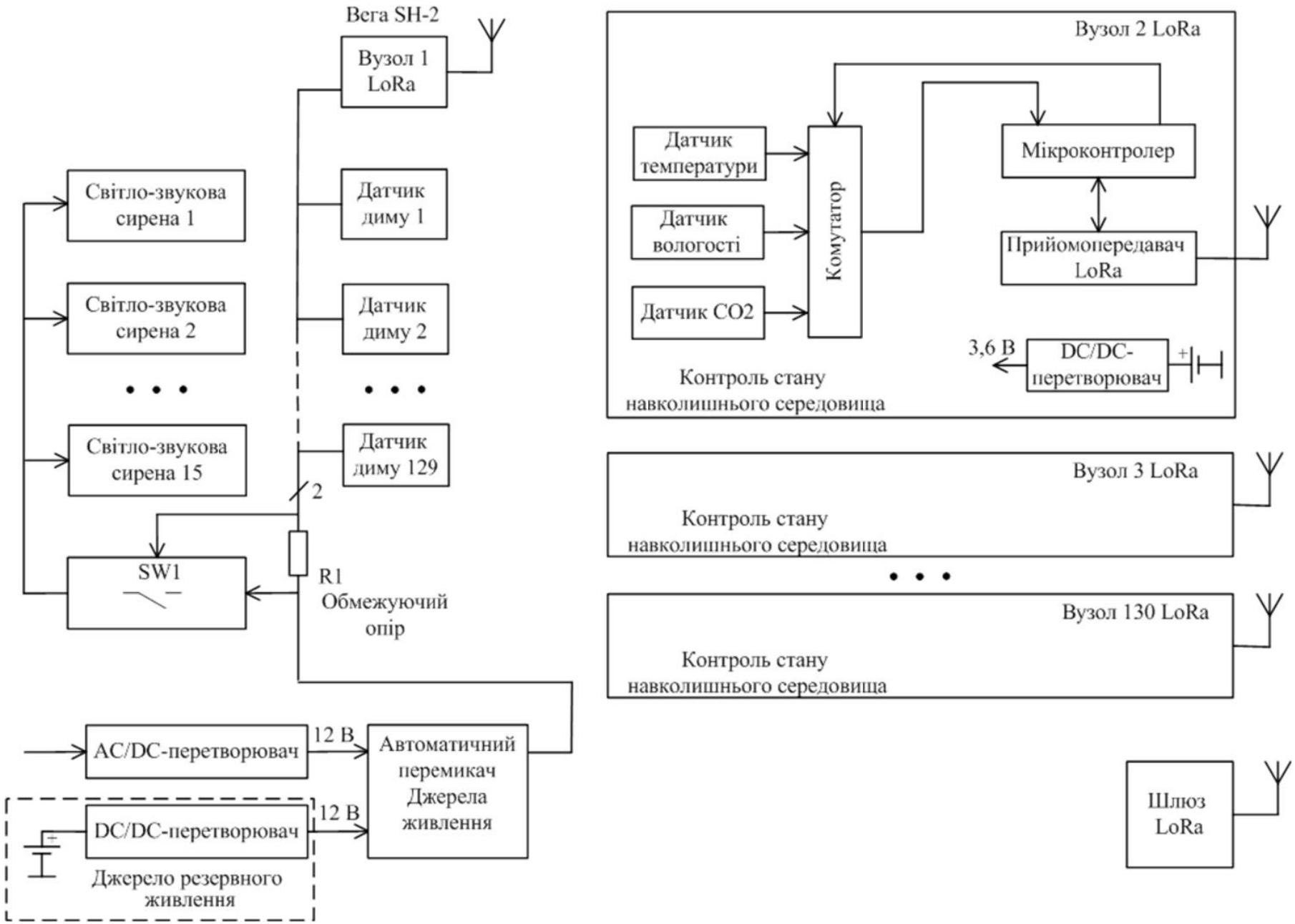

Рисунок 2.8 – Функціональна схема системи збору та контролю даних безпроводової сенсорної мережі

Висновки до розділу

Впровадження Інтернету речей на територію НТУУ "КПІ ім. Ігоря Сікорського" за допомогою технологій безпроводової мережі LoRa доцільна, тому що у НТУУ "КПІ ім. Ігоря Сікорського" важлива підтримка безпеки в приміщеннях для різних видів діяльності, де необхідні наднадійні комунікації.

IoT доцільно впроваджувати на території університета в першу чергу для раннього виявлення джерела пожежі та контролю температури повітря в лекційних приміщеннях, додатково IoT використаємо для моніторингу стану якості повітря навколишнього середовища.

На великій території кампус багато інженерних споруд, тому спочатку доцільно проаналізувати IoT систему з одним шлюзом LoRa на одному факультеті, обраний ФЕЛ, а після тестування на практиці, розповсюдити мережу на всю територію НТУУ "КПІ ім. Ігоря Сікорського".

У розділі розглянуті структурна схема системи контролю критичних параметрів підключення мережі LoRa та особливості використання засобів інтернету речей у сферах критичного застосування, конфігурація мережі на території НТУУ "КПІ ім. Ігоря Сікорського" та інтеграція системи IoT-моніторингу в мережі LoRa з архітектурою підключення системи. Сформована система збору та контролю даних про інженерні споруди університету, розгортання системи Інтернету речей для моніторингу стану температури, вологості повітря, CO і CO2.

У спроектованої БСМ на основі LoRa робота пристроїв відноситься до Класу А. Для забезпечення максимальної відстані покриття і підвищення чутливості зв'язку використовують коефіцієнт розширення 12, ширину смуги 125 кГц, антена діапазону 868 МГц, потужність передавача 20 дБм.

Всі кінцеві пристрої LoRa та шлюз LoRa будуть живитися від джерела постійного струму, а при автономному режимі від літієвих акумуляторів.

3 ОБҐРУНТУВАННЯ ТЕХНІЧНИХ РІШЕНЬ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ

3.1 Вибір шлюзу

У якості головної базавої станції або шлюзу було обрано LoRaWAN Conduit от Multi-Tech. У комплект поставки шлюзу входять: блок живлення 12В, антена 3G/LTE, кабелі microUSB і Ethernet, інструкція та модуль LoRaWAN (MTAC-LORA-868). Шлюз зображено на рис. 3.1. Параметри та характеристики LoRaWAN Conduit у табл.3.1.

Рисунок 3.1 – Шлюз LoRaWAN Conduit от Multi-Tech

Таблиця 3.1 – Параметри та характеристики LoRaWAN Conduit

Параметр	LoRaWAN Conduit
Процесор	RM9, 400 МГц
Підтримка мереж	3G/LTE
Живлення	9...32 В
Ethernet	Ethernet 10/100 (RJ-45)
USB Host	USB Host (Type A), Micro USB D
Габаритні розміри	161×107×43 мм
Діапазон робочих температур	-30...70 °C

Необхідна кількість шлюзів для підключення кінцевих вузлів – 1 шт.

Вартість контролера – 14325 грн.

3.2 Вибір антени

Штирові антени для діапазону 868 МГц. Призначені для використання в пристроях охоронної сигналізації, які працюють в діапазоні 868-868,2 МГц.

Антена W1063 рекомендована компанією MultiTech для використання з модулями LoRa MTDOT-868 і шлюзами LoRaWAN. Антена діапазону 868 МГц з круговою діаграмою спрямованості і посиленням 5 дБ використовується в якості "базової" в системах збору даних при невеликій дальності зв'язку.

Рисунок 3.2 – Антена W1063

Антена W1063 являє собою колінеарну 5/8 лямбда випромінює систему з гамма-узгодженням (j-образна антена), на рис. 3.2. Антена заземлена за постійним струмом і не має виступаючих противаг завдяки використанню четвертьволнового відсікаючого склянки. Стійка до впливу атмосферних явищ і УФ випромінювання, що забезпечує тривалий термін експлуатації і надійність в роботі.

Антена має габаритні розміри у довжину 198.6 мм. Антена обладнана роз'ємом SMA male swivel для підключення антенного фідера (кабелю). Як антенного фідера слід використовувати кабель з хвильовим опором 50 Ом. Для фідера довжиною понад 10 ... 20 м рекомендується використовувати марки кабелю з малими втратами (близько 0,1 дБ/м.)

Необхідна кількість антен – 1 шт.

Вартість контролеру – 620 грн.

3.3 Вибір вузла LoRaWAN

У якості універсального модему було обрано Вега SH-2, розроблений компанією "Вега-Абсолют", призначений для збору, накопичення і передавання даних в мережу LoRaWAN або LTE NB-IoT [32, 33]. Зовнішній вигляд модему зі знятою кришкою наведено на рис. 3.3.

Рисунок 3.3 – Зовнішній вигляд модему Вега SH-2 зі знятою кришкою і підключеними антенами

Для підключення зовнішніх датчиків в модемі передбачено 2 аналогових і два цифрових входу. Дані, що надходять від зовнішніх пристроїв, зчитуються періодично з налаштованим інтервалом часу 5, 15, 30 хвилин, 1, 6, 12 або 24 години. Лічені дані зберігаються в пам'яті модему у вигляді пакету з зазначенням часу збереження даних і передаються при черговому сеансі зв'язку з мережею LoRaWAN. Інтервал часу між сеансами зв'язку для передавання даних також налаштовується і може мати такі ж значення, як і період зчитування даних. Пам'ять модему розрахована на збереження 100 пакетів даних. У режимі передавання даних спочатку відправляються пакети з найбільш ранніми даними, а потім більш пізні.

Харчування модему здійснюється від вбудованої батареї ємністю 6400 мАг. Передбачена можливість підключення двох батарей ємністю 6400 мАг або зовнішнього джерела живлення напругою 4,5 ... 55 В.

Час внутрішнього годинника встановлюється автоматично при підключенні до "Vega LoRaWAN Configurator" через інтерфейс USB, а також може бути скориговано через мережу LoRaWAN.

Основні технічні характеристики модему наведені в табл. 3.2.

Цифрові входи COUNT1 і COUNT2 [34] можуть працювати як в імпульсному, так і в охоронному режимі (рис. 3.4). Коли вхід не підключений, на ньому присутня логічна "1". При роботі в імпульсному режимі модем підраховує кількість імпульсів на вході. Фіксація відбувається по спаду імпульсу. В охоронному режимі пристрій відстежує зміну стану входу і відправляє повідомлення в мережу при виникненні однієї з подій: охоронна ланцюг замкнута, розімкнути, або в обох випадках. Вибрати подія, за яким буде відбуватися спрацьовування охоронного входу, можна за допомогою програми "Vega LoRaWAN Configurator".

Аналогові входи ADC1 і ADC2 підключені до входів 12-розрядних АЦП і дозволяють вимірювати напругу постійного струму, подану на них в діапазоні значень від 0 до 21 В з точністю до 100 мВ.

