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 654.9

«До захисту допущено»
Завідувач кафедри
С.А. Найда
(ініціали, прізвище)
“ 16” грудня 2021 р.

Магістерська дисертація

спеціальність 171 Електроніка
(код і назва спеціальності)

на тему: «Система безпеки з використанням технології LoRa»

Виконав: студент II курсу, групи ДВ-01мп
(шифр групи)
Бельдягіна Анна Владиславівна
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доцент, к.т.н., доц. Оникієнко Ю. О.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент доцент каф. ЕІ, к.т.н., доц. Іванько К.О.
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)
(підпис)

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

Студент
(підпис)

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Інститут/факультет Факультет електроніки
(повна назва)

Кафедра Акустичних та мультимедійних електронних систем
(повна назва)

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

Спеціальність (спеціалізація) 171 Електроніка
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
С.А. Найда
(ініціали, прізвище)
«_7_»_вересня____2021_ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Бельдягіна Анна Владиславівна
(прізвище, ім'я, по батькові)

1. Тема дисертації Система безпеки з використанням технології LoRa

науковий керівник дисертації Оникієнко Юрій Олексійович, к.т.н., доц. ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету №3666-с від 03.12.2021

2. Строк подання студентом дисертації 12.12.2021 р.

3. Об'єкт дослідження безпроводові системи безпеки як елемент IoT.

4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою) апаратне забезпечення та програмне забезпечення, безпроводові системи безпеки.

5. Перелік завдань, які потрібно розробити:
аналіз архітектури системи безпеки, аналіз існуючих типів системи безпеки, аналіз апаратного та програмного забезпечення IoT.

6. Перелік графічного (ілюстративного) матеріалу комплект презентацій з матеріалами проведеного дослідження та застосування технології NB-IoT.

7. Орієнтовний перелік публікацій Yuri Onykiienko, Pavlo Popovych, Anastasiia Mitsukova, Anna Beldyagina and Roman Yaroshenko “LoRa Evaluation for University Campus in Urban Conditions” IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), September 21 - 25, Lviv, 2021

8. Консультанти розділів дисертації*

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

9. Дата видачі завдання 7. 09.2020 р

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Огляд літературних джерел	01.09.2021-15.09.2021	виконано
2	Написання перших двох розділів.	15.09.2021-25.10.2021	виконано
3	Аналіз безпроводових систем безпеки. Створення власної системи.	26.10.2021-27.11.2021	виконано
4	Оформлення розділів диплому. Оформлення висновків та переліку літературних посилань.	28.11.2021-06.12.2021	виконано
5	Підготовка та оформлення презентації для доповіді	07.12.2021-14.12.2021	виконано

Студент _____ А.В. Бельдягіна
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Ю.О. Оникієнко
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника

УДК 654.9

РЕФЕРАТ

Бельдягіна А.В. Система безпеки з використанням технології LoRa: магістерська дис. : 171 Електроніка / Бельдягіна Анна Владиславівна. – Київ, 2021. – 92 с.

Ключові слова: безпека, бездротові охоронні системи, бездротові сенсорні мережі, LoRa**.**

Актуальність дослідження.

Бездротові системи безпеки відрізняються рядом суттєвих переваг, оскільки відсутність проводів значно спрощує монтаж і дозволяє розміщувати їх в будь-якому зручному місці, а злочинці не зможуть дезактивувати такі відеокамери спостереження або датчики, перерізавши їх кабелі. Завдяки вказаним перевагам попит на бездротові системи безпеки вище, ніж на традиційні системи безпеки.

Бездротові системи безпеки використовують найсучасніші технології передачі даних та технології енергозбереження. Більшість компонентів системи безпеки, наприклад, охоронні датчики, працюють від акумулятора. Кінцеві пристрої використовують радіочастотні технології для зв’язку з централлю. Централі мають вихід в Інтернет.

Однак бездротові системи безпеки мають і певні недоліки: вища ціна та необхідність заміни батарей. Також необхідно контролювати якість зв’язку.

Вибрана тема актуальна тому що:

- бездротові системи безпеки набирають все більшу популярність;
- радіопротокол для передачі даних має велике значення для енергоефективності, зручності користування, можливості системи бути стійкою до завад.

Метою роботи є створення системи безпеки з покращеними функціональними характеристиками, а саме з використанням безпроводового каналу зв’язку на основі технології LoRa.

Об’єкт дослідження – програмне та апаратне забезпечення для систем безпеки.

Предмет дослідження – радіопротоколи для передачі даних між кінцевими пристроями та централлю в системах безпеки.

Методи дослідження – теоретично-аналітичний і практичний аналіз радіопротоколів для передачі даних між кінцевими пристроями та централлю в системах безпеки.

Наукова новизна отриманих результатів: оцінено вплив особливостей функціонування технології LoRa на роботу каналу передачі даних системи безпеки.

Практичне значення одержаних результатов: запропоновано варіант системи безпеки, яка базується на технології LoRa, і має ряд суттєвих переваг перед конкуруючими системами. Практичну цінність роботи підтверджено компанією Ajax Systems.

Апробація результатів дисертації: Доповідь на IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), September 21 - 25, Lviv, 2021.

ABSTRACT

Beldiahina Anna. Security system using LoRa technology: master's thesis: 171 Electronics. Kyiv, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, 2021. 92 p.

Keywords: security, wireless security systems, wireless sensor networks, LoRa.

Relevance of research.

Wireless security systems have a number of significant advantages, as the lack of wires greatly simplifies installation and allows you to place them in any convenient location, and criminals will not be able to deactivate such surveillance cameras or sensors by cutting their cables. Given these facts, the demand for them is higher than the demand for traditional security systems, and continues to grow. Wireless security systems are relatively new solutions that use state-of-the-art data transmission and energy-saving technologies. Most components of the security system, such as security sensors, run on batteries. Terminal devices use radio frequency technology to communicate with the exchange.

However, wireless security systems also have certain disadvantages: higher cost and the need to replace batteries. You also need to monitor the quality of the connection.

The chosen topic is relevant because:

- wireless security systems are gaining popularity;
- radio protocol for data transmission is of great importance for energy efficiency, ease of use, the ability of the system to be resistant to interference.

The aim of the work is to create a security system with improved functional characteristics, namely using a wireless communication channel based on LoRa technology.

The object of research is software and hardware for security systems.

The subject of research is radio protocols for data transmission between end devices and control panel in security systems.

Research methods - theoretical-analytical and practical analysis of radio protocols for data transmission between end devices and control panel in security systems.

Scientific novelty of the obtained results: the influence of the peculiarities of LoRa technology functioning on the work of the data transmission channel of the security system is estimated.

Practical significance of the obtained results: a variant of the security system based on LoRa technology is proposed, which has a number of significant advantages over competing systems. The practical value of the work has been confirmed by Ajax Systems.

Approbation of dissertation results: Report at the IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), September 21 - 25, Lviv, 2021.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

IoT – Internet of Things

ITU - Міжнародний союз електрозв'язку

LPWAN - Low Power Wide Area Networks

M2M - Machine-to-Machine

API - Application programming interface

SDR - Sigfox Radio Defined

TCO - Загальна вартість експлуатації

UNB - Ultra Narrow Band

ISM – Innovation and Technology Management

CSS - Chirp Spread Spectrum

FSK - Frequency shift keying

OFDM - Orthogonal Frequency-Division Multiplexing

SC-FDMA - Single-carrier Frequency Division Multiple Access

TAU - Tracking Area Update

eDRX - Extended discontinuous reception

PTW - Paging Time Window

HLCOM - High latency communication

СКУД або СКД - Система контролю і управління доступом

NSA - Нестандартна мережева архітектура

ВСТУП

Бездротові системи безпеки відрізняються рядом суттєвих переваг, оскільки відсутність проводів значно спрощує монтаж і дозволяє розміщувати їх в будь-якому зручному місці, а злочинці не зможуть дезактивувати такі відеокамери спостереження або датчики, перерізавши їх кабелі. Завдяки вказаним перевагам попит на бездротові системи безпеки вище, ніж на традиційні системи безпеки.

Бездротові системи безпеки використовують найсучасніші технології передачі даних та технології енергозбереження. Більшість компонентів системи безпеки, наприклад, охоронні датчики, працюють від акумулятора. Кінцеві пристрої використовують радіочастотні технології для зв’язку з централлю. Централі мають вихід в Інтернет.

Однак індустріальні електромагнітні завади та будівлі та їх елементи значно знижують максимальну відстань роботи бездротові системи безпеки і функціонування окремих її елементів. В таких випадках система може видавати хибні сигнали та надсилати недостовірну інформацію користувачу. Тому необхідно підвищувати завадостійкість бездротових системи безпеки та збільшувати максимальну відстань роботи їх складових.

Наведені вище недоліки можуть бути виправленими новою системою с розширеним функціоналом, низькою ціною та можливістю роботи на більших відстанях в умовах значних електромагнітних завад.

Метою роботи є створення концепції бездротової системи безпеки з розширеним функціоналом, а саме з використанням радіочастотного каналу зв’язку на основі технології LoRa.

Розділ 1. Радіочастотні технології передачі даних для Інтернету речей

1.1 Особливості IoT. Технології Long Range у системах Інтернету речей

Одним з ключових напрямків розвитку індустрії стала концепція Інтернету речей (IoT). Міжнародний союз електрозв'язку (ITU) наводить визначення IoT як поєднання фізичних та віртуальних речей [1].

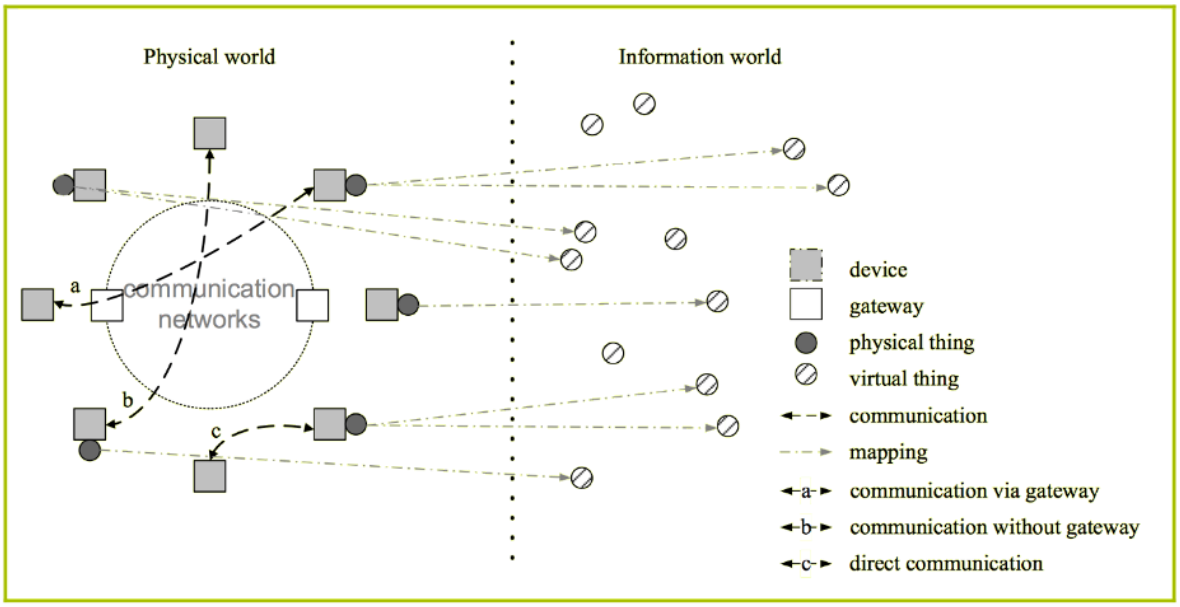


Рисунок 1.1 – Визначення поняття IoT Міжнародним союзом електрозв'язку (ITU)

Фізичні речі:

- Існують у фізичному світі їх можна відчувати, приводити в дію та з'єднувати.
- Приклади: промислові роботи, товари та електрообладнання.

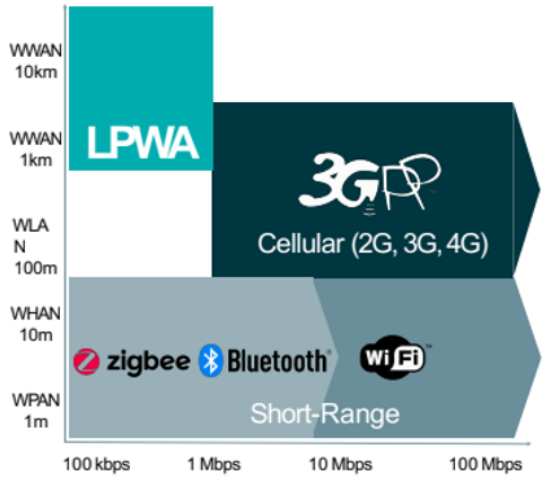
Віртуальні речі:

- Існують в інформаційному світі і можуть зберігатись, оброблятись та отримувати доступ.
- Приклади: мультимедійний контент, прикладне програмне забезпечення.

В недалекому майбутньому до Інтернету буде підключено кілька мільярдів пристроїв. Більшість пристроїв матиме батарейне живлення. У зв'язку з цим, однією з важливих характеристик інтернет речей є тривала робота пристрою без додаткового обслуговування і зарядки. Для ефективного вирішення завдань, пов'язаних з енергоживленням, з'явилися нові типи мереж LPWAN (Low Power Wide Area Networks). Технології, які дозволяють підключати автономні пристрої до глобальної мережі, з'явилися в 2015-2016 рр. і поступово набирають популярність.