Інтерфейси RS-485 (Modbus) і 1-Wire не можуть використовуватися одночасно. Вибір інтерфейсу здійснюється за допомогою перемичок, які встановлюються на роз'ємах XP4 і XP5 на платі (рис. 3.4). Інтерфейс 1-Wire дозволяє підключити до 10 зовнішніх датчиків (наприклад, термодатчиків).

Таблиця 3.2 –Основні технічні характеристики модему Вега SH-2

Параметр	Значення
Основні	
Входи цифрові	2
Входи аналогові	2
Розрядність вбудованих АЦП	12
Напруга постійного струму на аналоговому вході	0 ... 21 В
Інтерфейс	1-Wire, RS-485 (Modbus)
USB-порт	micro, type B
Діапазон робочих температур	-40 ... 85 ° С
Технології передавання даних	LTE NB-IoT або LoRaWAN
Вбудований датчик температури	є
Інтервал часу між сеансами зв'язку	5, 15, 30 хвилин, 1, 6, 12 або
Період накопичення даних	5, 15, 30 хвилин, 1, 6, 12 або
Обсяг пам'яті для накопичення пакетів даних	100 пакетів
Ємність вбудованої батареї	6400/12800 мАч
Напруга зовнішнього джерела живлення	4,5…55 В
Ступінь захисту корпусу	IP65
Габаритні розміри корпусу без урахування	95×95×50 мм
LoRaWAN	
Клас пристрою LoRaWAN	A
Кількість каналів LoRa	16
Частотні діапазони	RU868, EU868, IN865,
Спосіб активації в мережі LoRaWAN	ABP і OTAA
Тип антени LoRa	зовнішня
Чутливість приймача	-138 дБм
Дальність радіозв'язку в щільній міській забудові	до 5 км
Дальність радіозв'язку в сільській місцевості	до 15 км
Потужність передавача за замовчуванням	25 мВт (настроюється)
Максимальна потужність передавача	100 мВт
Час безперервної роботи від батареї	10 років від однієї батареї при передавання даних раз

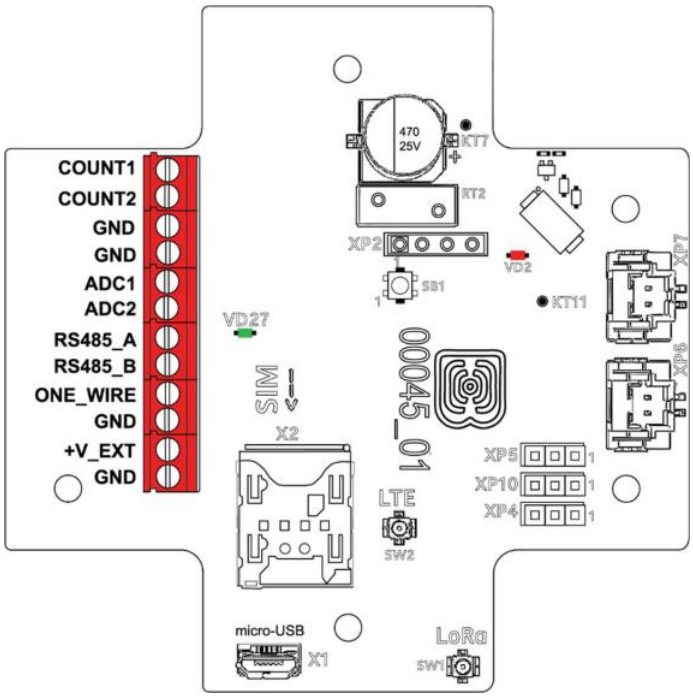

Рисунок 3.4 – Розташування роз'ємів на платі модему

На платі розташовано два світлодіодних індикатора (рис. 3.4). Червоний використовується для контролю в режимі активації пристрою в мережі LoRaWAN, при передавання даних за технологією NB-IoT і при зміні режимів роботи. Зелений індикатор використовується для налагодження в процесі виробництва. Детально про режими роботи та сигналах, що формуються індикатором червоного кольору, можна дізнатися в [34].

Харчування модему може здійснюватися від зовнішнього джерела живлення або від вбудованих батарей. Якщо використовується одна батарея, то вона підключається до роз'єму XP6 або XP7. При використанні двох батарей задіяні обидва цих роз'єму.

Особливості роботи модему по технології LoRaWAN

Модем підтримує два способи активації в мережі LoRaWAN – ABP і OTAA. Вибір способу активація здійснюється за допомогою програми "Vega LoRaWAN Configurator".

При активації за способом ABP після підключення живлення пристрій відразу починає працювати в режимі "Активний".

При активації за способом OTAA після підключення живлення модем здійснює три спроби підключення до мережі в заданому при налаштуванні частотному діапазоні. При отриманні підтвердження активації в мережі LoRaWAN пристрій подає сигнал індикатором червоного кольору (світіння протягом 3 секунд) і переходить в режим "Активний". Якщо всі спроби підключитися до мережі виявляться невдалими, модем переходить в режим зниженого енергоспоживання на добу, після чого повторює спробу реєстрації в мережі. Спроби будуть повторюватися раз на добу до тих пір, поки модем не зареєструється в мережі.

Необхідна кількість модемів для підключення датчиків – 1 шт.

Вартість модема – 2863 грн.

3.4 Вибір датчиків диму

Для побудови охоронної системи було обрано датчик виявлення диму Артон СПД-3.3. Датчик диму Артон СПД-3.3 зображено на рис. 3.5.

Рисунок 3.5 – Датчик виявлення диму Артон СПД-3.3

Принцип дії цих пожежних сповіщувачів заснований на періодичному кон-контролі оптичної щільності навколишнього середовища: її поточне значення Порівнюються з граничним значенням амплітуди відбитих від частинок диму імпульсів інфрачервоного випромінювання, що генеруються електронної схемою приладів. Параметри та характеристики Артон СПД-3.3 наведені в табл. 3.3.

Таблиця 3.3 – Параметри та характеристики Артон СПД-3.3

Параметр	Значення
Чутливість	0,05-0,2 дБ/м
Інерційність	10 с
Напруга живлення	12 ± 1,2 В
Порогова температура спрацьовування	70 ± 3 °С
Температурна інерційність при + 30 °С/хв	39…162
Температурна інерційність при + 3 °С/хв	433…1120
Спосіб формування вихідного сигналу	Контактами реле
Спосіб підключення до приймального пристрою	Чотирьохпроводовий
Струм споживання в черговому режимі	0,095 мА
Максимально допустимий струм в спрацювала стані	22 мА
Максимальна напруга комутації	100 В
Максимальний комутований струм	100 мА
Опір розімкнутих контактів реле	200 кОм
Опір замкнутих контактів реле	0,5 Ом
Габаритні розміри	100 × 46 мм
Маса	0,15 кг
Діапазон робочих температур	-30 ... 55 °С
Середній термін служби	10 років

Сповіщувач пожежний комбінований тепло-димовий СПД-3.3 призначений для виявлення загорянь в закритих приміщеннях різних будівель і споруд, що супроводжуються появою диму, а також перевищення порогового значення

температури навколишнього повітря і передавання сигналу "ПОЖЕЖА" приймально-контрольних приладів (ПКП).

Сповіщувач розрахований на безперервну цілодобову роботу з охоронно-пожежними ПКП з чотирьох схемою підключення сповіщувачів і номінальною напругою живлення шлейфу 12 В.

Сповіщувач має функцію індикації чергового режиму роботи (миготіння червоного світлодіода).

Для контролю напруги живлення шлейфу і для установки кінцевого резистора сповіщувач може комплектуватися модулем М-1.

При виявленні диму датчик диму та температури передає код "Пожежа". Шлюз при отриманні коду "Пожежа" включає сирену. При надходженні живлення на сирену, вона видає звукове оповіщення.

Необхідна кількість – 129 шт.

Вартість сповіщувача – 236 грн.

3.5 Вибір датчиків контролю повітря

Було обрано внутрішній багатофункціональний датчик навколишнього середовища SE81Z6GCN470-N з кількома варіантами додатків на різні функції: температура, вологість, світло, CO2 і присутність. Датчик встановлюється у всіх кімнатах, де э кондиціонер з функцією підключення Wi-Fi. Цей датчик передає дані з використанням будь-якої мережі LoRa (загальнодоступною або приватною) і має автономність від батарей від 2 до 5 років залежно від конфігурації.

Датчик контролю навколишнього повітря:

- температура;
- рівень вологості;
- рівень CO2;
- рівень освітленості.

Датчик LoRaWAN SE81Z6GCN470-N зображено на рис. 3.6, а характеристики наведені у табл. 3.4.

Рисунок 3.6 – Датчик контролю повітря SE81Z6GCN470-N

Таблиця 3.4 – Параметри та характеристики

Параметр	Значення
Автономний режим	Літієва батарея 3,6 В / 3500 мАг (до 4 років)
Робоча напруга	AC 220 В
Габаритні розміри	86×86×22 мм
Передача даних	LoRa
Сенсори	Температура, вологість, CO2, CO, світло, PIR (присутність). Точність: 0,5 °C/2% вологості
Діапазон робочих частот	868 МГц
Клас LoRa	Класс А

Необхідна кількість контролерів для підключення датчиків – 25 шт.

Вартість контролера – 600 грн

3.6 Вибір сирени оповіщення

Для забезпечення світло-звукового сповіщення пожежі було обрано сирену С-03-12 гучністю 100 дБ. Світло-звукова сирена С-03-12 зображена на рис. 3.7, характеристики наведені в табл. 3.5.

Рисунок 3.7 – Світло-звукова сирена С-03-12

Таблиця 3.5 – Параметри та характеристики

Параметр	Значення
Тип пристрою	Звуковий оповіщувач
Тип установки	Внутрішній
Тип підключення	Проводове
Акустична потужність	95 дБ
Тип сповіщення	Звукове
Напруга живлення	АС, 220 В
Струм споживання	55 мА
Матеріал	П'єзокераміка
Робоча температура	-30… 55 °С
Габаритні розміри	72×52×46 мм

Ціна звукової сирени С-03-12– 152 грн.

Необхідна кількість – 129 шт.

3.7 Приклад реалізації вузла контролю

Сервер мережі (Network Server) призначений для управління мережею: формуванням розкладу, адаптацією швидкості, зберіганням і обробкою прийнятих даних. В якості серверу було обрано ноутбук Lenovo ThinkPad X1 Extreme рис. 3.8. Діагональ екрану 15.6" (процесор Intel Core i7-8750H, 2,2 ГГц, 16 ГБ ОЗУ).