Low-Power Wide-Area (LPWA) мережі новий клас бездротових технологій, спеціально розроблених для додатків IoT із низьким рівнем споживання енергії та невеликою швидкістю передачі даних. Найбільш популярними серед таких технологій є LoRa, SIGFOX, NB-IoT, Weightless P та ін. Їх поява зумовлена необхідністю підключення великої кількості приладів обліку і телеметрії для централізованого збору даних на хмарних серверах.

Порівняння бездротових технологій LPWA з технологіями стільникового зв’язку та технологіями ближнього радіусу дії наведено на рис.1.2 та рис.1.3



	LPWA	Cellular 2G, 3G, 4G	Short-Range PAN | WLAN
Data Rate (speed)	Low	High	Low/Med
Cost (+complexity)	Low	High	Low/Med
Power (consumption)	Low	High	Low/Med
Range (+penetration)	V. Long	Med	Short
Install (ie. pairing)	Easy	Easy	Hard

Рисунок 1.2 – Порівняння бездротових технологій за основними параметрами.

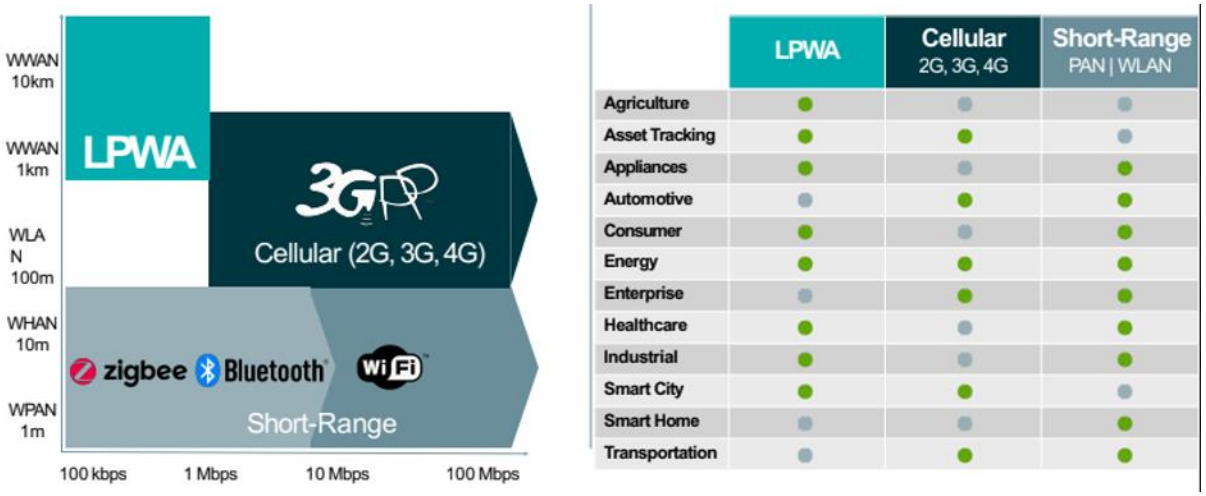


Рисунок 1.3 – Порівняння бездротових технологій за сферами використання.

Як видно з малюнків технології LPWA призначені для M2M (Machine-to-Machine)-додатків, які вимагають передачі даних по радіоканалу з низькою швидкістю і роботи без нагляду протягом тривалого періоду часу, можливо, у віддалених або важкодоступних місцях.

Особливості LPWA - низьке енергоспоживання (low-power) і широкий територіальне охоплення (wide-area).

Прогнозується, що мережі LPWA будуть застосовуватися в широкому спектрі додатків інтернету речей, таких, як відстеження виробничих активів, облік споживання води і газу, інтелектуальні мережі, міські парковки, торгові автомати і міське освітлення. Технологія може використовуватися і для підключення переносних пристроїв. Модулі LPWA повинні мати низьку вартість, то ж стосується і їх підключення. Це допоможе IoT-ринку рости.

Вимоги IoT-додатків настільки різноманітні, що всі випадки використання LPWA єдиною технологією не охоплюються, в зв'язку з цим в даний час розглядаються три взаємодоповнюючих стандарту, які поряд з LTE-Advanced Pro увійдуть в пакет стандартів 3GPP Release 13. Це стандарти

для вузькосмугових IoT- пристроїв (NB-IoT), для розширеного GPRS-покриття (EC-GPRS) і межмашинного LTE-з'єднань (LTE-MTC). Ці технології передбачають роботу в це дозвіл частот і будуть охоплювати всі варіанти використання пристроїв LPWA.

1.2 Використання технологій Long Range у системах Інтернету речей

1.2.1 Технологія Sigfox

Sigfox забезпечує стандартний спосіб збору даних з датчиків та пристроїв за допомогою єдиного стандартного набору API. Крім того, технологія Sigfox, що руйнує, доповнює традиційні стільникові M2M, забезпечуючи глобальні, повсюдні, надзвичайно довгі рішення щодо автономної роботи при найменших витратах.

Sigfox має великий потенціал як додаткове рішення для підключення, що дозволяє зменшити споживання батареї та покращити взаємодію з користувачем. Sigfox забезпечує мережу, технології та експертну екосистему, які необхідні, щоб допомогти компаніям та організаціям максимально використати свої амбіції щодо IoT.

Sigfox використовує 192 кГц загальнодоступного діапазону для обміну повідомленнями в ефірі (рис.1.4). Модуляція - надвузька смуга. Кожне повідомлення має ширину 100 Гц і передається зі швидкістю передачі даних 100 або 600 біт на секунду залежно від регіону.

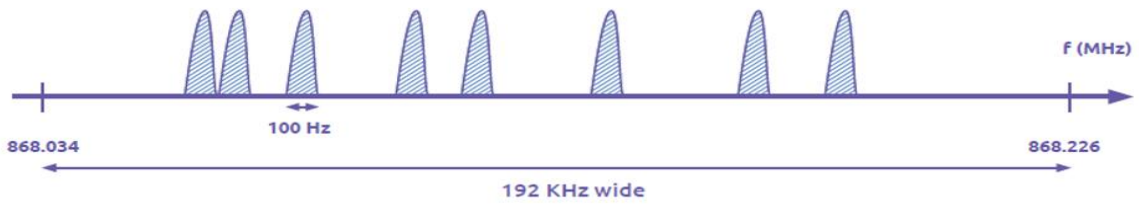


Рисунок 1.4 – Технологія Sigfox базується на надвузькій смузі

Мережа Sigfox має горизонтальну і тонку архітектуру, що складається з 2 основних шарів.

Рівень мережевого обладнання складається, по суті, з базових станцій (та інших елементів, наприклад, антен), відповідальних за прийом повідомлень від пристроїв та їх передачу до систем підтримки Sigfox.

Система підтримки Sigfox - це другий рівень, що становить основну мережу, відповідальну за обробку повідомлень та надсилання їх через зворотні виклики до системи клієнтів. Цей рівень також забезпечує точку входу для різних суб'єктів екосистеми (Sigfox, операторів Sigfox, каналів та кінцевих споживачів) для взаємодії з системою через інтерфейси веб-догляду або API. Цей рівень також включає модулі та функції, які є найважливішими для забезпечення розгортання, роботи та моніторингу мережі, такі як Система підтримки бізнесу для замовлення та виставлення рахунків, планування радіо, що підтримує розгортання мережі, моніторинг для забезпечення доброго робота мережі. Крім того, цей рівень включає сховище та інструменти для аналізу даних, зібраних або сформованих мережею.

Як згадувалося на рисунку вище, зв'язок між двома рівнями забезпечується загальнодоступним Інтернетом, але захищений за допомогою VPN-з'єднання. У наступних розділах описуються різні компоненти цих двох рівнів мережі Sigfox

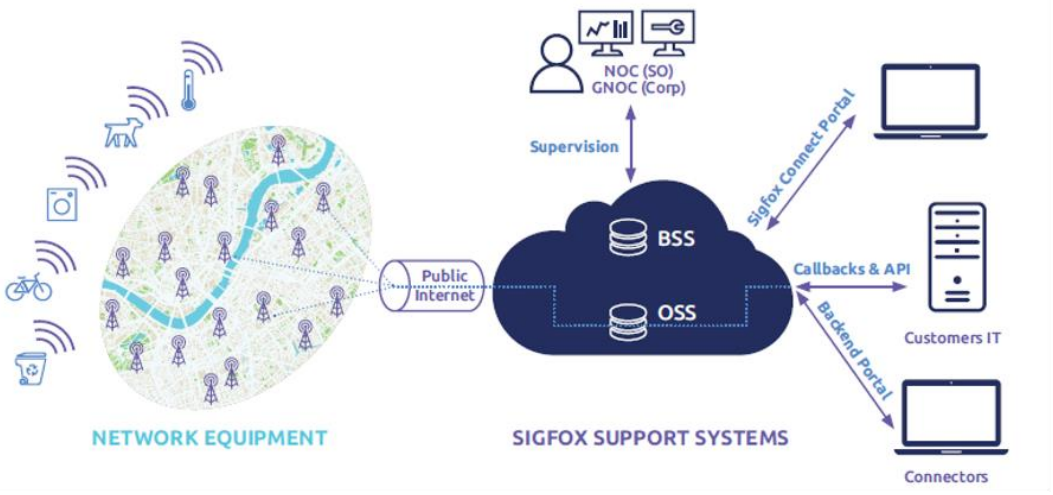


Рисунок 1.5 – Архітектура високого рівня мережі Sigfox

Архітектура плоских мереж

Плоска архітектура Sigfox є ключовою для мінімізації як CAPEX, так і OPEX. Програмне забезпечення Sigfox Radio Defined (SDR) допомагає подолати високі витрати на обладнання для базових станцій. Спеціальне обладнання не використовувалося, але натомість програмний алгоритм ефективно обробляє демодуляцію. Це значно зменшує загальну вартість експлуатації (TCO).

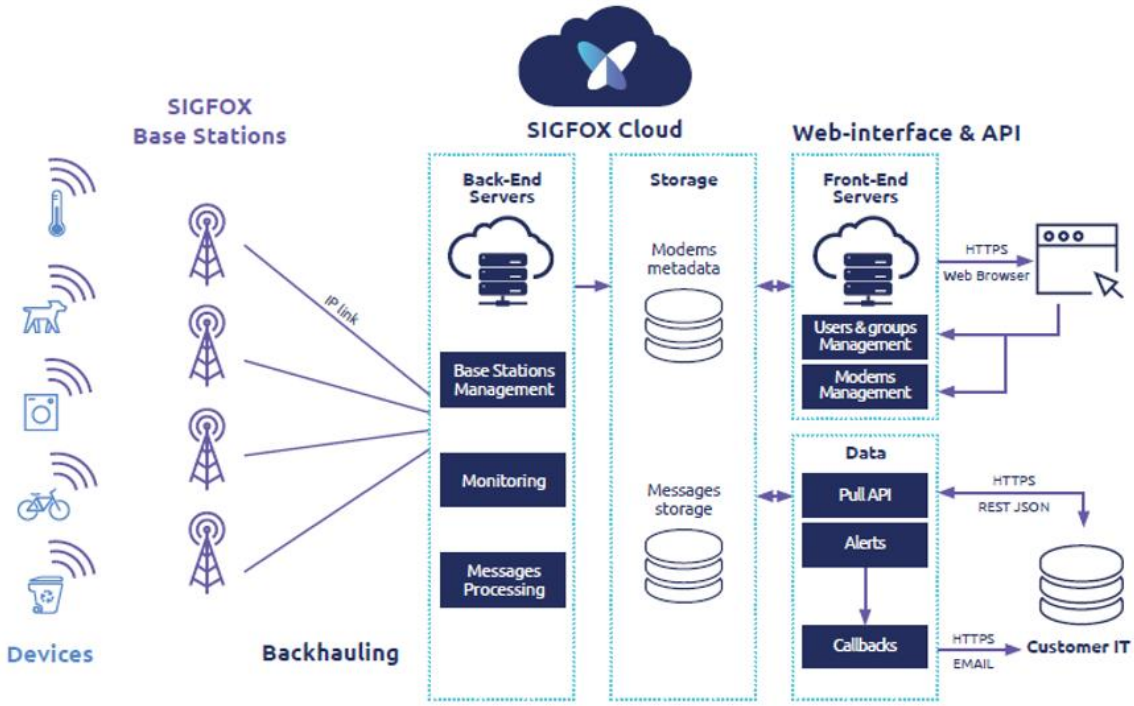


Рисунок 1.6 – Архітектура Flat

Дані передаються по повітрю до базових станцій, а потім проходять через зворотний зв'язок. Як правило, для резервного зв'язку використовується резервне копіювання DSL і 3G або 4G. Коли одне з двох недоступне, супутникове підключення можна використовувати як альтернативну технологію резервного копіювання.

Бек-енд керує обробкою повідомлень. Потенційно існує багато копій одного і того ж повідомлення, яке надходить у основну мережу, але слід

зберігати лише одне. Сервери базової мережі також контролюють стан мережі та керують базовими станціями в усьому світі.

Мережева інфраструктура також зберігає повідомлення в двох місцях: метадані можуть бути використані для створення служб, з одного боку, і повідомлень клієнтів, щоб клієнти могли отримати їх пізніше, з іншого.

Нарешті, веб-інтерфейс та API дозволяють клієнтам отримувати доступ до своїх повідомлень. Вони можуть отримати доступ до платформи через свій веб-браузер або використовувати REST API, щоб синхронізувати їх зі своєю IT-системою та надсилати повідомлення на пристрій вниз.