Рисунок 3.8 – Ноутбук Lenovo ThinkPad X1 Extreme

ПК підключено через Ethernet до шлюзу і використовується для конфігурації LoRaWAN Network Server. Додаток для роботи з системою створюється в графічному середовищі Node-Red. Додаток буде приймати повідомлення від кінцевих пристроїв LoRaWAN і посилати їх назад (режим луни), відображаючи прийняті повідомлення в інтерфейсі Node-Red. Приклад використання Node-Red наведено на рис 3.9.

Сервер додатків (Application Server) може віддалено контролювати роботу кінцевих вузлів і збирати з них необхідні дані. Для зручності експлуатації можна скористатися хмарної платформою Antares, що дозволяє віддалено конфігурувати і

управляти базовими станціями і шлюзами Conduit. Разом з тим шлюзи ніяк не прив'язані до якого-небудь хмарного сервісу і можуть експлуатуватися автономно.

Якщо надалі буде потрібно використовувати більш складний додаток, користувач може перепрограмувати шлюз або базову станцію дистрибутивом mLinux з підтримкою Java, Ruby, Perl, Python, C/C ++, PHP, C#, JavaScript, а також попередньо встановленими SQLite (Database), Ligttpd (Web Server), BusyBox (Core Utilities).

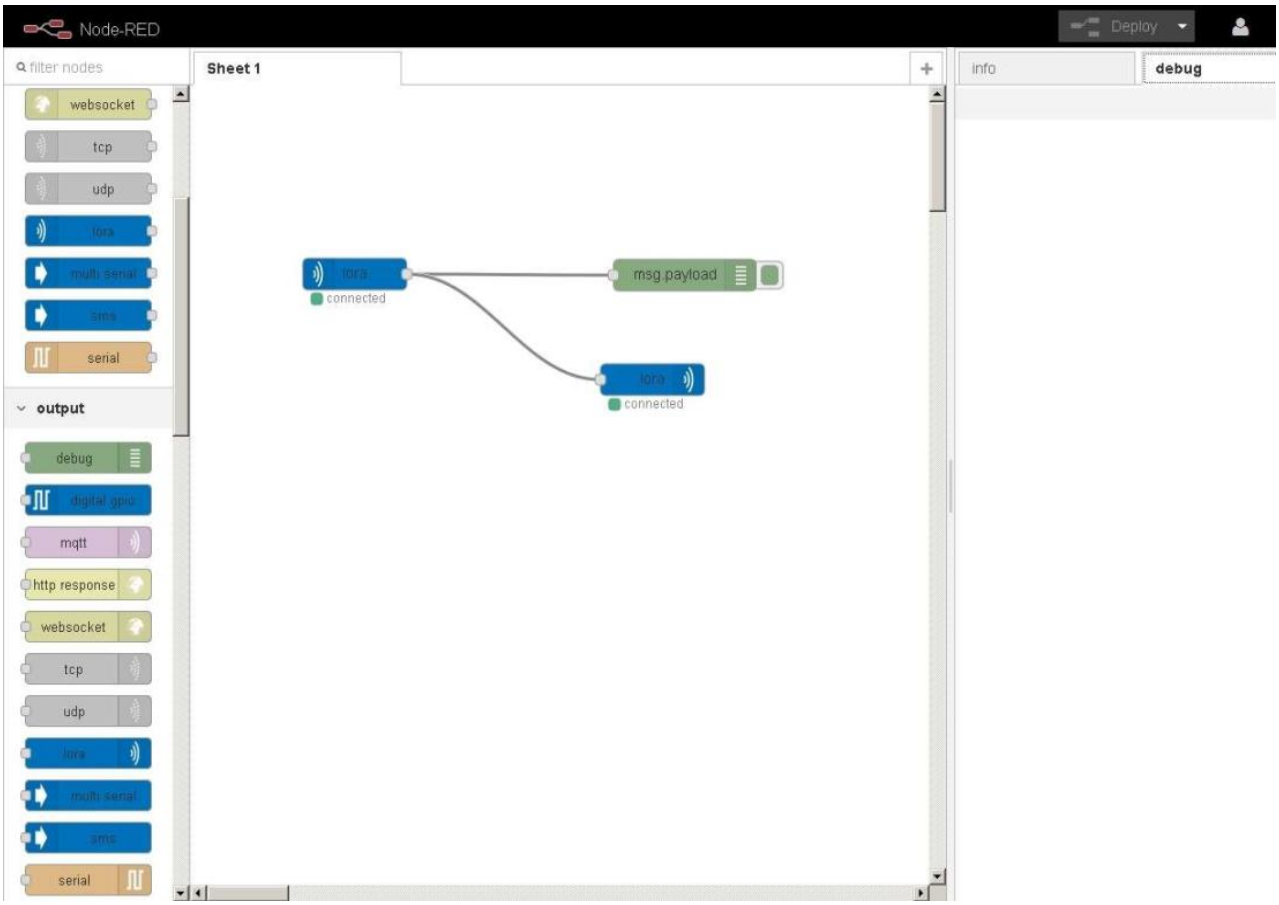

Рисунок 3.9 – Інтерфейсі Node-Red

Ціна ноутбука Lenovo ThinkPad X1 Extreme – 65000 грн.

Необхідна кількість – 1 шт.

3.8 Налаштування БСМ

На території НТУУ "КПІ ім. Ігоря Сікорського" безпроводова мережа LoRaWAN це шлюз (gateways), який пересилає повідомлення між кінцевими пристроями (end-devices) і центральним сервером (Network Server, NS), і характеризується "зірковою" топологією "star-of-stars".

Кінцеві вузли призначені для здійснення керуючих і вимірювальних функцій. Вони містять датчики контролю повітря SE81Z6GCN470-N з вбудованим керуючим елементом та датчики виявлення диму Артон СПД-3.3, що підключені до модему Вега SH-2. Для забезпечення світло-звукового сповіщення пожежі було обрано сирену С-03-12.

Обладнання, що отримує дані від кінцевих пристроїв за допомогою радіоканалу й передає їх у транзитну мережу – шлюз LoRaWAN Conduit. Шлюз і кінцеві пристрої утворюють мережну топологію типу "зірка" за допомоги антени W1063 діапазону 868 МГц.

Всі кінцеві пристрої LoRa та шлюз LoRa будуть живитися від джерела постійного струму, а при автономному режимі – від літієвих акумуляторів.

Для користування БСМ потрібно на початку налаштувати LoRaWAN Network Server, та створити додаток в графічному середовищі Node-Red, Antares буде служити хмарною платформою, а потім активувати кінцеві пристрої. Використовуємо для цього: шлюз Conduit от Multi-Tech, з встановленим модулем LoRa, антену W1063 діапазону 868 МГц та комп'ютер Lenovo ThinkPad X1 Extreme (ПК).

ПК підключимо через Ethernet до шлюзу і будемо використовувати для настройки/конфігурації останнього. Шлюз Conduit – це по суті та ж базова станція, але для використання всередині приміщень (виконання indoor).

За замовчуванням в шлюзі встановлений фіксований IP 192.168.2.1, логін – admin, пароль – admin. Після успішного введення пароля відразу переходимо до пункту меню Setup $\Rightarrow$ LoRa Network Server (рис. 3.10).

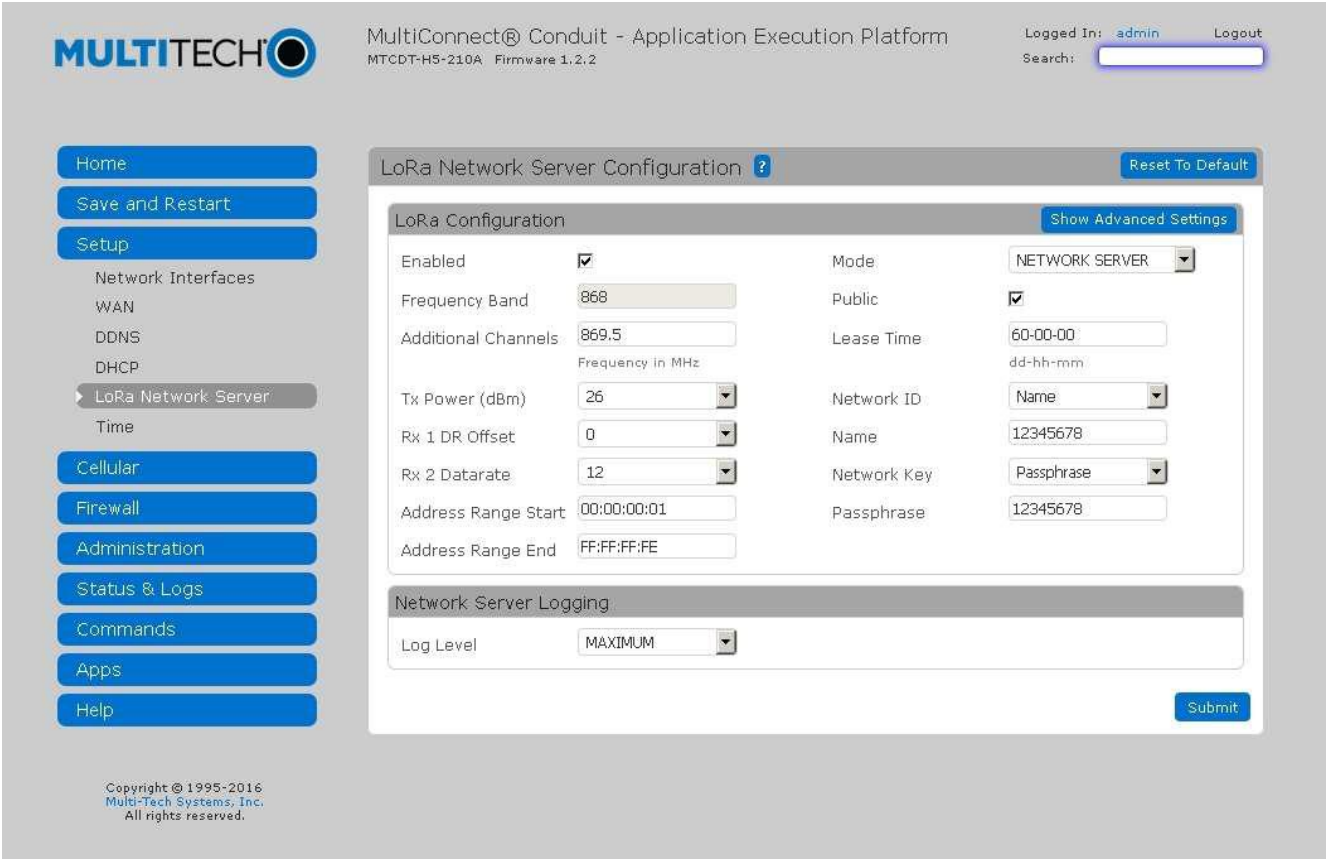

Рисунок 3.10 – Інтерфейсі налаштувань шлюзу Conduit

Налаштування:

1. Щоб включити сервер, поставимо галочку Enabled.