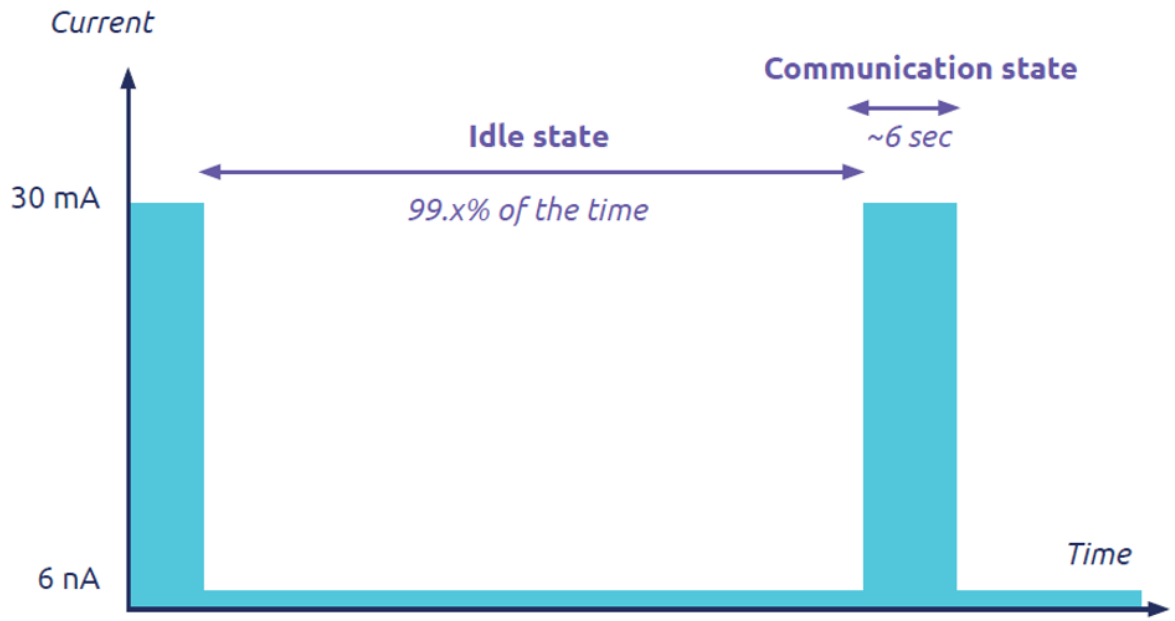


Рисунок 1.7 – Низьке споживання холостого ходу збільшує час автономної роботи

Висока енергоефективність, що забезпечується технологією Sigfox, також залежить від напівпровідникових партнерів Sigfox, оскільки їх мікросхеми споживають від 10 мА до 50 мА в передачі - залежно від партнера та використовуваного чіпа.

Ці значення застосовні в Європі, де вихідна потужність становить 14 дБм, але сила струму вища в США, де потрібно 22 дБм. Однак час

перебування в ефірі в шість разів нижчий, тому час автономної роботи приблизно однаковий.

Є ще два фактори, що пояснюють тривалий час автономної роботи Sigfox.

1. Не потрібно сполучення, що означає, що між об'єктом та базовою станцією не передаються повідомлення про синхронізацію перед передачею даних. Це велика перевага в порівнянні з іншими технологіями, які всі включають ці додаткові етапи.
2. Крім того, споживання холостого ходу дуже низьке, часто кілька наноамперів, що робить його майже незначним.

Далекобійність

Основна конкурентна перевага технології Sigfox полягає в розгортанні з великим покриттям і обмеженою кількістю базових станцій:

1) для даної вихідної потужності діапазон радіочастотної (RF) лінії зв'язку визначається швидкістю передачі даних, тобто меншою норма забезпечує більший діапазон;
2) другий фактор - бюджет зв'язку, сума чутливості базової станції та вихідна потужність об'єкта; сильно залежить від рельєфу;
3) хороше покриття в приміщенні завдяки використанню діапазону під ГГц.

Великий діапазон базових станцій дозволяє Sigfox розгорнути загальнодержавну мережу за мінімальних витрат. Що стосується діапазону радіочастот, Sigfox використовує метрику, яка називається бюджетом зв'язку:

1. бюджет зв'язку - це сума чутливості базової станції, коефіцієнтів посилення антени та вихідної потужності на стороні об'єкта;
2. це закінчується дещо вищим бюджетним зв’язком у зоні ETSI, що призводить до збільшення осередків;

3. хороше покриття Sigfox у приміщенні обумовлене використанням діапазону під ГГц. Інші технології, що вимагають вищого бюджетного зв'язку та використовують 2,4 ГГц, постраждають від випадків використання в приміщенні.

Стійкість до перешкод

Технологія Sigfox представляє унікальні можливості проти глушення завдяки внутрішній міцності UNB в поєднанні з просторовою різноманітністю базових станцій.

UNB надзвичайно надійний в середовищі з іншими сигналами, включаючи сигнали з розширеним спектром. Однак на мережі розширеного спектру впливають сигнали UNB. Тому надвузький діапазон є найкращим вибором для роботи в державній промисловій, науковій та медичній діапазоні (ISM).

Висока стійкість до перешкод є ключовим фактором для ефективної роботи в публічному діапазоні ISM.

Найкращим доказом високої стійкості до перешкод є здатність передавати, незважаючи на наявність сигналів перешкод. Ультравузька смугова модуляція має певну нерівність, оскільки перекриття з шумом дуже низьке. Для отримання повідомлення сигнал повинен бути принаймні на 8 дБ вище рівня шуму.

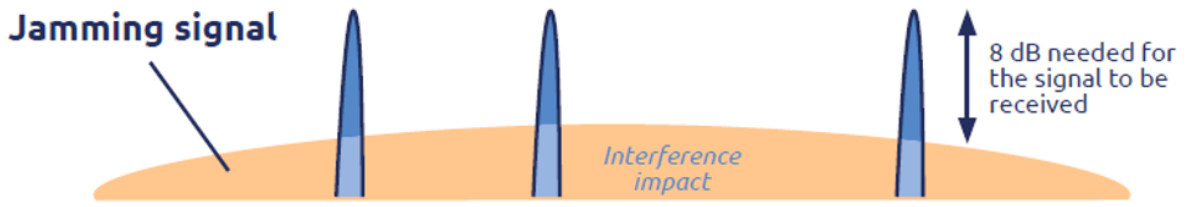


Рисунок 1.8 – Стійкість до перешкод, надана UNB

Конкуруючі технології, побудовані на модуляції розширеного спектра, сильно піддаються впливу шуму, оскільки загальна їх площа значно більша. UNB є найкращим можливим вибором сигналізації для роботи в загальнодоступному діапазоні ISM.

1.2.2 Технологія LoRa

LoRa ™ (від англ. Long Range) - це технологія і однойменний метод модуляції.

Запатентований метод модуляції з розширеним спектром, отримана на основі існуючої технології Chirp Spread Spectrum (CSS), LoRa пропонує компроміс між чутливістю та швидкістю передачі даних, працюючи в каналі з фіксованою пропускною здатністю 125 або 500 кГц. Крім того, LoRa використовує коефіцієнти ортогонального розповсюдження. Це дозволяє мережі зберегти термін служби батареї підключених кінцевих вузлів шляхом адаптивної оптимізації рівнів потужності та швидкості передачі даних окремого кінцевого вузла [2].

LoRa дозволяє демодулювати сигнали на рівні 20dB нижче рівня шумів, тоді як більшість систем з частотної маніпуляцією (frequency shift keying, FSK) можуть коректно працювати з сигналами на рівні не нижче 8-10dB над рівнем шумів. Модуляція LoRa визначає фізичний, який може використовуватися в мережах з різною архітектурою - mesh-мережі, зірка, точка-точка і інші.

Завдяки своїй високій чутливості (-148dbm) LoRa підходить до приладів з вимогами високої стійкості зв'язку на великих відстанях та низького споживання електроенергії.

Коли говорять про технології LoRa, то найчастіше мають на увазі і метод модуляції LoRa, що належить Semtech, і відкритий протокол LoRaWAN, розвитком якого займається некомерційна організація LoRa Alliance, в яку входять різні компанії: як виробники устаткування і програмного забезпечення, так і оператори зв'язку. У числі членів LoRa AllianceIBM, Semtech і інші.

Що таке LoRa? Абревіатурою LoRa (Long Range) позначають лише вид модуляції, тобто рівень l1 по моделі OSI. Протокол канального рівня носить ім'я LoRaWAN. Але найчастіше «Лорою» називають сукупну систему, яка використовує LoRa на фізичному і LoRaWAN на канальному рівні.

Працює це таким чином. Базова станція слухає ефір в заданому діапазоні частот. Коли вона чує запит від будь-якого з пристроїв, то відповідає йому на частоті звернення. Ширина каналу при цьому становить 125, 250, 500 кГц, максимальна швидкість - трохи більше 5 кілобіт / с. Цей стандарт Інтернету речей не створений для перегляду потокового відео. Його завдання максимально швидко і гарантовано передати невелике повідомлення від датчика на базову станцію. Залежно від радіо умов вибирається оптимальний набір параметрів зв'язку. За це відповідає SF (spreading factor) - коефіцієнт, до якого прив'язуються параметри передачі і прийому. SF - це ціле число, в стандарті він передбачений від 12 до 7. Чим вище SF, тим краще перешкодозахищеність лінії, але тим нижче швидкість і тим більше часу в ефірі займає передача. Для прикладу, максимальна перешкодозахищеність досягається на SF = 12. При цьому час пакета в ефірі становить 2,466 с, а швидкість - 292 біт / с.

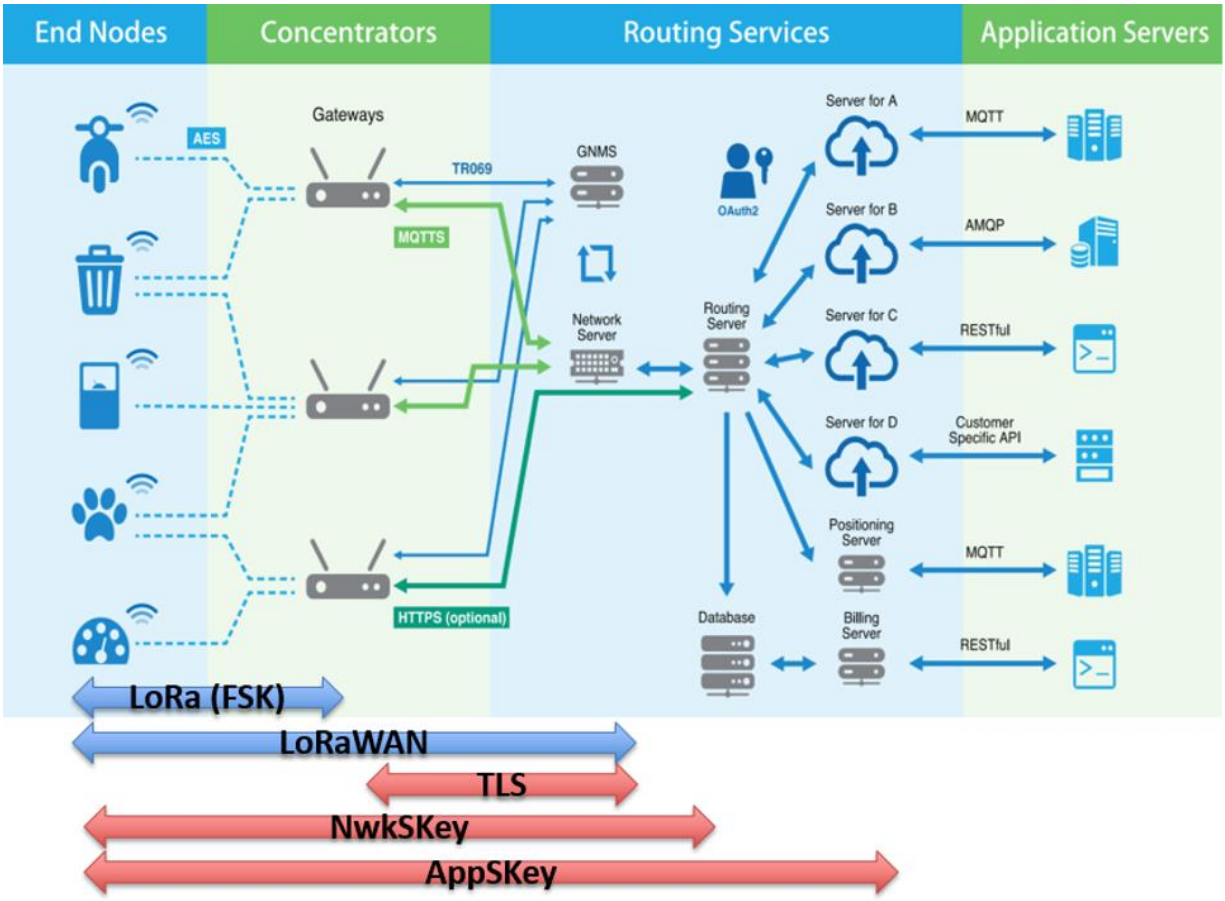


Рисунок 1.9 - Архітектура LoRaWAN

Однак чим більше датчиків будуть використовувати базову станцію, тим більше часу в ефірі вони займуть. Тому, при хороших радіо умовах, SF буде менше. Зростає швидкість - падає час передачі.

Пакети приймаються базовою станцією (в архітектурі LoRa її частіше називають шлюзом), однак обробляє їх наступна ланка ланцюга - мережевий сервер. Цей сервер відповідає за управління всіма шлюзами, він вирішує через який шлюз спілкуватися з датчиком (якщо датчик чутно через кілька шлюзів) і визначає ще ряд важливих параметрів.

Однак мережевий сервер не обробляє корисну інформацію з пакетів. Це робить наступне і найважливіша ланка - сервер додатків. Саме на сервері додатків відбувається розшифровка показань від датчиків, вони в зрозумілій

формі поступають або в білінг, або в інтерфейс споживачеві, або в інше задане місце.