2. У шлюзу зконфігуровані 3 фіксовані канали шириною 125 кГц (центральні частоти – 868,1, 868,3 і 868,5 МГц), і можна конфігурувати п'ять додаткових каналів шириною 125 кГц і з відстанню між центральними частотами 200 кГц. Ці додаткові канали конфігуруються заданням центральної частоти додаткового діапазону в полі Additional Channels. Наприклад, якщо в полі Additional Channels ми задаємо значення 869,3, то отримуємо додаткові канали з наступними центральними частотами: 868,9; 869,1; 869,3; 869,5; 869,7 МГц.

Діапазони допустимих значень в полі Additional Channels – 863,5…867,5 і 869,1…869,5 (МГц).

3. Поле Mode може приймати два значення: NETWORK SERVER і PACKET FORWARDER. Якщо ми плануємо використовувати LoRaWAN Network Server на

самому шлюзі, то залишаємо значення NETWORK SERVER, а якщо, в хмарі – то PACKET FORWARDER. У нашому випадку залишаємо NETWORK SERVER.

4. Галочка Public відноситься до типу мережі – Public або Private. Якщо використовується тип Private (галка не встановлена), то швидше відбувається приєднання до мережі LoRaWAN кінцевих пристроїв (1…2 сек.), а також при бажанні можна відключати шифрування корисного навантаження.

5. Найбільш важливими є поля Network ID і Network Key. По суті вони відповідають значенням AppEUI і AppKey специфікації LoRaWAN, але так як використання досить довгих (8 і 16 байт відповідно) шістнадцяти-розрядних значень не завжди зручно, Multi-Tech вирішив надати користувачам право вибору. У шлюзах/БС Conduit AppEUI і AppKey можна задавати двома способами:

- в полі Network ID обираємо Name і нижче пишемо зрозуміле ім'я мережі (шлюз сам переведе наше ім'я в значення AppEUI);
- відповідним специфікації LoRaWAN – в полі Network ID обираємо EUI і записуємо шістнадцяти-розрядне значення AppEUI.

Значення AppEUI і AppKey в шлюзі/БС повинні бути значення, запрограмовані у кінцевих пристроях LoRaWAN.

6. Інші настройки залишимо.

Після конфігурації сервера LoRaWAN потрібно натиснути Save and Restart, щоб застосувати внесені зміни.

Потім можна знову увійти у систему і перейти в пункт меню Apps -> Node-Red, щоб створити демонстраційний додаток.

Після повторного введення логіна/пароля admin/admin (це вже для доступу до Node-Red) потрапляємо в Node-Red, рис. 3.11.

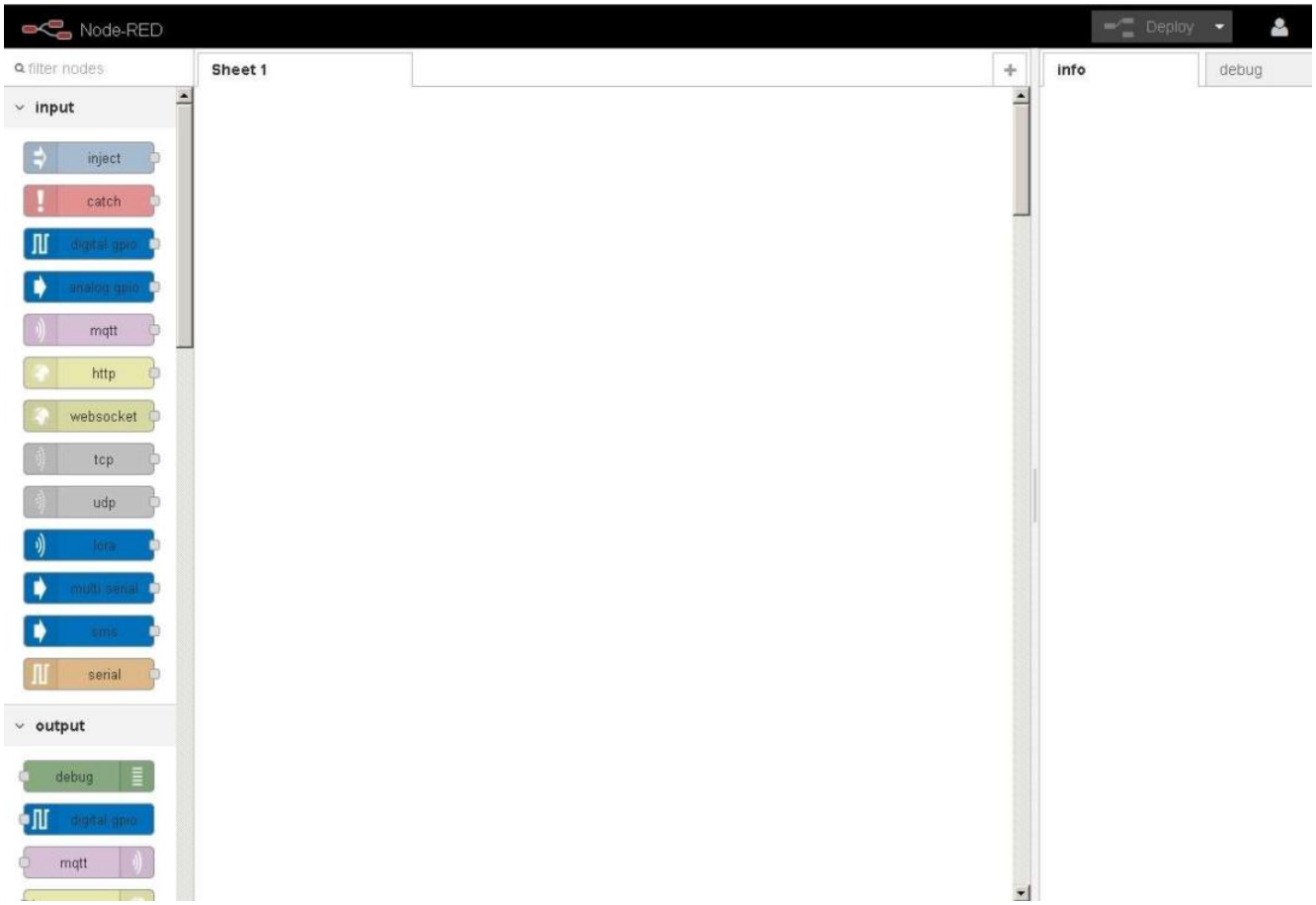

Рисунок 3.11 – Інтерфейс Node-Red

У лівій частині знаходяться вузли, які можна перетягувати в основне поле і з'єднувати між собою за допомогою миші. Для прикладу візьмемо з розділу Input вузол lora, а з розділу Output – вузли Debug і Lora, і з'єднаємо їх так, як показано на рис. 3.12.

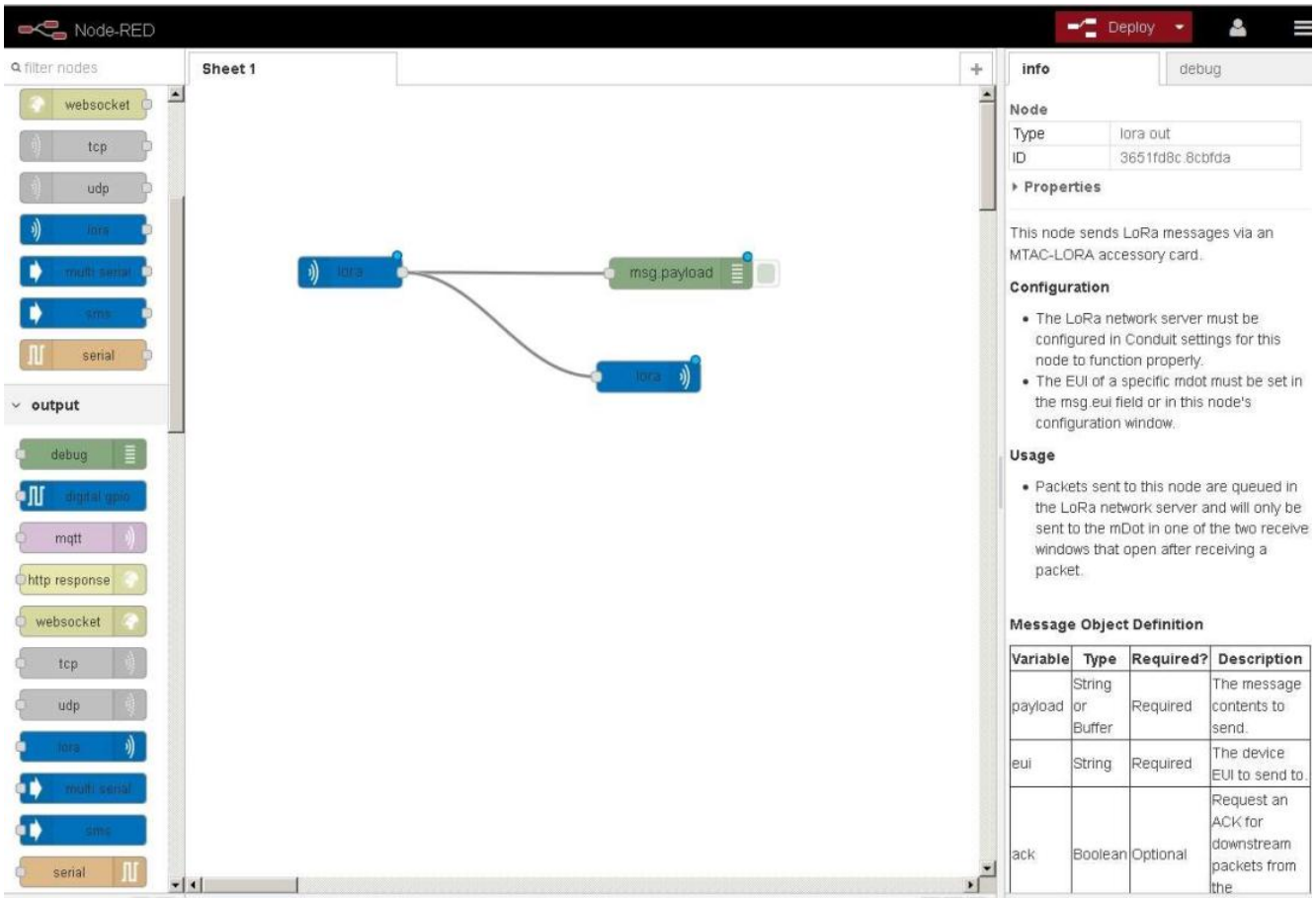

Рисунок 3.12 – З’єднання вузлів у додатку Node-Red

Натиснемо кнопку Deploy в верхньому правому куті вікна Node-Red – програма готова до роботи, рис. 3.13