Сильні та слабкі сторони технології LoRa

На даний момент існує кілька десятків стандартів для Інтернету речей. Частина з них універсальні, частина пристосовані вирішувати своє коло завдань. Є навіть стандарти на базі Wi-Fi і LTE. Так чому саме LoRa?

Переваги LoRaWAN:

- LoRa - це відкритий стандарт. Чіпи для кінцевих пристроїв у вільному продажі, є вся документація, і вона відкрита всім охочим. Вона не «річ у собі», навіть якщо пропаде один з виробників, залишаться інші.
- Більша дальність передачі радіосигналу за порівнянням з іншими непровідними технологіями, що використовуються для телеметрії, досягає 10—15 км. LoRa має хороший радіус дії, вона може приймати інформацію від пристроїв в підвалі будинку або в кілометрі від базової станції. Насправді, може прийняти інформацію і від датчика в 4 кілометрах міських умов. Але тут страждає стабільність, оскільки починається втрата пакетів. Однак, кілометр або два ми маємо.
- Низьке енергоспоживання в кінцевих пристроях, завдяки мінімальним затратам енергії на передачу невеликого пакету даних Кінцеві вузли LoRa живляться від батарейки мінімум рік. Тут є залежність від класу кінцевих вузлів (A, B або C). Самий живучий - A-клас - може протриматися кілька років.
- Висока проникаюча здатність радіосигналу в міській забудові при використанні частот субгігагерцового діаграми.
- Висока масштабність мережі на більших територіях.

Недоліки LoRaWAN:

- Відносно низька пропускна здатність, яка змінюється в залежності від використання технологій передачі даних на фізичному рівні, складається з кількох сотень біт / с до кількох десятків кбіт / с.
- Затримка передачі даних від датчика до кінцевого додатку, пов'язана з часом передачі радіосигналу, може досягати від декількох секунд до декількох десятків секунд.
- Ризик зашумленості спектра неліцензованого діаграми частоти.
- Відсутність єдиного стандарту, який визначає фізичний шар та управління доступом до середовища для безпровідних LPWAN-мереж.
- Проприєтарна технологія модуляції LoRa, «закрита» патентом Semtech.

1.2.3 Технологія NB-IoT

Технологія NB-IoT багато в чому схожа на LTE - починаючи з фізичної структури радіосигналу і архітектури. Для LTE сигналу використовується принцип розділення каналів OFDM з рознесенням підлеглих на 15кГц. В передачі від базової станції до кінцевого пристрою (Downlink, DL) використовується OFDMA, а від кінцевого пристрою до базової станції (Uplink, UL), використовується SC-FDMA. Вся несуча в LTE розділена на ресурсні блоки (RB), кожен з яких складається з 12 піднесучих і загальною шириною полоси в 12х15кГц = 180кГц (рис.1). Кожен ресурсний блок розділений на 12х7 = 84 ресурсних елементів (ресурсний елемент, RE).

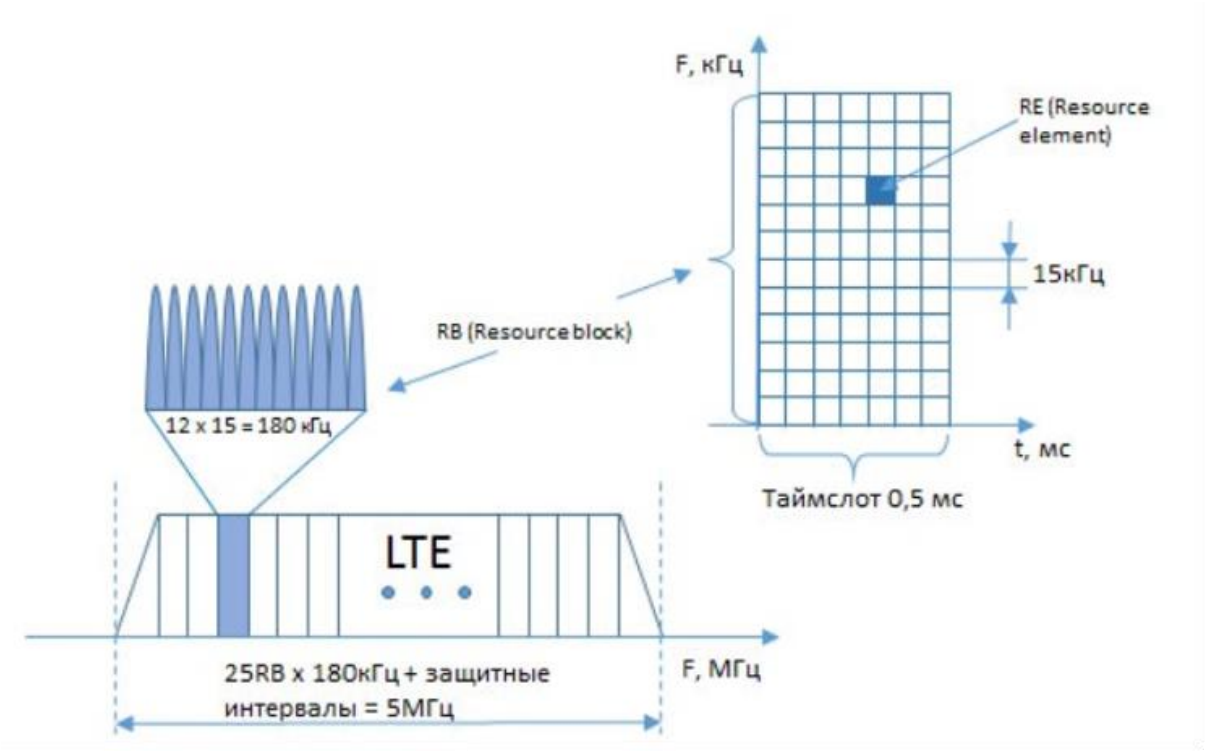


Рисунок 1.10 - Блок ресурсів, елемент ресурсу

Для досягнення великої пропускної здатності однієї стільникової комірки застосовуються високі порядки модуляцій QAM256 для DL і QAM64 в UL. З цією метою було придумано технології MIMO2x2 і MIMO4x4.

Особливості радіосигналу NB-IoT:

Найважливіше в NB-IoT - можливість роботи при більш низьких рівнях сигналу і при високих показниках шумів, а також економії батареї. Також NB-IoT призначений для передачі коротких повідомлень, і від нього не вимагається передача аудіо-відео контенту, тобто великих файлів.

На фізичному рівні є певні особливості, які допомагають забезпечити необхідні характеристики:

- передача і прийом рознесені в часі, тобто це по суті напівдуплексний режим;
- спільна полоса для NB-IoT обмежена в один RB шириною в 180кГц;

- радіотракт користувацького пристрою має лише одну антенну, приймач і передавач;
- типи модуляції, що використовуються обмежені BPSK і QPSK;

Використання вузької смуги частот в один RB, однієї антени і напівдуплексний режим передачі дозволяє спростити пристрій та досягнути:

- зниження вимог до потужності;
- зниження споживання енергії;
- зменшення габаритів;
- зменшення вартості пристрою.

Механізми енергозбереження PSM і eDRX:

Одним з ключових переваг LPWAN мереж є енергоефективність. Заявляється строк до 10 років автономної роботи пристрою на одній батареї. Розберемося, яким чином досягаються такі значення.

Коли пристрій споживає найменше енергії? Правильно, коли воно вимкнене. І якщо повністю знеструмити пристрій не можна, то можна знеструмити радіо модуль, на той час, поки в ньому немає необхідності. Тільки попередньо треба узгодити це з мережею..

PSM (режим енергозбереження):

Режим енергозбереження PSM дозволяє пристрою надовго вимикати радіо модуль, залишаючись при цьому зареєстрованим в мережі, і не встановлювати заново PDN кожен раз при необхідності передати дані.

Щоб мережа знала, що пристрій, як і раніше є, воно періодично ініціює процедуру актуалізації - Tracking Area Update (TAU). Частота цієї процедури задається мережею за допомогою таймера T3412, значення якого передається пристрою під час процедури Attach або чергового TAU. У

класичному LTE значення за замовчуванням цього таймера 54 хвилини, а максимальне - 186 хвилин. Однак, для забезпечення високої енергоефективності, необхідність виходу в радіоефір кожні 186 хвилин - це занадто дороге задоволення. Для вирішення цієї проблеми і був розроблений механізм PSM.

Пристрій активує режим PSM передаючи в повідомленнях «Attach Request» або «Tracking Area Request» значення двох таймерів T3324 і T3412-Extended. Перший визначає час, який пристрій буде доступний після переходу в «Idle Mode». Другий - це час, через яке повинен бути проведений TAU, тільки тепер його значення може досягати 35712000 секунд або 413 днів. Залежно від налаштувань, MME може прийняти значення таймерів, отримані від пристрою, або змінити їх, передавши нові значення в повідомленнях «Attach Accept» або «Tracking AreaUpdate Accept». Тепер пристрій може не включати радіо модуль 413 днів і залишатися при цьому зареєстрованим в мережі. В результаті отримуємо колосальну економію ресурсів мережі та енергоефективність пристроїв.

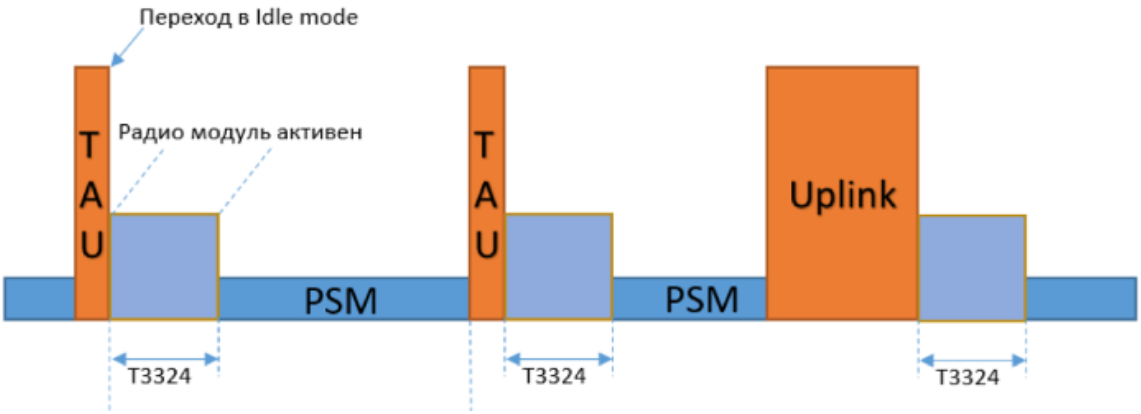


Рисунок 1.11 – Реалізація режиму енергозбереження PSM

Однак в цьому режимі пристрій недоступно тільки для вхідних комунікацій. При необхідності передати що-небудь в сторону сервера додатків пристрій може в будь-який момент вийти з PSM і відправити дані,

залишившись після цього активним протягом таймера T3324 для прийому інформаційних повідомлень від AS (якщо такі будуть).

eDRX (extended discontinuous reception):

eDRX, розширений режим переривчастого прийому. Щоб передати дані на пристрій, який знаходиться в «Idle mode», мережа виконує процедуру оповіщення - «Paging». При отриманні пейджінга пристрій ініціює встановлення SRB для подальшої комунікації з мережею. Але щоб не пропустити адресоване йому повідомлення Paging, пристрій повинен постійно моніторити радіоефір, що також досить енерговитрато.

eDRX - це режим, при якому пристрій приймає повідомлення від мережі не постійно, а періодично. Під час процедур Attach або TAU пристрій погоджує з мережею тимчасові проміжки, в які воно буде «слухати» ефір. Відповідно, в ці ж проміжки буде проводитися процедура Paging. У режимі eDRX робота пристрою розбивається на цикли (eDRX cycle). На початку кожного циклу йде так зване «вікно пейджінга» (Paging Time Window, далі PTW) - це час, який пристрій слухає радіоканал. Після закінчення PTW пристрій відключає радіо модуль до кінця циклу.

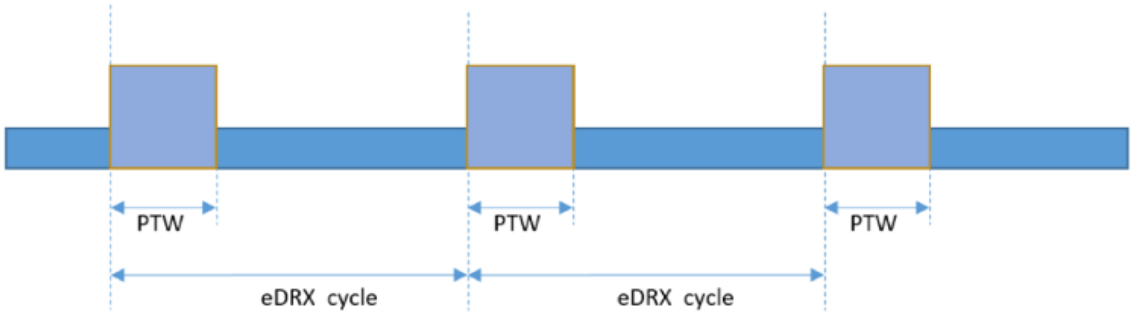


Рисунок 1.12 – Реалізація режиму переривчатого прийому eDRX

HLCOM (high latency communication):

При необхідності передати дані в Uplink пристрій може вийти з будь-якого з цих двох режимів енергозбереження, не чекаючи закінчення PSM або eDRX циклу. Але ось передати дані на пристрій можливо, тільки коли він активний.

Функціонал HLCOM або комунікація з високими затримками - це буферизація Downlink пакетів на SGW на час, поки пристрій знаходиться в режимі енергозбереження та недоступно для комунікації. Буферізіровані пакети будуть доставлені, як тільки пристрій вийде з PSM, зробивши TAU або передавши Uplink трафік, або, коли настане PTW.

1.2.4 Технології 5G

Бездротовий зв’язок п’ятого покоління (5G) — це остання ітерація технології стільникового зв’язку, розроблена для значного збільшення швидкості та швидкості реагування бездротових мереж. З 5G дані, що передаються через бездротові широкосмугові з’єднання, можуть передаватися на швидкості в багато гігабіт, за деякими оцінками, з потенційною піковою швидкістю до 20 гігабіт на секунду (Гбіт/с). Ці швидкості перевищують швидкість дротової мережі та пропонують затримку в 1 мілісекунду (мс) або менше, що корисно для програм, які потребують зворотного зв’язку в реальному часі. 5G дозволить різко збільшити обсяг даних, що передаються через бездротові системи, завдяки більш доступній пропускній здатності та передовій технології антени.

Попередні покоління бездротових технологій використовували низькочастотні діапазони спектру. Щоб компенсувати проблеми, пов’язані з відстанню та перешкодами міліметрових (ММ) хвиль, бездротова індустрія також розглядає можливість використання низькочастотного спектру для мереж 5G, щоб оператори мережі могли використовувати спектр, який вони вже володіють, для побудови своїх нових мереж. Низькочастотний спектр

досягає більших відстаней, але має меншу швидкість і потужність, ніж ММ хвилі.

4G може підтримувати до 2 Гбіт/с і повільно продовжує покращувати швидкість. 4G має швидкість до 500 разів швидше, ніж 3G. 5G може бути в 100 разів швидше, ніж 4G.

Однією з головних відмінностей між 4G та 5G є рівень затримки, якої у 5G буде набагато менше. 5G використовуватиме кодування з ортогональним мультиплексуванням з частотним розподілом (OFDM), подібно до 4G LTE. 4G, однак, використовуватиме канали 20 МГц, з'єднані разом на 160 МГц. 5G буде мати канали від 100 до 800 МГц, що вимагає більших блоків частот, ніж 4G [3].

ITU-R визначено основні області застосування 5G для розширених можливостей [4]:

- покращений мобільний широкосмуговий зв'язок (eMBB);
- зв'язок з надзвичайно високою надійністю та низькою затримкою (URLLC);
- масовий зв'язок машинного типу (mMTC).

Рисунок 1.13 – Області застосування для розширення можливостей 5G

На даний момент розгорнуто лише eMBB. Технології URLLC і mMTC у процесі розгортання

5G використовує переваги багатьох технологій, намагаючись досягти таких високих швидкостей. Існує не лише одна інновація. Новий стандарт використовуватиме абсолютно новий діапазон радіочастот від 4G. 5G використовуватиме переваги «міліметрових хвиль», які транслюються на частотах від 30 до 300 ГГц у порівнянні з діапазонами нижче 6 ГГц, які використовувалися в минулому. Раніше вони використовувалися лише для зв'язку між супутниками та радіолокаційними системами. Але міліметрові хвилі не можуть легко проходити крізь будівлі чи інші тверді об'єкти, тому 5G також використовуватиме переваги «малих клітин» — менших мініатюрних станцій, які можна розташовувати приблизно через кожні 250 метрів у густих міських районах. Це забезпечить набагато краще покриття в таких місцях [5].

Архітектура мережі 5G

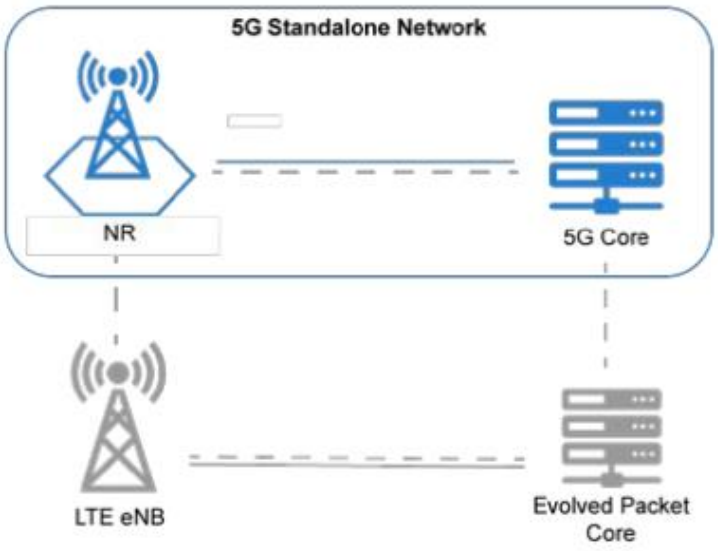


Рисунок 1.14 — Автономна мережева архітектура

Автономна мережева архітектура (Standalone Network, SA). SA означає наявність незалежної мережі 5G. Він матиме як новий повітряний інтерфейс 5G, нове радіо (NR), так і 5G Core (5GC). Окрема мережа 5G мережа надає користувачеві наскрізний досвід 5G. Мережа SA все одно буде взаємодіяти з існуючою Мережа 4G/LTE для забезпечення безперервності обслуговування між двома поколіннями мережі.

Як показано на Рис. 1.14, мережа 5G може працювати незалежно. У той же час відбувається взаємодія з мережею LTE, щоб охопити території, які ще не охоплені 5G, і з’єднати користувачів 5G з користувачами, які не є 5G.

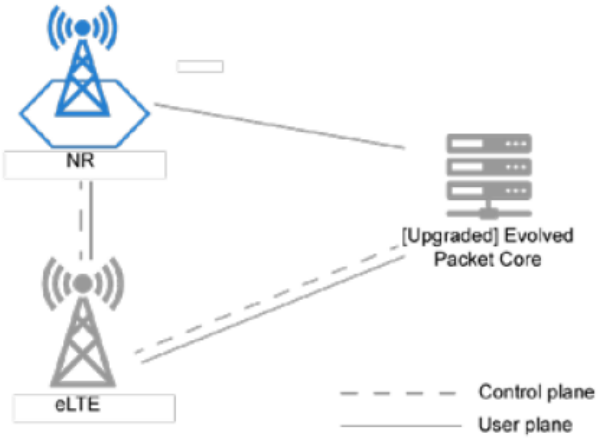


Рисунок 1.15 — Нестандартна мережева архітектура

Нестандартна мережева архітектура (NSA). Нестандартна 5G мережа, має на увазі наявність тільки 5G NR осередків з EPC в якості ядра, структура наведена на рис. 1.15. Оператори будуть розгортати осередки 5G і повністю залежати від існуючої мережі LTE для всіх функцій управління і додаткових сервісів. Архітектура 5G NSA працює за структурою "ведучий-ведений", де вузол доступу 4G є ведучим, а вузол доступу 5G — веденим [6] .

Висновки до розділу 1

Основою для передачі даних в бездротових системах безпеки є радіочастотні технології, які мають забезпечити достатньо велику відстань передачі даних і споживати незначну кількість енергії.

Для передачі невеликих обсягів даних і забезпечення терміну живлення від батареї у декілька років найкраще підходять технології LPWAN.

Висока енергоефективність, що забезпечується технологією Sigfox, також залежить від напівпровідникових партнерів Sigfox, оскільки їх мікросхеми споживають від 10 мА до 50 мА в передачі - залежно від партнера та використовуваного чіпа.

Завдяки своїй високій чутливості (-148dbm) LoRa ідеально підходить до пристроїв з вимогами низького споживання електроенергії і високої стійкості зв'язку на великих відстанях.

Найважливіше в NB-IoT - можливість роботи при більш низьких рівнях сигналу і при високих показниках шумів, а також економії батареї.

Для передачі великих обсягів даних у системах безпеки, у першу чергу відеоданих, гарну перспективу мають технології 5G. Недоліками таких технологій є те, що технологія має архітектуру стільникової мережі, в якій площа покриття поділяється на невеликі зони – соти або стільники. Дані при переміщенні між сотами можуть бути втрачені, або перепідключення від однієї базової станції до іншої займає певний час в момент коли сенсор мав надіслати свої дані.

Розділ 2. Принципи побудови та складові систем безпеки

Система безпеки - це сукупність упорядкованих і взаємопов'язаних об'єктів, що включають в себе технічні, правові, соціально-економічні, організаційні, методичні, санітарно-гігієнічні та інші засоби і заходи для цілей забезпечення безпеки.

Компоненти в систему безпеки підбираються для кожного замовника індивідуально, в залежності від його вимог і об'єкта, на якому буде реалізована її установка. Багато виробників пропонують спеціалізоване обладнання, призначене для установки в квартирі, будинку, офісі, магазині або виробничих приміщеннях. Всі підсистеми, що входять до складу комплексної системи безпеки є автономними, і, при необхідності, можуть самостійно виконувати покладені на них функції.

В цілому, системи безпеки поділяються на дві категорії за топологією об'єкта. Всі елементи можуть бути з'єднані проводовим підключенням, або використовуючи радіоефір.

2.1. Складові систем безпеки: пожежна, охоронна (відеоспостереження), контроль доступу.

Є системи, які спеціалізуються за одним певним напрямом: пожежний, охоронний, напрям систем контролю доступу (СКД) або “розумний будинок”, тобто напрям автоматизації буденних дій користувача. Також є системи, в яких поєднуються одразу кілька напрямків.

Системи пожежної безпеки - це комплекс технічних засобів та організаційних заходів, які спрямовані на запобігання пожежам та збиткам від них. Протипожежна сигналізація призначена для безперервного контролю пожежонебезпечних зон і реагування в автоматичному режимі у

випадку виникнення пожежі (включення системи оповіщення, передачі повідомлення в пожежну службу, індикації пожежі на пульті контролю).

Рисунок 2.1 – Конфігурація типової пожежної сигналізації

Система контролю і управління доступом (скорочено СКУД або СКД) — це комплекс технічних та програмних засобів, які призначені для організації входу / виходу на визначену територію та переміщень людей чи транспортних об’єктів на територіях, які знаходяться під охороною, згідно з певними правами доступу, для адміністративного моніторингу та попереджень несанкціонованого проникнення.

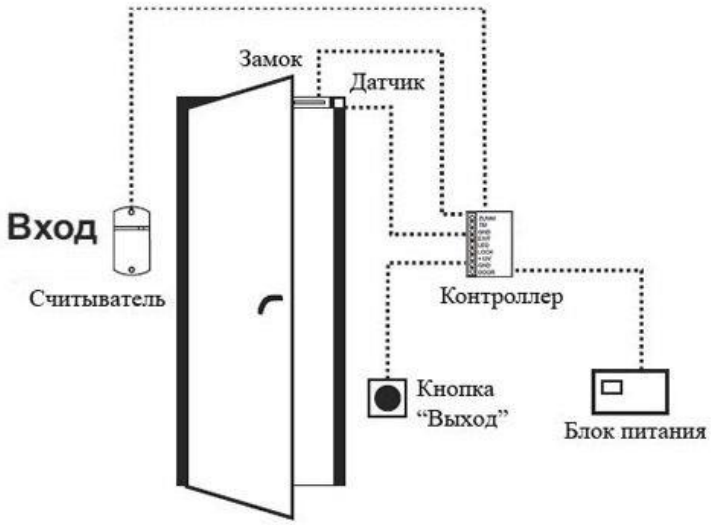


Рисунок 2.2 - Схема СКУД для однієї контрольної точки

За допомогою системи контролю доступу також досягається:

- ідентифікація осіб, що мають право доступу;
- розмежування доступу до різних приміщень;
- керування автоматичними режимами;
- реєстрація часу перебування особи на об’єкті;
- обробка інформації та ведення статистики.

Для кінцевого користувача прилади і сенсори Інтернету речей утворюють автоматизовані системи, якими він користується щоденно. Простим прикладом такої системи є Apple Home Kit (рисунок 2.3).

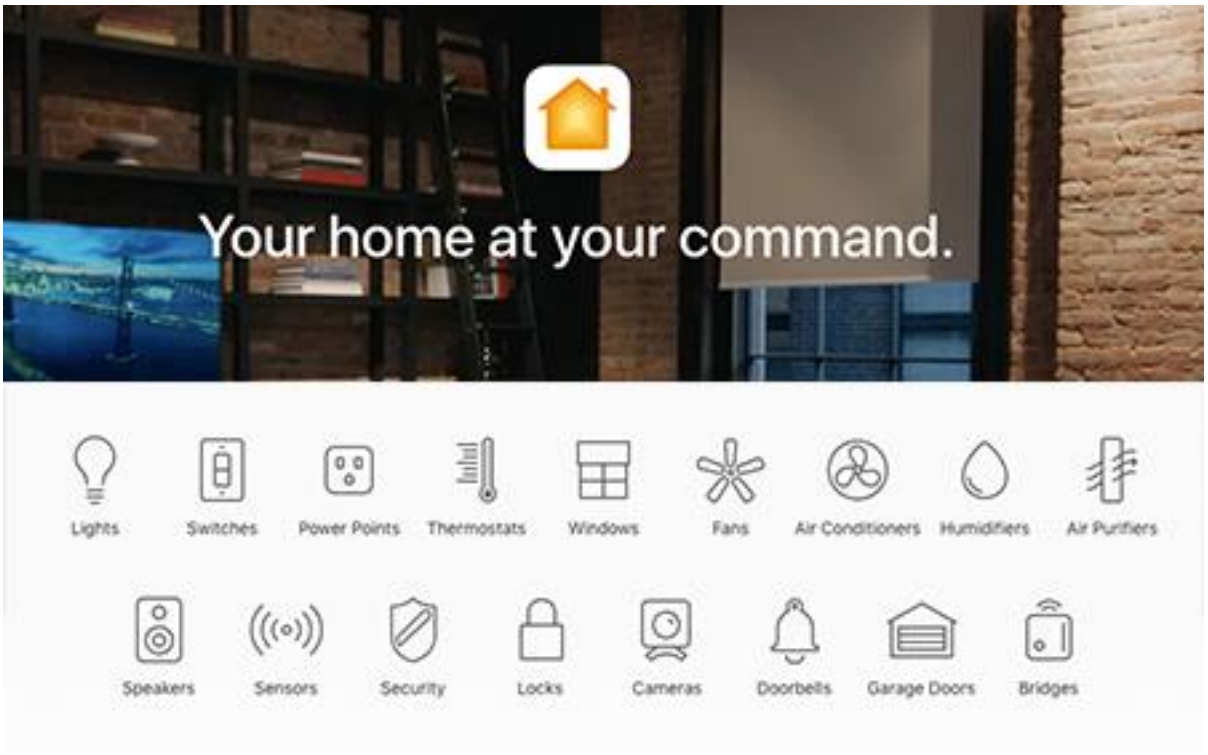


Рисунок 2.3 - Можливості керування автоматизованої системи Apple Home Kit

Як видно з рисунку 2.3 автоматизована система Apple Home Kit забезпечує можливість керування освітленням, вимикачами, розетками, термостатами, вентиляторами та кондиціонерами, зчитувати дані з різноманітних датчиків та багато інших функцій.