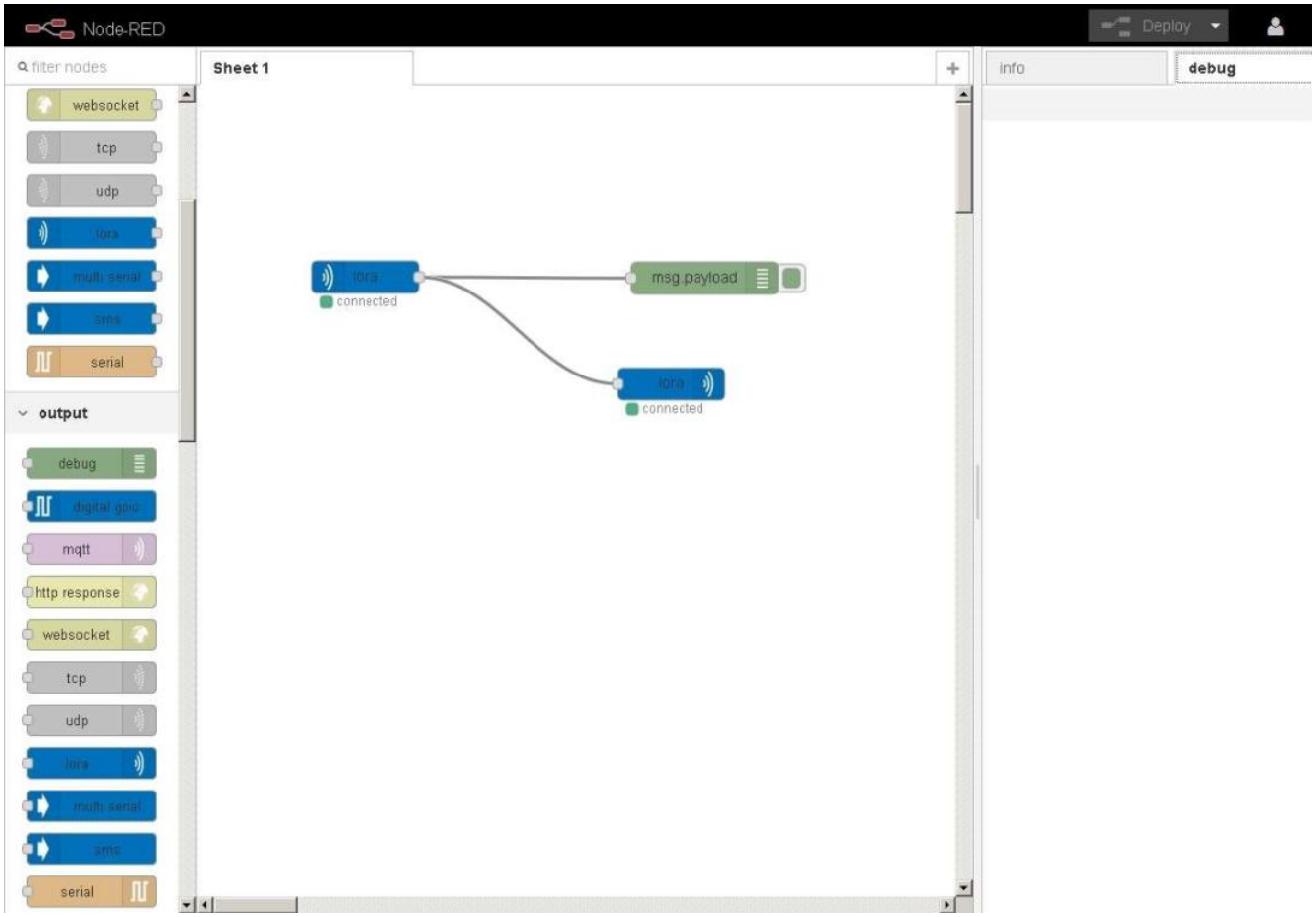

Рисунок 3.13 – Робоча программа у Node-Red

Тепер можна подивитися, що виходить при відправці повідомлень з пристрою LoRaWAN на шлюз Conduit. Після успішного прийому повідомлення від пристрою повинні отримати відповідь, яку було надіслано на цей пристрій, а також побачимо це повідомлення (Hello_Habroworld!) На вкладці debug в правій частині вікна Node-Red (завдяки підключеному вузлу debug), рис. 3.14.

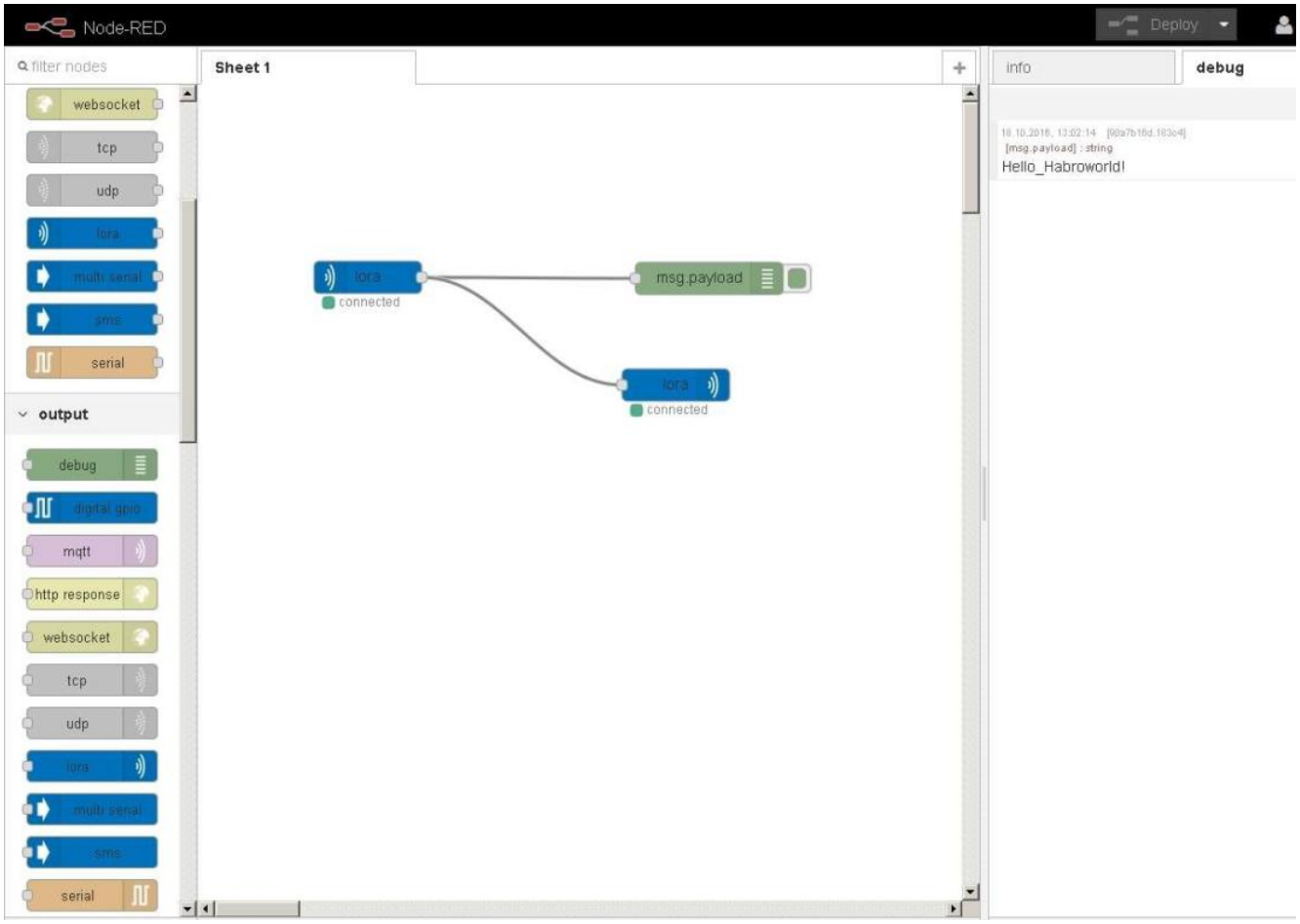

Рисунок 3.14 – Демонстрація отримання повідомлення у Node-Red

У демонстраційному прикладі отримані повідомлення луною відправляються назад, в реальної конфігурації їх можна без додаткових зусиль пересилати на певні порти TCP/UDP віддаленого сервера, посилати у вигляді повідомлень MQTT, SMS, e-mail, зберігати в файл, публікувати в Twitter, обробляти на шлюзі/БС та ін.

Дані про стан навколишнього середовища краще публікувати у відкритому доступі, як Twitter, а для термінового повідомлення про пожежу відправляти миттєві просиляння у вигляді SMS, а також система ввімкне світло-звукові сирени автоматично.

Щоб приєднатися до мережі LoRaWAN, кінцевий пристрій повинен пройти процедуру активації (End-Device Activation).

Специфікація передбачає два варіанти активації пристроїв: OTAA та ABP.

OTAA, Over-The-Air Activation (потрібно пройти процедуру приєднання (join procedure), під час якої виробляються сесійні ключі шифрування і адреса DevAddr).

ABP, Activation By Personalization (не потрібно проходити процедуру приєднання, ключі шифрування і адреса DevAddr записуються в пристрій заздалегідь (персоналізація пристрою)).

Після активації пристрій повинен містити наступні значення:

1. End-device address (DevAddr) – локальну адресу пристрою в даній мережі, 32 біта. DevAddr складається з двох полів: NwkID (ідентифікатор мережі, біти 31...25) і NwkAddr (мережеву адресу, біти 24...0).

2. Network session key (NwkSKey) – мережевий сесійний ключ, 128 біт, який використовується для розрахунку і перевірки поля MIC (message integrity code) повідомлень при обміні між кінцевим пристроєм та сервером мережі (Network Server), а також шифрування повідомлень MAC-рівня.

3. Application session key (AppSKey) – сесійний ключ, 128 біт, який використовується для шифрування даних на рівні додатку (між кінцевим пристроєм і сервером додатка).

4. Application identifier (AppEUI) – ідентифікатор додатку, 64 біта, який записується заздалегідь.

При активації OTAA термінал має проходити процедуру приєднання до мережі кожен раз, коли сесійної інформації (локальна адреса DevAddr, ключі NwkSKey, AppSKey) в пристрої немає, або вона неактуальна. Процедура приєднання завжди ініціюється кінцевим пристроєм і складається з двох повідомлень, якими обмінюються термінал і мережевий сервер: join request (пристрій → сервер) і join accept (сервер → пристрій).