2.2. Особливості побудови систем безпеки.

Системи безпеки, в тому числі і охоронні системи, глобально поділяються на дві категорії за способом обміну даними між приладами та централлю, а саме: проводові та бездротові.

2.2.1 Проводові системи безпеки.

Прикладом проводової системи безпеки є **Satel (Integra 64 Plus)**.

Завдяки повній відповідності вимогам стандарту EN50131 3, блоки управління INTEGRA Plus ідеально підходять для впровадження передових систем безпеки в місцях з особливо високим ризиком крадіжки, таких як банки, ювелірні магазини або комунальні послуги. Блоки управління характеризуються розширеною функціональністю, завдяки чому їх можна використовувати для впровадження систем контролю доступу або навіть інтелектуальних будівельних рішень. Зовнішній вигляд плати керування INTEGRA 64 Plus наведено на рис 2.4.

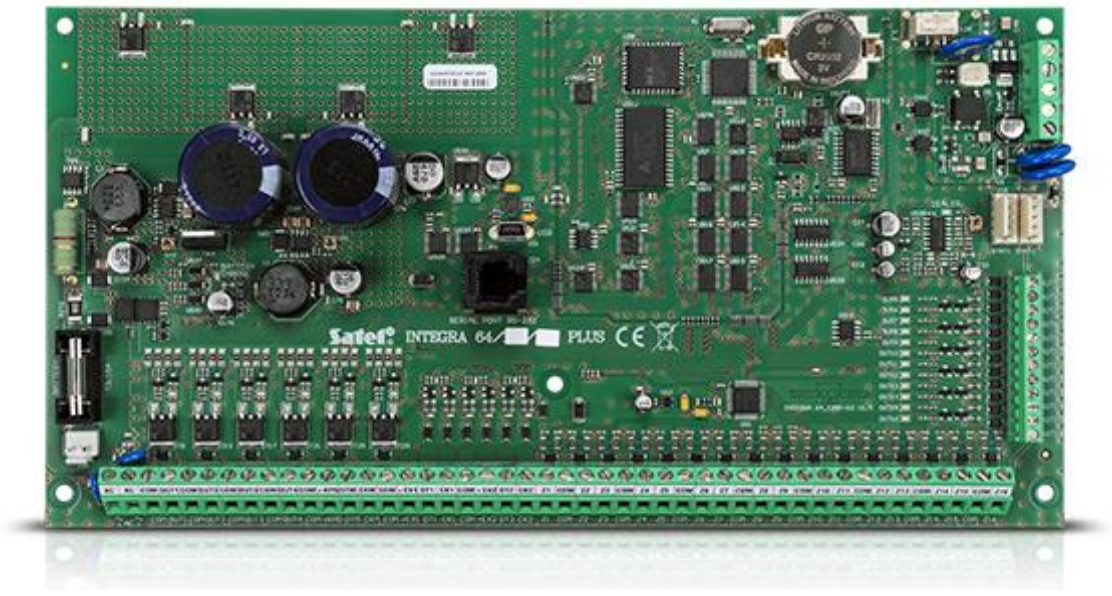


Рисунок 2.4 - Основна плата панелі керування сигналізацією INTEGRA 64 Plus із від 16 до 64 зонами та виходами

- повна відповідність стандартам EN50131 для обладнання класу 3

- вбудований розширений блок живлення 2 А+1,5 А з розширеною автодіагностикою
- до 64 зон з програмованим значенням EOL та підтримкою 3 конфігурацій EOL
- USB -порт для програмування через ПК
- до 32 розділів, 8 об’єктів
- до 64 повністю програмованих виходів
- виділені шини для зв'язку з клавіатурами та модулями розширення
- управління системою через сенсорні клавіатури, РК-клавіатури, розділові клавіатури, брелки дистанційного керування або безконтактні карти
- віддалене управління системою за допомогою ПК, смартфона або телефонного меню з голосовим керуванням
- 64 незалежних таймера для автоматичного керування
- функції контролю доступу та автоматизації будинку
- енергонезалежний журнал подій з 5631 записами, з підтримкою он-лайн друку
- підтримка 192+8+1 кодів користувачів
- оновлення прошивки через ПК
- можливість не повідомляти про можливі проблеми з підключенням до сервера SATEL як про помилку [7].

На даний момент спостерігається тенденція ринку на перехід до безпровідних систем оскільки вони мають ряд переваг. А саме: простіша в установці, не потребує додаткових матеріалів для підключення сенсорів до централі, використовує внутрішні закриті протоколи (наприклад в охоронних системах), або загальноприйняті та доступні (Wi-Fi, Z-Wave, ZigBee), для легкого масштабування власної мережі сторонніми датчиками.

2.2.2 Бездротові системи безпеки.

Прикладом бездротових систем є Hikvision, Tyco Security Products, Ajax Systems

Hikvision

Бездротова панель управління безпекою AX містить 32 бездротові зони, підтримує способи зв'язку Wi-Fi, TCP/IP та GPRS/3G/4G. Вона також підтримує ISAPI, Hik-Connect та DC-09, що застосовуються для таких об'єктів: магазин, будинок, фабрика, склад, офіс тощо. Зовнішній вигляд бездротової системи AX Hub Kit (868MHz) наведено на рис 2.5.

Рисунок 2.5 - Бездротова системи безпеки AX Hub Kit (868MHz)

- Комплект концентратора AX (868 МГц)
- Підтримує до 32 бездротових входів, 4 розширювачі бездротових виходів
- Пропонує кілька способів спілкування: LAN + Wi-Fi
- До 2 каналів. бортова відеоперевірка

- Забезпечує надійний захист за допомогою двосторонньої бездротової технології
- Бездротове з'єднання скорочує час установки
- Зв'язок на відстані до 800 м (на відкритих майданчиках)
- Підтримує постановку/зняття з охорони шляхом переміщення картки з вбудованим безконтактним зчитувачем
- Містить DS-PWA32-HGR (білий, 868 МГц) x 1
- DS-PD2-P10P-W x 1
- DS-PD1-MC-WWS x 1 [8]

Tyco Security Products

Tyco Security Products та ціла низка брендів становлять одну з найбільших корпорацій безпеки у світі. Інженери, що э спеціалістами з відео безпеки, контролю доступу, безпеки на основі місцезнаходження та безпеки вторгнення, надають Tyco Security Products конкурентну перевагу, коли мова йде про системну інтеграцію [9].

На прикладі бренду Visonic розглянемо панель сигналізації, яка є однією з найбільш популярних за реалізацією систем на ринку - PowerMaster-10 G2.

Компактна бездротова контрольна панель Series PowerG PowerMaster-10 G2. Бездротова контрольна панель на 30 зони охорони з двостороннім протоколом обміну PowerG. Ідеальне рішення для захисту квартири і невеликого офісу. Підтримка відеопідтвердження тривог. Завдання, які вирішуються: безпека, запобігання аварійним ситуаціям і екстрений викликів. Зовнішній вигляд бездротової системи PowerMaster-10 G2 наведено на рис 2.6.

Рисунок 2.6 - Панель PowerMaster-10 G2

Функціональні можливості PowerMaster-10 G2:

- Підтримка протоколу PowerG.
- Помаранчевий ЖК-дисплей.
- 30 радіоканальних зон + 1 дротова зона.
- 3 незалежних розділи охорони + 1 загальний розділ.
- Підтримка більше 40 радіоканальних пристроїв: 8 клавіатур, 8 брелків, 2 сирени, 1 ретранслятор.
- 8 кодів користувачів і 8 безконтактних жетонів.
- Повне управління системою з мобільного телефону.
- SMS повідомлення на телефони користувача.
- Канали, які підтримує панель: PSTN, GSM, GPRS, SMS.
- Вбудована сирена: 85дБ / 3м.
- 1 порт RS232 [10].

Ajax Systems

StarterKit - стартовий комплект системи безпеки Ajax. Складається з хаба, датчика руху, датчика відчинення та брелка з тривожною кнопкою. Зовнішній вигляд бездротової системи Ajax Starter Kit наведено на рис 2.7.

Рисунок 2.7 - Стартовий комплект системи безпеки Ajax.

- Комплектація: інтелектуальна централь, бездротовий датчик руху, бездротовий датчик відкриття, бездротовий брелок
- Максимальна кількість пристроїв у системі - 100
- Максимальна кількість користувачів - 50
- Мобільні застосунки: iOS 11.0 і вище, Android 4.4 і вище
- Час доставки сигналу тривоги - 0,15 с
- Радіопротокол Jeweller
- Канали зв'язку - Ethernet, GSM (850/900/1800/1900 МГц)
- Підтримка SIM-карт - Micro SIM 2G
- Відеоспостереження - до 10 камер або відеореєстраторів
- Строк служби - до 10 років [11].

2.3. Датчики для систем безпеки. Типи та особливості

При виборі датчиків для об'єкту необхідно враховувати перешкоди різного роду: теплові, інфрачервоні, акустичні. Контрольний рівень таких датчиків повинен бути набагато вище можливих перешкод.

Отже, на сьогоднішній день існують наступні типи датчиків охоронної системи:

- Об’ємний датчик або датчик руху
- Магнітно-контактний датчик або датчик відкриття
- Радіохвильовий датчик
- Датчик розбиття скла
- Вібраційний датчик
- Комбінований датчик

Почнемо із самого розповсюдженого датчика, який базується на принципі фіксації зміни потоку тепла, яке випромінюється людським тілом при перетині зон, які охороняються.

Об’ємний датчик або датчик руху вловлює переміщення об'єкта з інфрачервоним (тепловим) випромінюванням. Сучасні об’ємні датчики дозволяють розрізняти людину та домашніх тварин. Загалом використовуються для захисту житлових приміщень, володіють високою надійністю та низькою ціною.

Дані в ІЧ-датчику аналізуються аналоговим засобом чи з використанням цифрових технологій. Оптимальним місцем для розміщення ІЧ-датчиків є стіни. Не рекомендується ставити біля джерел тепла, вентиляційних отворів та інших місць теплових перешкод. Сучасні ІЧ-датчики характеризуються більшим різноманіттям можливих форм та діаграм направленості.

Магнітно-контактний датчик або датчик відкриття – другий за розповсюдженістю датчик. Встановлюється локально на дверях та вікнах. При відкритті вікна чи дверей відбувається видалення магніту, встановленого на рухомій частині від геркону, розташованого в нерухомій частині, що визиває його спрацювання. Це найнадійніший та недорогий тип датчика.

Радіохвильовий датчик виявляє переміщення будь-яких рухомих предметів. Він посилає та аналізує прийнятий відбитий сигнал. В основному використовується в офісах, довгих коридорах та приміщеннях з високою температурою. До недоліків відноситься можливість хибного спрацювання при русі будь-яких предметів чи рідин за матеріалами, які пропускають ці радіохвилі (наприклад, пластикові труби системи водопроводу чи каналізації).

Датчик розбиття скла спрацьовує на звук розбиття скла. Він аналізує частотний діапазон і може розрізняти звуки розбиття скла різних типів (звичайне, армоване, склопакет). Широко використовується у всіх типах приміщень.

Вібраційний датчик спрацьовує при вібрації поверхні, на якій він закріплений. Встановлюється, в основному, в нежитлових приміщеннях в поєднанні з іншими датчиками для додаткового захисту стін від пролому (комора цінностей, банк та ін.)

Комбіновані датчики, звані також датчиками подвійний технології, з’явилися відносно недавно і в даний час стають все більш популярними. Перевага таких датчиків полягає в істотному зниженні частоти помилкових сигналів «тривога». Це досягається за рахунок того, що в одному датчику використовується комбінація двох різних фізичних принципів виявлення [12].

Зразки продукції від компанії Ajax Systems наведені на рис 2.8.

Рисунок 2.8 - Лінійка пристроїв компанії Ajax Systems

На рисунку 2.8. зображені зразки продукції компанії Ajax Systems: інтелектуальна централь, бездротовий датчик руху, бездротовий датчик відкриття, бездротовий брелок та інші.

Висновки до розділу 2

Системи безпеки, в тому числі і охоронні системи, глобально поділяються на дві категорії за способом обміну даними між пристроями та централлю, а саме: проводові та бездротові.