"Активація шляхом персоналізації" означає, що в пристрій безпосередньо записуються значення DevAddr, NwkSKey і AppSKey (відбувається персоналізація пристрою). Згідно зі специфікацією, кожен пристрій має містити унікальні значення сесійних ключів NwkSKey і AppSKey, щоб компрометація цих значень,

що містяться в одному пристрої, не приводила до компрометації інших пристроїв мережі.

При такому способі активації кінцевого пристрою не потрібно проходити процедуру приєднання до мережі, відразу після включення пристрій готовий до передачі даних.

3.9 Розрахунок вартості БСМ

Таблиця 3.6 – Розрахунок вартості БСМ

Назва обладнання	Кількість	Ціна за одиницю (грн)	Загальна вартість (грн)
Шлюз LoRaWAN Conduit от Multi-Tech	1	14325	14325
Антена W1063	1	620	620
Вузол LoRaWAN Вега SH-2	1	2863	2863
Датчик диму IP40	129	236	30444
Датчик контролю повітря SE81Z6GCN470-N	129	600	77400
Світло-звукова сирена С-03-12	15	152	2280
Lenovo ThinkPad X1 Extreme	1	65000	65000
Сумарна вартість, грн	**192932**		

Висновки до розділу

Безпроводова мережа LoRaWAN являє собою сукупність шлюзів (gateways), які пересилають повідомлення між кінцевими пристроями (end-devices) і центральним сервером (Network Server, NS), і характеризується "зірковою" топологією "star-of-stars".

Для реалізації впровадження системи було обране надійне обладнання. Розраховано орієнтовну суму матеріальної частини проекту, що складає **192932** грн.

Кінцеві вузли призначені для здійснення керуючих і вимірювальних функцій. Вони містять датчики контролю повітря SE81Z6GCN470-N з вбудованим керуючим елементом та датчики виявлення диму Артон СПД-3.3, що підключені до модему Вега SH-2. Вузли включають передачу даних лише на деякий проміжок часу, по закінченню якого відкривається два тимчасові вікна для приймання даних. Решта часу прийомопередавачі кінцевих вузлів перебувають в неактивному стані, завдяки класу пристрою А. Для забезпечення світло-звукового сповіщення пожежі було обрано сирену С-03-12.

Обладнання, що отримує дані від кінцевих пристроїв за допомогою радіоканалу й передає їх у транзитну мережу – шлюз LoRaWAN Conduit от Multi-Tech. Транзитними мережами можуть виступати Ethernet, Wi-Fi, стільникові мережі й будь-які інші телекомунікаційні канали. Шлюз і кінцеві пристрої утворюють мережну топологію типу "зірка" за допомоги антени W1063 діапазону 868 МГц. Шлюз містить багатоканальні прийомопередавачі для обробки сигналів у декількох каналах одночасно або навіть, декількох сигналів в одному каналі. Відповідно, кілька таких пристроїв забезпечують зону покриття мережі й двонаправлене передавання даних між кінцевими вузлами й сервером.

Всі кінцеві пристрої LoRa та шлюз LoRa будуть живитися від джерела постійного струму, а при автономному режимі – від літієвих акумуляторів.

Сервер мережі ноутбук Lenovo ThinkPad X1 Extreme призначений для управління мережею: формуванням розкладу, адаптацією швидкості, зберіганням і обробкою прийнятих даних.

Сервер додатків може віддалено контролювати роботу кінцевих вузлів і збирати з них необхідні дані. Для зручності експлуатації можна скористатися хмарної платформою Antares, що дозволяє віддалено конфігурувати і керувати шлюзами Conduit, для аналізу даних краще експлуатувати Node-red.

4 РОЗРОБКА СТАРТАП ПРОЕКТУ

4.1 Опис ідеї проекту

Світ стрімко рухається назустріч новій епосі, відмінною рисою якої є поява технологій Інтернету речей. Звичні пристрої навчилися підключатися до мережі і обмінюються даними без участі людини. Програмна, апаратна, комунікаційна інфраструктура, а також "підключені" пристрої, що беруть участь в процесі обміну даними, об'єднуються в технологічну екосистему, яка дістала назву Інтернет речей. Динамічному поширенню Інтернету речей сприяє масова поява пристроїв, оснащених електронними компонентами, програмним забезпеченням і комунікаційними можливостями, які збирають і передають дані.

Актуальність роботи полягає у тому, що зі зростанням кількісті підключеної техніки в Інтернеті зростає потреба у безпроводових сенсорних мережах, що доцільно використовувати у критичних сферах застосування. Це дозволяє вирішити проблему передачі важливих даних або підтримки безпеки в приміщеннях для різних видів діяльності, як наслідок, підтримати безпечні умови роботи, де важливі наднадійні комунікації з малою затримкою.

Сутність стартапу полягає у впровадженні Інтернету речей на територію НТУУ "КПІ ім. Ігоря Сікорського" ФЕЛ у сферах критичного застосування, використовуючи технологію мережі LoRa, та у розроблені системи контролю ключових параметрів інфраструктури на території студмістечка НТУУ "КПІ ім. Ігоря Сікорського" на основі технології мережі LoRa з сенсорами для систем Інтернету речей, а далі у розповсюдженні аналогічних БСМ іншим університетам та приватним компаніям.

Проект втілення БСМ, як форма малого ризикового підприємництва, може набути широкого розповсюдження у світі через зниження бар’єрів входу в ринок, завдяки появі Інтернету, як інструменту комунікацій та збуту. Стало простіше

знаходити споживачів та інвесторів, займатись пошуком ресурсів, перетинати кордони між ринками різних країн.

Обґрунтування бізнес моделі стартапу:

- сегменти споживачів – масовий ринок;
- ціннісна пропозиція – легкість у використанні, сучасне рішення, новизна, надійність;
- канали збуту – однорівневий, з роздрібним торговцем;
- інтернет-маркетинг – свій сайт та вірусний маркетинг;
- ключові ресурси – постачання деталей для пристроїв;
- ключові види діяльності – виробництво та розробка ПО;
- ключові партнери – стратегічне співробітництво між не конкуруючими компаніями та компаніями які здійснюватимуть продаж.

4.2 Технологічний аудит ідеї проекту

Основна ідея проекту полягає в тому, що БСМ працює на основі технології мережі LoRa. Така технологія існує, але для використання потрібно окремо розроблювати та налаштовувати параметри мережі під місцевість розміщення.

Безпроводова мережа LoRaWAN являє собою сукупність шлюзів (gateways), які пересилають повідомлення між кінцевими пристроями (end-devices) і центральним сервером (Network Server, NS), і характеризується "зірковою" топологією "star-of-stars".

Середа розгортання мережі LoRa впливає на якість сигналу, особливо високий рівень щільності завад між шляхами передавання має найбільший вплив на погіршення якості сигналу. Коефіцієнт поширення і пропускна здатність основний фактор, який впливає на продуктивність мережі LoRa. Більш високий коефіцієнт розширення і більш низька смуга пропускання дозволяють збільшити дальність зв'язку і підвищити стійкість перед завадами. Мережа LoRa не може охопити весь кампус одним шлюзом, якщо розраховувати на всю територію НТУУ

"КПІ ім. Ігоря Сікорського". Параметри LoRa повинні бути налаштовані на оптимальну настройку для кожного місця розташування, оскільки різні настройки матимуть різне енергоспоживання.

Такий проект може бути технологічно реалізований при налаштовуванні параметрів мережі під місцевість розміщення.

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Маркетинговий аналіз – це перспектива реалізації запропонованих науково-технічних рішень та пропозицій, оцінювання можливостей їх ринкового впровадження.

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Підприємства з продажу систем пожежної безпеки або впровадження систем "Розумних" будинків, розташовані в Києві, є основними конкурентами. Підприємство з продажу систем пожежної безпеки пропонує такі послуги: створення попереднього проекту для установки пожежної сигналізації і систем оповіщення; установка пожежної сигналізації та систем оповіщення про пожежу; подальше обслуговування і ремонт пожежної сигналізації та систем оповіщення про пожежу. Ці послуги не мають таких характеристик: IoT-моніторинг та використання технологій мереж LoRa. Підприємство з впровадження систем "Розумних" будинків пропонує такі послуги: створення попереднього проекту для установки Інтернету речей, установка IoT-моніторингу та використання технологій мереж LoRa. Вони користуються попитом серед споживачів завдяки якості і високого рівня довіри до компанії та додаткових послуг.

Конкуренти мають можливість проводити агресивну цінову політику завдяки дешевим поставкам та відсутності альтернативних пропозицій на ринку.

Згідно з даними, отриманими з Інтернету, місцевий ринок послуг генерує щорічні продажі на суму 500 тис. доларів. За нашими оцінками, наша компанія зможе зайняти 13 % ринку протягом наступних 3 років.

4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку – опис цільових груп потенційних споживачів. Формування портрета цільової аудиторії – важливий етап в розробці бізнес-плану стартапу. До цільової аудиторії нашої компанії належать чоловіки і жінки у віці 30 років, що перебувають у шлюбі, з вищою освітою, з рівнем доходу більше середнього, що працюють на умовах повної зайнятості. Вони проживають у великих містах, як правило, часто користуються інтернетом.

За результатами аналізу потенційних груп споживачів цільова група, для пропонування послуг – інші університети та приватні компанії. Стратегія охоплення ринку – диференційований маркетинг, так як компанія працює із кількома сегментами груп споживачів, розробляючи для них окремо програми ринкового впливу.

4.5 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для реклами і продажу використаємо вірусний маркетинг, за допомогою власного сайту та сторінки в Instagram. 86,6% американських представників малого та середнього бізнесу вважають сайт компанії головним інструментом інтернет-маркетингу.

Наступним кроком є визначення оптимальної системи збуту. Канал збуту буде однорівневим з посередником. На споживчих ринках цим посередником зазвичай буває роздрібний торговець, а на ринках товарів промислового призначення – агент по збуту або брокер.

Після формування маркетингової моделі товару слід особливо зазначити – чим саме проект буде захищено від копіювання. Це буде організовано за рахунок захисту ідеї товару та інтелектуальної власності, та комплексного поєднання властивостей і характеристик.

4.6 Фінансово-економічний аналіз та оцінка ризиків проекту

Для реалізації впровадження системи було обране надійне обладнання. Перелік необхідних матеріалів і розрахунок вартості БСМ на табл. 4.1. Розраховано орієнтовну суму матеріальної частини проекту, що складає 192932 грн.

Таблиця 4.1 – Розрахунок вартості БСМ

Назва обладнання	Кількість	Ціна за одиницю (грн)	Загальна вартість (грн)
Шлюз LoRaWAN Conduit от Multi-Tech	1	14325	14325
Антена W1063	1	620	620
Вузол LoRaWAN Вега SH-2	1	2863	2863
Датчик диму IP40	129	236	30444
Датчик контролю повітря SE81Z6GCN470-N	129	600	77400
Світло-звукова сирена С-03-12	15	152	2280
Lenovo ThinkPad X1 Extreme	1	65000	65000
Сумарна вартість	**192932**		

Розроблення проекту передбачає здійснення кроків, в яких визначають принципи організації виробництва, фінансовий аналіз та аналіз ризиків.

Зазвичай компанія, що займається пожежною сигналізацією, пропонує наступні послуги: створення попереднього проекту для установки пожежної сигналізації і систем оповіщення; установка пожежної сигналізації та систем оповіщення про пожежу; подальше обслуговування і ремонт пожежної сигналізації та систем оповіщення про пожежу. За даними з Інтернету оснащення протипожежної системи без вбудованої системи IoT-мониторингу коштуватиме 150 тис. грн. за проектування та монтаж, а також додатково потребує 680 грн. у місяць за обслуговування, що не вигідно у порівнянні з БСМ на основі LoRa, яка не потребує додаткового обслуговування.

Економічні показники та ризики підраховані та занесені в табл. 4.2 – 4.4.

1. Сума інвестицій у проект становить 200 тис. грн.

2. Дисконтовані грошові потоки в результаті реалізації проекту становитимуть 217,25 тис. грн..

3. Чиста теперішня вартість проекту 217,25 – 200,0 = 17,25 тис. грн. Оскільки, NPV > 0, інвестиційний проект є вигідним для підприємства-інвестора. За три роки функціонування проекту грошовий потік не лише задовольняє очікування інвестора у відношенні щодо одержання доходу, а й перевищують очікувані доходи на 17,25 тис. грн.

4. Термін окупності інвестицій: ТО = 2,24 роки.

5. Внутрішня норма рентабельності. IRR = 0,18, або при ставці 18% сумарні дисконтовані вигоди дорівнюють сумарним дисконтованим витратам. Тобто IRR є ставкою дисконту, при якій NPV проекту дорівнює нулю.

6. Коефіцієнт вигід/витрат дорівнює 2,54. Отже на 1 грн. теперішньої вартості вкладених коштів у проект підприємство отримає 2,54 грн. теперішньої вартості доходу.

7. Індекс прибутковості. 17,25/200,0 = 0,086. Отже, PI > 0 і проект є ефективним.

Таблиця 4.2 – Розрахунок економічної складової проекту

Показник	**0 рік**	**1 рік**	**2 рік**	**3 рік**
Сума інвестицій, тис. грн.	200,0	-	-	-
Виручка від реалізації, тис. грн.	-	80,0	150,0	300,0
Витрати на експлуатацію проекту, тис. грн.	-	100,0	40,0	45,0
Ставка дисконту, %	-	18	18	18
Грошові потоки, тис. грн.	-	-20	110	255
Дисконтовані грошові потоки, тис. грн.	-	-16,95	79,00	155,20
Дисконтовані вигоди, тис. грн.	-	67,80	107,73	182,59
Дисконтовані витрати, тис. грн.	-	84,75	28,73	27,39

Таблиця 4.3 – Показники економічної складової проекту

Показник	Скорочення	Значення
Вартість проекту за 3 рока	PV	217,25 тис. грн.
Чистий дисконтований дохід	NPV	17,25 тис. грн.
Коефіцієнт вигід-витрат	BCR	2,54
Середню рентабельність інвестицій	R	51,41%
Індекс прибутковості проекту	PI	0,086
Вигідність		1

Таблиця 4.4 –Економічні ризики проекту

Ризик	Небезпека	Ймовірність	Важливість
Некваліфікований персонал	5	0,01	0,02
Хакерські атаки	1	0,1	0,05
Зміни законодавства/податкової в інших країнах	2	0,2	0,1
Зміна у торгових відносинах з іншими країнами	8	0,01	0,1
Непостійні клієнти	1	0,8	0,5
Неприйняття ідеї	10	0,1	1

Висновки до розділу

На даний момент не існує схожих проектів БСМ розгорнутих у ВУЗах країни. Система БСМ на основі технології LoRa на території НТУУ "КПІ ім. Ігоря Сікорського" економічно вигідна та цікава, як нова сучасна ідея в IoT сфері.

На основі отриманих даних можна впроваджувати аналогічні БСМ на різноманітні об’єкти та використовувати їх у критичних сферах застосування. Це дозволяє вирішити проблеми передачі важливих даних або підтримки безпеки в приміщеннях для різних видів діяльності, як наслідок, підтримати безпечні умови роботи, де важливі наднадійні комунікації з малою затримкою.

Проект впровадження системи БСМ на основі технології LoRa комерційно вигідний та має можливість окупити впровадження на масовому ринку за 2,5 роки. Завдяки легкості у використанні, сучасним рішенням, новизні та надійності доцільно реалізувати проект та впровадити на ринок, використовуючи інтернет-маркетинг.

ВИСНОВКИ

Для забезпечення умов роботи та підтримки безпеки в приміщеннях критичних сфер використання необхідно впроваджувати безпроводові сенсорні мережі.

У результаті виконання роботи отримано такі висновки:

1. Впровадження Інтернету речей на територію НТУУ "КПІ ім. Ігоря Сікорського" доцільна, тому що у університеті важлива підтримка безпеки в приміщеннях для різних видів діяльності, для раннього виявлення джерела пожежі та контролю температури повітря в лекційних приміщеннях, додатково IoT використаємо для моніторингу стану якості повітря навколишнього середовища.

2. Проаналізувавши параметри технологій Інтернету речей, найбільш оптимальним і збалансованим рішенням для БСМ може бути використання технології LoRaWAN.

3. Середа розгортання мережі LoRa впливає на якість сигналу, особливо високий рівень щільності завад між шляхами передавання має найбільший вплив на погіршення якості сигналу. Коефіцієнт поширення і пропускна здатність основний фактор, який впливає на продуктивність мережі LoRa. Більш високий коефіцієнт розширення і більш низька смуга пропускання дозволяють збільшити дальність зв'язку і підвищити стійкість перед завадами. Мережа LoRa не може охопити весь кампус одним шлюзом, якщо розраховувати на всю територію НТУУ "КПІ ім. Ігоря Сікорського". Параметри LoRa повинні бути налаштовані на оптимальну настройку для кожного місця розташування, оскільки різні настройки матимуть різне енергоспоживання.

4. Спроектована структурна та функціональна схема БСМ на основі технології LoRaWAN, план об’єкту та розташування обладнання на території корпусу ФЕЛ. Розраховано орієнтовну суму матеріальної частини проекту, що складає 192932 грн.

5. Мережа LoRa складається з кінцевих пристроїв, шлюзу, серверу мережі та серверу додатків. Кінцеві пристрої LoRa являють собою комбінацію вузлів LoRa та датчиків, що підходить для моніторингу стану рівнів якості повітря та виявлення диму. Всі кінцеві пристрої LoRa та шлюз LoRa будуть живитися від джерела постійного струму, а при автономному режимі від літієвих акумуляторів.

6. Для забезпечення максимальної відстані покриття і підвищення чутливості зв'язку у кампусі ФЕЛ використовують коефіцієнт розширення 12, ширину смуги 125 кГц, антену діапазоном 868 МГц, потужність передавача 20 дБм. На практиці скористаємося Antares, як хмарним сервісом для збереження даних і відображення, для аналізу даних краще експлуатувати Node-red.

7. На даний момент не існує схожих проектів БСМ розгорнутих у ВУЗах країни. Система БСМ на основі технології LoRa на території НТУУ "КПІ ім. Ігоря Сікорського" економічно вигідна та цікава, як новий сучасний проект в IoT сфері.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. "Интернет всего" (Internet of Everything, IoE). URL: https://www.it.ua/ru/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot. (Дата звернення: 03.12.2020).

2. C. Noris, Функціональна безпека частина 6 з 6. Оцінювання показників функціональної безпеки і надійності, [Online]. Available: https://habrahabr.ru/post/323776. (Дата звернення: 03.12.2020).

3. Palagin O.V., Romanov V.O., Galelyka I.B., Voronenko O.V., Brayko Yu.O., Imamutdinova R.G. Wireless sensor network for precision farming and environmental protection//Information theories and applications. - Vol.24, Number 1. - 2017. P. 19-34.

4. Лінії зв'язку. Organization of computer networks. URL: http://dubovenkolk.blogspot.com/2017/10/2.html. (Дата звернення: 03.12.2020).

5. Комп’ютерна інженерія. Новітні технології для сучасних людей. Лінії зв'язку і канали передачі даних. URL: https://oksim.top/index.php/komp-yuterni-tekhnologiji/peredacha-danikh/158-liniji-zv-yazku-i-kanali-peredachi-danikh. (Дата звернення: 03.12.2020).

6. Кабельні лінії зв'язку. Учбові матеріали та реферати URL: http://um.co.ua/1/1-6/1-65982.html. (Дата звернення: 03.12.2020).

7. Ipkey: Що таке бездротові технології? Червень 2017. URL: https://ipkey.com.ua/uk/faq/965-wireless-technologies.html. (Дата звернення: 03.12.2020).

8. L. Alliance, “White Paper: A Technical Overview of LoRa and Lorawan,” 2015. [Online]. Available: https://www.tuv.com/media/corporate/products_1/electronic_components_and_laser/TUeV_Rheinland_Overview_LoRa_and_LoRaWANtmp.pdf. (Дата звернення: 03.12.2020).

9. Daikin-conditions: Що таке 4 ж. Категоріювання приймальних пристроїв. URL: https://daikin-conditions.ru/uk/nalogi/chto-takoe-4-zh-kategorirovanie-priemnyh-ustroistv/. (Дата звернення: 03.12.2020).

10. A. Zourmand, N. W. Sheng, A. L. K. Hing, and M. AbdulRehman, “Human Counting and Indoor Positioning System Using WiFi Technology,” in Automatic Control and Intelligent Systems, Shah Alam. IEEE, October 2018, pp. 142–147. [Online]. Available: https://www.researchgate.net/publication/330253846_Human_Counting_and_Indoor_Positioning_System_Using_WiFi_Technology. (Дата звернення: 03.12.2020).

11. Nokia: LTE evolution for IoT connectivity | Open Ecosystem Network, Available at: http://bit.ly/Nokia2DsnEj6 [Accessed 23 Apr. 2019]. (Дата звернення: 03.12.2020).

12. Ukrbukva: Бездротові системи передачі даних. URL: https://ukrbukva.net/page,2,99789-Besprovodnye-sistemy-peredachi-dannyh.html. (Дата звернення: 03.12.2020).