Проводові системи мали перевагу в швидкості передачі даних в надійності каналу зв'язку. Однак на даний момент радіо технології не поступаються провідному підключенню і все більше систем починають використовувати різні технології.

Оскільки системи переходять на бездротовий зв'язок між пристроєм та централлю необхідно використовувати енергоефективний принцип роботи приладів та протоколи, котрі будуть сприяти низькому споживанню енергії, так як вони працюють виключно від батареї на противагу підключення до шини (через яку прилад має живлення від централі).

Тож бездротові системи безпеки необхідно будувати з урахуванням даних параметрів.

Розділ 3. Порівняльний аналіз бездротових систем безпеки

В бездротовій системі безпеки кінцевий пристрій (датчик) спілкується з централлю без дротів. Користувачу не потрібно фізично підключати його до решти системи або підключати до свого дому. Він спілкується з іншими пристроями та будь-якими службами моніторингу за допомогою Wi-Fi, Bluetooth, радіочастот або стільникових сигналів.

3.1. Перелік і технічні характеристики радіопротоколів для систем безпеки.

Системи безпеки часто використовують внутрішні радіопротоколи для того, щоб зловмисникам було важче підібрати пакети та зламати систему. Розглянемо декілька системи безпеки.

Visonic Ltd. використовує свій радіопротокол - Power G.

Visonic Ltd. — міжнародний розробник і виробник високоякісних електронних систем безпеки та компонентів. Прості у використанні та інноваційні системи домашньої безпеки та компоненти є життєво важливими частинами повсякденного сімейного життя для людей будь-якого віку. Забезпечуючи зв’язок у режимі реального часу між сім’ями, будинками, майном, особами, які надають допомогу, і мережами підтримки громади, компанія надає людям можливість продовжувати своє повсякденне життя з повною впевненістю, що люди та речі, про які вони найбільше піклуються, є безпечними та комфортними.

Power G — це революційна бездротова технологія Visonic для систем охоронної сигналізації. Це буквально перевизначає надійність бездротової сигналізації про вторгнення. І він повністю відповідає найвимогливішим потребам і вимогам, які стоять перед індустрією безпеки сьогодні, а також викликам завтрашнього дня.

Система безпеки та розумного будинку **Ring Alarm** використовує Z-Wave та Wi-Fi.

Ring Alarm – це доступна і комплексна система безпеки будинку своїми руками. Створена для зниження рівня злочинності, ця настроювана система безпеки підвищує ефективність дверних дзвінків, кулачків та аксесуарів Ring. Повна інтеграція Ring Alarm і всієї лінійки продуктів Ring через додаток Ring захищає будинки як зсередини, так і ззовні.

Z-Wave – це радіо протокол, який спочатку замислювався для використання в домашній автоматизації. Чіпи для Z-Wave пристроїв виготовляє компанія Silicon Labs, а протокол суворо стандартизований від фізичного рівня передачі даних до прикладного рівня. Всі пристрої Z-Wave проходять обов'язкову сертифікацію, яку контролює Z-Wave Alliance. Сертифікація гарантує сумісність пристроїв Z-Wave всіх виробників у світі. На даний момент до Z-Wave Alliance входить понад 700 компаній, що виробляють понад 3000 сумісних між собою пристроїв.

Рисунок 3.1 – Способи керування системою безпеки Ring

Ajax Systems використовує свій радіопротокол - Jeweller.

Ajax — охоронна сигналізація для квартири, будинку, офісу, яку легко встановити власноруч. Обравши Ajax, користувачі отримують комплексний захист із миттєвою реакцією, стійку до злому та зручну в керуванні охоронну систему. Сигналізація Ajax виконує не одну, а одразу три захисні функції: миттєво повідомляє, якщо в дім забралися грабіжники, з’явився дим або почався потоп. До неї підключаються відеокамери стеження сторонніх виробників, що перетворює Ajax на єдиний центр безпеки [13].

Jeweller - це розроблений Ajax Systems протокол радіозв'язку, що гарантує безперебійну взаємодію хаба та пристроїв системи безпеки. Радіопротокол Jeweller дозволяє будувати як малі, так і великі системи безпеки з 200 пристроїв під управлінням однієї централі — хаба. Пікової дальності зв'язку між пристроями 2000 метрів і площею покриття радіомережі до 12 км² достатньо для захисту квартир, приватних будинків, комерційної нерухомості та офісів [14].

3.2. Порівняння протоколів. Ajax, Visonic/DSC (Power G), LoRa.

Таблиця 3.1 – Порівняння радіопротоколів Jeweller, LoRa, Power G.

	Jeweller	LoRa	Power G
Дальність	до 2 км	до 15 км	до 2 км
Потужність радіосигналу	до 25 мВт	до 25 мВт	до 25 мВт
Час доставки тривоги	0.15 с	-	-

Шифрування	Блочне шифрування даних з плаваючим ключом. (Алгоритм на основі стандарту AES)	AES - 128	AES - 128
Автономність	до 7 років	до 10 років	до 8 років
Тип зв'язку	двосторонній	двосторонній	двосторонній
Частотний діапазон	868,0 – 869,2 МГц 915 МГц	433 МГц, 863-870 МГц 470 – 510 МГц 779 – 787 МГц 902 – 928 МГц 2.4 ГГц	433 - 434 МГц 868 - 869 МГц 912 - 918 МГЦ
Чутливість	-120 dBm	-148 dBm	-
Відношення сигнал/шум	-	на 20 dB нижче рівня шуму	-

3.3. Порівняння функціональних особливостей систем безпеки

Для порівняння розглянемо дві централі: Ajax Hub першого покоління (виробник Ajax Systems) і систему PowerMax 30 (виробник Visonic Ltd).

Характеристики Ajax Hub:

- Централь радіоканальна з модулями GSM і Ethernet
- Пристроїв, що під'єднуються – 100
- Користувачів – 50

- Кімнат – 50
- Груп – 9
- Мобільний застосунок - iOS 11.0 і вище, Android 4.4 і вище
- Канали зв’язку - Ethernet, GSM (850/900/1800/1900 МГц)
- Зв’язок з пультом охорони - Contact ID, SIA
- Операційна система - OS Malevich
- Живлення

  110−250 В від мережі або 12 В з 12V PSU для Hub/Hub Plus/ReX

  Вбудований резервний акумулятор: Li-Ion 2 А·год

  До 15 годин автономної роботи при вимкненому Ethernet

  Енергоспоживання від мережі — 10 Вт
- Радіопротокол Jeweller
- Підтримка SIM-карток - Micro SIM 2G
- Діапазон робочих температур - Від -10°C до +40°C
- Антисаботаж

  Захист від фальсифікації

  Повідомлення про глушіння

  Тампер на відкривання та відривання
- Відеоспостереження - До 10 IP камер або відеореєстраторів
- Віддалене налаштування
- Розміри - 163 × 163 × 36 мм
- Вага - 350 г
- ReX, що під'єднуються – 1
- Під’єднуваних сирен - до 10
- Сценаріїв – 5
- Підтримка датчиків MotionCam – Hi [15].

Характеристики PowerMaster-30 G2:

- До 64 зон, 32 клавіатури, 32 брелки, 8 сирен, 4 ретранслятора
- 48 кодів користувача
- Груп – 3
- 2 дротових зони, 1 дротова сирена та 1 програмований вихід
- Вбудований номеронабирач PSTN
- Канали зв’язку - 3G, GSM/GPRS та IP
- Зберігає 1000 записів журналу
- Додатковий зчитувач
- Дистанційне налаштування та діагностика з індикацією стану системи
- Широкий асортимент периферійних пристроїв Power G для будь-якого застосування
- Дистанційне оновлення програмного забезпечення [10].

Всі системи безпеки, в тому числі і ті, які розглянуті в даному пункті, призначені для інформування користувачів про тривожні сигнали завдяки сирені на об’єкті або push-повідомлень в мобільному додатку.

Висновки до розділу 3

Бездротові системи безпеки за використаними протоколами можна поділити на дві категорії: ті, які використовують загальнодоступні протоколи (наприклад Wi-Fi, Z-Wave, Bluetooth) або свої внутрішні протоколи (наприклад Power G або Jeweller).

Однак найбільшою популярністю користуються змішані системи, котрі мають підтримку і загальнодоступних протоколів, і внутрішніх протоколів. Саме завдяки цьому користувач може досить гнучко налаштувати свою систему підключивши охоронні датчики використовуючи внутрішні протоколи, а датчики для автоматизації підключити використовуючи загальнодоступні протоколи.

Результати порівняння радіопротоколів Jeweller, LoRa, Power G показують, що технологія LoRa має ряд суттєвих переваг [16]. А саме:

- велику дальність дії
- високу чутливість
- можливість приймати сигнали, рівень яких може бути менше рівня завад до 20 dB
- висока енергоефективність

Таким чином бездротові система безпеки, побудована на технології LoRa, може скласти конкуренцію існуючим системам за рахунок можливості розташування елементів системи на великих відстанях, підвищеної завадостійкості, довго тривалість автономної роботи пристроїв.

Розділ 4. Опис запропонованої бездротової системи безпеки на основі протоколу LoRa.

4.1. Вимоги до системи та її структура

Системи безпеки з бездротовим каналом передачі даних повинна відповідати наступним вимогам:

- Забезпечувати сигналізацію про вторгнення шляхом передачі користувачу відповідного сигналу з датчиків руху або датчиків розбиття скла у приміщенні або сигналу з вуличного датчику руху.
- Забезпечувати сигналізацію про пожежу шляхом передачі користувачу відповідного сигналу з датчиків диму або датчиків підвищення температури.
- Забезпечувати сигналізацію про протікання води шляхом передачі користувачу сигналу з відповідного датчику.
- Забезпечувати включення-виключення пристрою сповіщення (сирени).
- Забезпечувати можливість налаштування параметрів системи за допомогою брелка для керування системою безпеки з тривожною кнопкою та захистом від випадкових натискань та кімнатної сенсорна клавіатура для керування системою безпеки

Схема взаємодії елементів системи безпеки на основі LoRa наведена на рис. 4.1. Структура система схожа зі структурою системи безпеки від компанії Ajax Systems [15] і містить такі основні складові:

- охоронні датчики
- інтелектуальний шлюз з процесорним вузлом (хаб)
- хмарний сервіс
- користувацькі застосунки

Кінцевий пристрій– це всі типи датчиків або виконавчих пристроїв, які за допомогою мікроконтролера підключені до шлюзу через радіочастотний канал LoRa [17]. Мікроконтролер також контролює рівень напруги живлення і забезпечує гарантовану доставку повідомлення шлюзу.

При виготовленні, пристроям на основі LoRa присвоюється унікальні ідентифікатори. Ці ідентифікатори використовуються для безпечної активації та адміністрування пристрою, забезпечення безпечного транспортування пакетів через приватну або загальнодоступну мережу та доставки зашифрованих даних у Хмару.

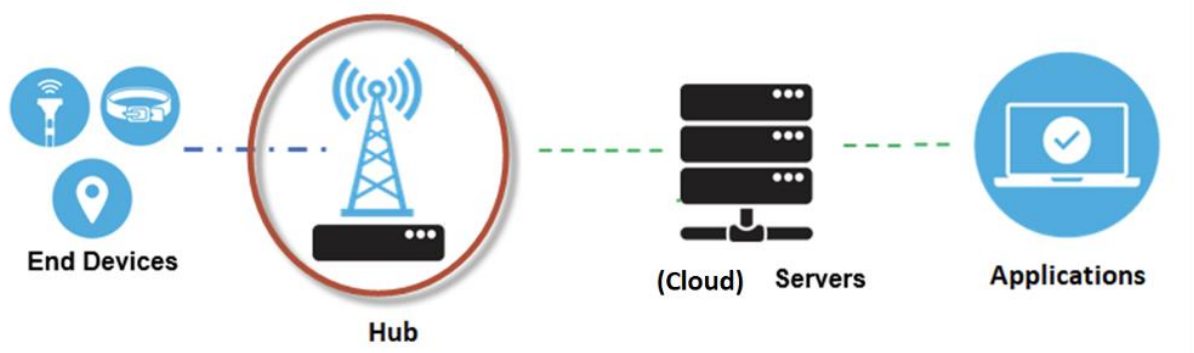


Рисунок 4.1. - Структура безпровідної системи безпеки на основі LoRa

Інтелектуальний шлюз отримує радіочастотні повідомлення з модуляцією LoRa від будь-якого кінцевого пристрою і аналізує їх. В першу чергу хаб перевіряє цілісність даних кожного вхідного повідомлення LoRa RF. Якщо цілісність порушена, тобто якщо CRC неправильний, повідомлення буде видалено і видано запит на повторне повідомлення. В залежності від типу датчика шлюзом приймається рішення про сповіщає користувачів та охоронну компанію та / або включення сирени. Також шлюз контролює стан живлення кінцевих пристроїв, наявність каналу, спроби демонтажу чи втрату зв'язку з пристроєм і при необхідності сповіщає користувача.

На основі рівнів RSSI кінцевих пристроїв шлюз визначає алгоритм взаємодії з ними для забезпечення надійного каналу зв’язку. IP-трафік від

шлюзу до хмарного сервера може передаватися через Wi-Fi, проводовий Ethernet або через стільникове з’єднання.

Хмарний сервіс використовується для забезпечення надійного зв’язку між шлюзом і застосунками користувача, а також для збереження інформації. Роботу шлюзу та кінцевих точок можна налаштовувати та контролювати з будь-якого місця через застосунки для смартфона та ПК. Через застосунки також відслідковується наявність зв'язку з хмарним сервісом. Дані про події користувач може отримувати в сповіщеннях, у застосунках для смартфона та ПК, а також в SMS та за дзвінками від шлюзу.