13. L. Alliance, “White Paper: A Technical Overview of LoRa and Lorawan,” 2015. [Online]. Available: https://www.tuv.com/media/corporate/products_1/electronic_components_and_laser/TUeV_Rheinland_Overview_LoRa_and_LoRaWANtmp.pdf. (Дата звернення: 03.12.2020).

14. Cabel-set: Устаткування системи розумний будинок. URL: https://cabel-set.ru/uk/stroitelstvo/sobrat-umnyi-dom-kak-sdelat-umnyi-dom-svoimi-rukami-varianty/.(Дата звернення: 03.12.2020).

15. V. Romanov, I. Galelyuka; Сенсоры И Датчики: Wireless Sensor Networks For Agriculture And Environmental Protection [Number 2, Apr. 2017].

16. P. Dhaker; Технологии Интернета Вещей: Wireless Water Quality Monitoring System [Number 2, Apr. 2020].

17. H. Hashemi; В Помощь Разработчику Электронной Аппаратуры: Remote Sensing Using A High Precision Instrumentation Amplifier [Number 3, Apr. 2019].

18. C. Norris; В Помощь Разработчику Электронной Аппаратуры: Functional Safety In A Data Acquisition System [Number 4, Oct. 2018].

19. A. Zourmand, N. W. Sheng, A. L. K. Hing, and M. AbdulRehman, “Human Counting and Indoor Positioning System Using WiFi Technology,” in Automatic Control and Intelligent Systems, Shah Alam. IEEE, October 2018, pp. 142–147. [Online]. Available: https://www.researchgate.net/publication/330253846_Human_Counting_and_Indoor_Positioning_System_Using_WiFi_Technology. (Дата звернення: 03.12.2020).

20. C. Wongeun, C. Yoon-Seop, J. Yeonuk, and S. Junkuen, “Low-Power LoRa Signal-Based Outdoor Positioning Using Fingerprint Algorithm,” Goe- Information, vol. 7, no. 11, pp. 440–455, 2018. [Online]. Available: 10.3390/ijgi7110440; https://www.mdpi.com/2220-9964/7/11/440/pdf. (Дата звернення: 03.12.2020).

21. J. Teel, “Bluetooth or WiFi – Which is Best for Your New Wireless Product?” 2018. [Online]. Available: https://predictabledesigns.com/whattypeof-wireless-is-right-for-your-product-bluetooth-wifi/. (Дата звернення: 03.12.2020).

22. L. Alliance, “White Paper: A Technical Overview of LoRa and Lorawan,” 2015. [Online]. Available: https://www.tuv.com/media/corporate/products_1/electronic_components_and_laser/TUeV_Rheinland_Overview_LoRa_and_LoRaWANtmp.pdf. (Дата звернення: 03.12.2020).

23. S. R. Sharan, W. Y. Qiao, and H. Seung-Hoon, “A survey on LPWA technology: LoRa and NB-IoT,” ICT Express, vol. 3, no. 1, 2017. [Online]. Available: 10.1016/j.icte.2017.03.004. (Дата звернення: 03.12.2020).

24. E. Notes, “LoRa Physical Layer & RF Interface,” 2018. [Online].

25. Available: https://www.electronics-notes.com/articles/connectivity/lora/radio-rf-interface-physical-layer.php. (Дата звернення: 03.12.2020).

26. M. Saari, A. M. bin Baharudin, P. Sillberg, S. Hyrynsalmi and W.Yan, "LoRa — A survey of recent research trends," 2018 41st International Convention on

Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018, pp. 872-877.

27. “Why LoRa?” [Online]. Available: https://www.semtech.com/lora/whylora. (Дата звернення: 03.12.2020).

28. Про університет: КПІ ім. Ігоря Сікорського. Лідер технічної освіти України. URL: https://kpi.ua/kpi_about. (Дата звернення: 03.12.2020).

29. LoRa Alliance Technical committee, “Core LoRaWAN™ Specification” Version 1.1, October 2017.

30. A. Zourmand, C. W. Hung, A. L. K. Hing, and M. AbdulRehman, “Internet of Things (IoT) using LoRa technology” in International Conference on Automatic Control and Intelligent Systems IEEE, June 2019, Selangor, Malaysia.

31. Cattani Marco, A. Boano Carlo and Römer Kay, "An Experimental Evaluation of the Reliability of LoRa Long-Range Low-Power Wireless Communication", Journal of Sensor and Actuator Networks, vol. 6, no. 2, pp. 7, Jun. 2017.

32. L. Alliance, “White Paper: A Technical Overview of LoRa,” 2019. [Online]. https://lora-alliance.org/sites/default/files/2019-06/cr-lora-102_lorawanr_and_nb-iot.pdf. (Дата звернення: 03.12.2020).

33. Вега SH-2 – Універсальний модем LoRaWAN®/Nb-IoT. http://iotvega.com/product/sh2. (Дата звернення: 03.12.2020).

34. Універсальний модем ВЕГА SH-2. Інструкція з експлуатації. http://iotvega.com/content/ru/si/sh2/01-%D0%92%D0%95%D0%93%D0%90%20SH-2%20%D0%A0%D0%9F_rev%2004.pdf. (Дата звернення: 03.12.2020).

Додаток А

ABSTRACT

ABSTRACT

This paper provides a comparative analysis of existing IoT system using LoRa technology on the territory of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". IoT projects, solutions and deployments need more than the connected physical objects and the data they ‘sense’ and capture. The physical ‘things’ and sensors/technologies in IoT devices, assets and things in IoT, consumer IoT, enterprise IoT and Industrial IoT (IIoT) also need technology to communicate about their internal state and/or external environment.

LoRa is the new communication technology under the Low Power Wide Area Network (LPWAN). It emphasizes on the long-range communication with the high receiving sensitivity ability which allows it to work under the noise interference or noise floor effectively. The range of communication has become the critical part on most of the IoT system, especially in Wi- Fi and Bluetoothbased IoT system. With the emergence of LoRa technology, further improvements to applications of the Internet of Things (IoT) can be realized.

The structural and functional scheme of wireless sensor network on the basis of LoRaWAN technology, the plan of object and an arrangement of the equipment in the territory of the FEL case is designed. The estimated amount of the material part of the project, which is 192932 UAH.

LoRa network consists of end devices, a gateway, a network server, and an application server. LoRa end devices are a combination of LoRa components and sensors that are suitable for monitoring air quality levels and detecting smoke. All LoRa end devices and the LoRa gateway will be powered by a DC power source, and in stand-alone mode by lithium batteries.

To provide the maximum coverage distance and increase the sensitivity of the connection on the FEL campus, an expansion factor of 12, a bandwidth of 125 kHz, an antenna in the 868 MHz band, and a transmitter power of 20 dBm are used. In practice,

we will use Antares as a cloud service for data storage and display, for data analysis it is better to operate Node-red.

Додаток Б

ТЕХНІЧНЕ ЗАВДАННЯ

на магістерську дисертацію

"Особливості використання засобів інтернету речей у сферах критичного застосування"

1 Назва роботи

Особливості використання засобів інтернету речей у сферах критичного застосування

2 Підстави для виконання

Робота проводиться на підставі завдання на магістерську дисертацію відповідно до наказу № 3241-с від 05.11.2020 р.

3 Мета та актуальність роботи

Метою роботи є аналіз можливості впровадження Інтернету речей на територію НТУУ "КПІ ім. Ігоря Сікорського" ФЕЛ використовуючи технологію мережі LoRa, розробка архітектури системи підключення мережі LoRa та запропонування конфігурації безпроводової сенсорної мережі LoRa, розгорнутої у кампусі.

Актуальність дослідження полягає у тому, що зі зростанням кількісті підключеної техніки в Інтернеті зростає потреба у безпроводових сенсорних мережах, що доцільно використовувати у критичних сферах застосування. Це дозволяє вирішити проблему передачі важливих даних або підтримки безпеки в приміщеннях для різних видів діяльності, як наслідок, підтримати безпечні умови роботи, де важливі наднадійні комунікації з малою затримкою.

4 Основні технічні вимоги до виконання роботи

Надійність БСМ залежить від параметрів її компонентів і параметрів середовища, в якому мережі експлуатуються. Надійність мережі залежить від формату, швидкості передавання даних, надійності апаратних засобів, та від

зовнішніх факторів: електромагнітних завад, характеру місцевості, на якому розповсюджуються радіохвилі, дальності передавання, організації роботи мережі в умовах дії активних і пасивних перешкод.

Сучасна система управління БСМ має забезпечувати доступ до такої інформації:

- якості зв'язку за рівнем переданих сигналів;
- відсотку успішно прийнятих-переданих пакетів;
- кількості вузлів без альтернативних маршрутів приймання передавання даних;
- станом вузла і рівнем батарейного живлення.

5 Вимоги до технологічності

Пристрій повинен бути виконаний на елементній базі широкого застосування та відкритих стандартах і технологіях. Конструкція пристрою має передбачати багатократну заміну комплектуючих за необхідності. Пристрій має володіти вібро- та ударостійкістю до пошкоджень та захищений від стороннього проникнення.

6 Вимоги до рівня уніфікації

В конструкції необхідно намагатись максимально використовувати стандартні компоненти та уніфіковані вироби, а також запозичені складальні одиниці та деталі.

7 Вимоги до безпеки

По відношенню до безпеки пристрій, що працює повинен відповідати вимогам ДСТУ 4113-2001 і забезпечувати електробезпеку, пожежну безпеку,

механічну надійність та інші вимоги при монтажі, експлуатації, обслуговуванні і ремонті.

8 Економічні показники

Розроблювальний пристрій повинен бути ефективним по відношенню до його виробництва з економічної точки зору. Схемні рішення повинні мати мінімальну вартість реалізації.

9 Стадії та етапи розробки

Розробка виконується в один етап.

10 Порядок приймання роботи

Робота приймається Державною екзаменаційною комісією.

Додаток В

План об'єкта

Додаток Г

Структурна схема

Змін.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Макаренко Ю.В.			Структурна схема системи контролю критичних параметрів підключення мережі LoRa	Літ.	Аркуш 114 / Аркушів
Перев.		Макаренко В.В.					
Реценз.						НТУУ "КПІ ім. Ігоря Сікорського" ФЕЛ, ДВ-92 мп	
Н. Контр.							
Затв.							

Додаток Д

Схема функціональна

Змін.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Макаренко Ю.В.			Функціональна схема системи збору та контролю даних безпроводової сенсорної мережі	Літ.	Аркуш 116 / Аркушів
Перев.		Макаренко В.В.					
Реценз.						НТУУ "КПІ ім. Ігоря Сікорського" ФЕЛ, ДВ-92 мп	
Н. Контр.							
Затв.							