Користувацьке програмне забезпечення повинно мати широкий функціонал для адміністрування системи, а саме:

- додавати користувачів і керувати їхніми правами;
- створювати групи користувачів;
- переглядати історію подій;
- керувати налаштуванням та режимами охорони.

4.2. Опис апаратного забезпечення

Апаратним забезпеченням системи є власне кінцеві точки з датчиками та інтелектуальний шлюз.

4.2.1. Опис кінцевої точки охоронної системи

До складу кінцевої точки входить датчик або декілька датчиків, мікроконтролер з вбудованим радіочастотним трансивером, антена та батарея живлення.

Основним елементом системи є 32-х бітний мікроконтролер серії STM32WL від компанії STMicroelectronics. Мікроконтролери STM32WL оснащені радіоприймачем/передавачем для субгігагерцового на базі чипа Semtech SX126x, для використання у широкому спектрі бездротових

додатків малопотужної глобальної мережі (LPWAN), у промислових та побутових мережах Інтернету речей (IoT). Побудовані на ядрах Arm® Cortex®-M4 і Cortex®-M0+, мікроконтролери STM32WL підтримують декілька видів модуляції – LoRa®, (G)FSK, (G)MSK, BPSK – для роботи з різними бездротовими протоколами LoRaWAN®, Sigfox, W-MBUS, mioty® або будь-яким іншим відповідним протоколом у повністю відкритий спосіб.

Особливості архітектури мікроконтролера STM32WL [18]:

Радіоканал. Мікроконтролери STM32WL відповідають вимогам фізичного рівня специфікації LoRaWAN®, опублікованої LoRa Alliance®. Доступні модуляції LoRa®, (G)FSK, (G)MSK і BPSK також можуть використовуватися в інших протоколах, таких як Sigfox або W-MBUS, та ін.

Радіоприймач підходить для систем, які відповідають нормам радіозв'язку, включаючи, але не обмежуючись, ETSI EN 300 220, FCC CFR 47, частина 15, нормативні вимоги Китаю та японський ARIB T-108. Безперервне частотне покриття від 150 до 960 МГц забезпечує підтримку всіх основних діапазонів ISM субгігагерцового діапазону у всьому світі.

Системні периферійні пристрої. Мікроконтролери STM32WLEx (одноядерний M4) і STM32WL5x (двоядерний M4 і M0+) включають широкий спектр комунікаційних функцій, включаючи до 43 входів-виходів загального призначення, вбудоване джерело живлення ключового типу для оптимізації енергоспоживання, кілька режимів низького енергоспоживання для максимального терміну служби акумулятора. Подвійна вихідна потужність і широкий лінійний діапазон частот достатні для широкого спектру застосунків.

Серія STM32WL, розроблена з використанням тієї ж технології, що реалізована в мікроконтролерах STM32L4 з надмалопотужним споживанням енергії, дає можливість підключати аналогово-цифрові та аналогові

периферійні пристрої для створення систем, які потребують тривалого терміну служби батареї та великого радіочастотного діапазону на частотах роботи трансивера нижче 1ГГц.

Безпека та ідентифікація. На додаток до своїх бездротових функцій і особливостей з наднизьким енергоспоживанням, мікроконтролери STM32WL включають вбудовані апаратні функції безпеки, такі як 128-/256-бітове апаратне шифрування AES, захист від читання/запису PCROP і прискорювач відкритих ключів і криптографічний механізм з еліптичним ключем.

Для роботи з датчиками кінцевої точки у більшості випадків достатньо контролера STM32WLEx (одноядерний M4). Основні електричні характеристики такого мікроконтролера:

- модуляція: LoRa®, (G)FSK, (G)MSK і BPSK
- чутливість приймача: –123 дБм для 2-FSK (при 1,2 Кбіт/с), –148 дБм для LoRa® (на 10,4 кГц, коефіцієнт розповсюдження 12)
- вихідна потужність, програмована до +22 дБм
- струм споживання у режим вимкнення (Shutdown): 31 нА
- струм споживання у режим очікування (Standby): 360
- струм споживання у режимі прийому: 4,82 мА
- струм споживання у режимі передачі: 15 мА при 10 дБм і 87 мА
- при 20 дБм (LoRa® 125 кГц)
- апаратне шифрування AES 256-біт
- унікальний ідентифікатор пристрою (сумісний із 64-бітним UID
- зі стандартом IEEE 802-2001)
- 96-бітовий унікальний ідентифікатор кристала

Структурну схему кінцевої точки доступу на мікроконтролері STM32WLE4 наведено на рис. 4.2.

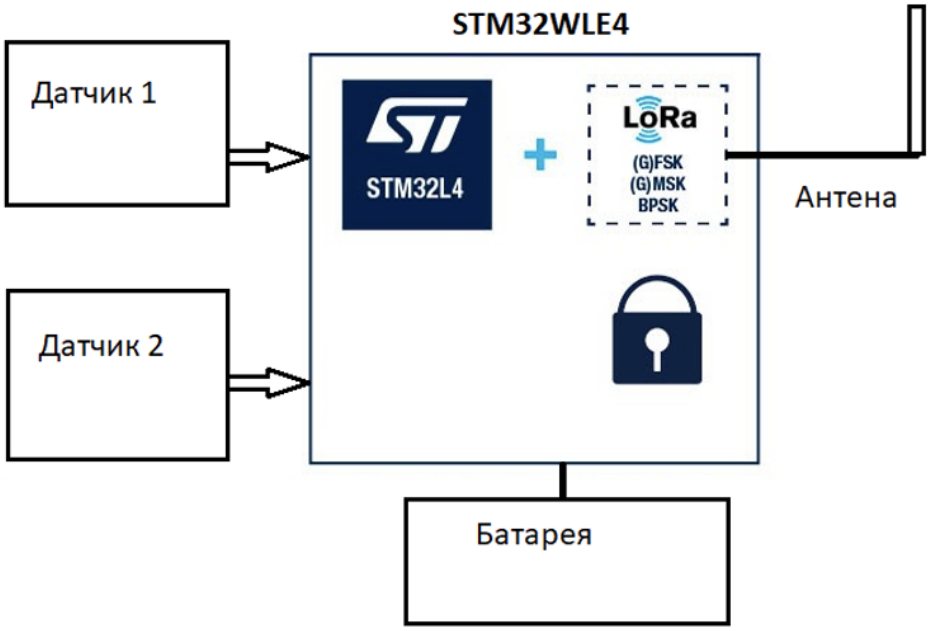


Рисунок 4.2 Кінцева точка системи на мікроконтролері STM32WLE4

У випадку необхідності передачі великих об’ємів даних від відеокамери можна використати модуль LoRa з робочою частотою передачі даних в 2,4 ГГц. Трансивер LoRa SX1280 діапазону 2,4 ГГц забезпечує високу чутливість, (до -132 дБм), вихідну потужність в +12,5 дБм та низьке споживання енергії [19]. Трансивер LoRa SX1280 забезпечує швидкість передачі даних до 250 кБіт/с. У порівнянні з іншими технологіями, що працюють у діапазоні 2,4 ГГц, LoRa забезпечує більший радіус дії, який становить до 800 м на відкритій місцевості. Радіус дії останнього стандарту Bluetooth становить 50 м і 165 м у приміщенні та на вулиці відповідно. Максимальний діапазон Wi-Fi мереж 2,4 ГГц зазвичай коливається близько 100 м. Таким чином, зовнішній діапазон LoRa більш ніж у п’ять разів більший, ніж зовнішній діапазон BLE 5, і більш ніж у вісім разів більший у порівнянні із типовими мережами IEEE 802.11 [20]. Також LoRa SX1280 надає можливість вимірювання відстані між точками мережі, що також може бути корисним [21] в системі безпеки. Структурну схему кінцевої точки доступу з відеокамерою та трансивером LoRa SX1280 наведено на рис. 4.3.

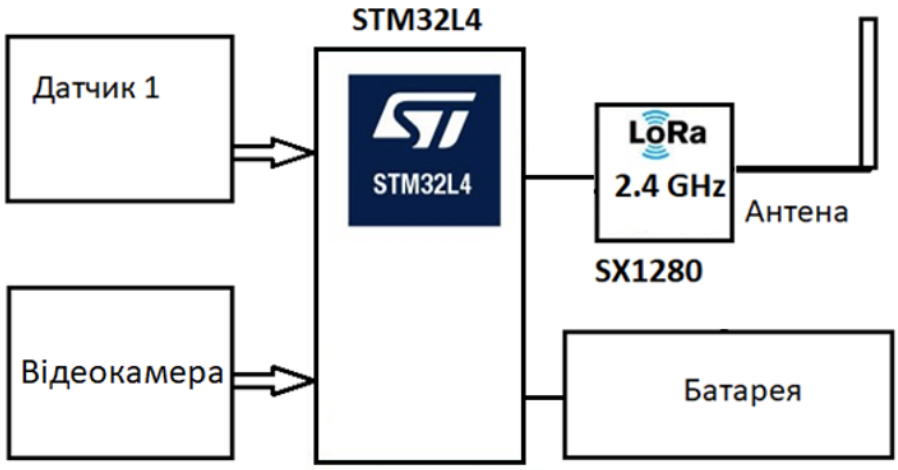


Рисунок 4.3 Кінцева точка з трансивером LoRa SX1280

Технологія LoRa працює на достатньо низьких швидкостях прийому-передачі і орієнтована в першу чергу на роботу з невеликим об'ємом даних. Однак існують технічні рішення, які забезпечують передачу зображень через радіочастотний канал LoRa [22-24], що також є додатковою перевагою при використанні в безпровідних системах безпеки. Крім того використання частоти 2,4 ГГц також спрощує передачу зображень.

4.2.2. Опис інтелектуального шлюзу охоронної системи

Інтелектуальний шлюз повинен працювати з одного боку з кінцевими пристроями через радіочастотний канал LoRa, з іншого боку шлюз має передавати дані на сервер і отримувати від нього команди та налаштування користувача. Канал зв'язку має бути достатньо надійним щоб без затримок і втрат передавати інформацію. Бажано щоб була можливість вибору технології передачі даних, що дозволить зробити систему більш гнучкою у виборі засобу зв'язку в залежності від умов використання. Отже, для забезпечення підвищеної надійності передачі інформації шлюз може використовувати декілька технологій передачі даних:

- Wi-Fi
- проводовий Ethernet

· стільниковий зв’язок

Шлюз у найпростішому (базовому) варіанті має містити наступні обов’язкові складові: мікроконтролер STM32WL з вбудованим трансивером LoRa з антеною, Wi-Fi модуль, Ethernet контролер, модуль GSM з SIM картою, джерело електроживлення. Структурну схему базового варіанту шлюзу на мікроконтролері STM32WL5x наведено на рис. 4.4.

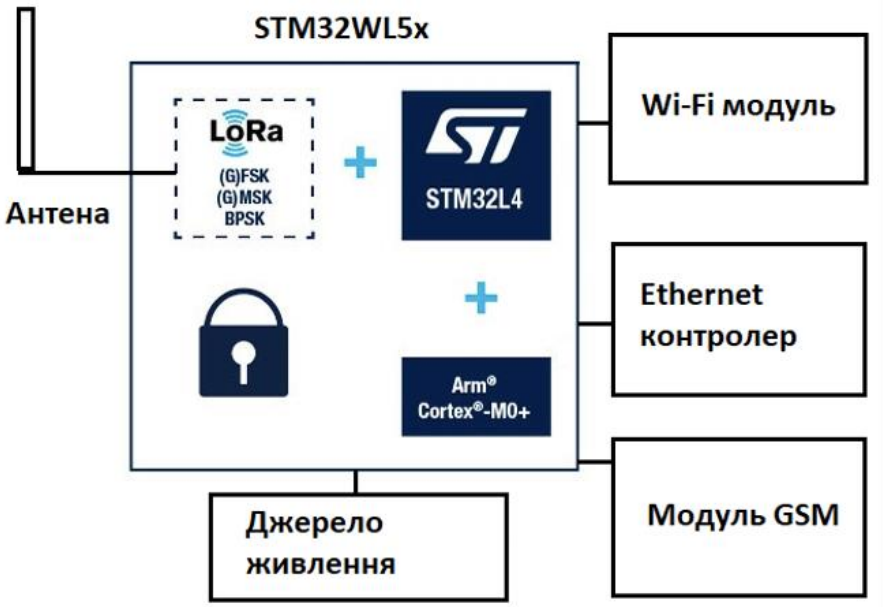


Рисунок 4.4 Базовий варіант шлюзу на мікроконтролері STM32WL5x

Двоядерні M4 і M0+ мікроконтролери STM32WL5x додатково мають розширені функції безпеки, такі як: послуги безпечного керування ключами (SKMS), апаратна ізоляція безпечних зон, безпечне завантаження та безпечне оновлення мікропрограми.

В залежності від кількості кінцевих точок, їх призначення, обсягу виконуваних задач та складності алгоритмів їх виконання може знадобитись більш потужний контролер або процесор під керування вбудованої операційної системи реального часу (RTOS). Особливо у випадках прийому та обробки даних з відеокамери. У цьому випадку шлюз має містити наступні складові: мікропроцесор з RTOS, трансивер LoRa з антеною на частоту 868 МГц [25], Wi-Fi модуль, Ethernet контролер, модуль GSM з SIM картою,

джерело електроживлення. Коли необхідно забезпечити максимальну швидкість передачі даних можна використати модуль LoRa з робочою частотою 2.4 ГГц. Структурну схему шлюзу з більш потужним процесором STM32MP1 і операційною системою реального часу наведено на рис. 4.5.

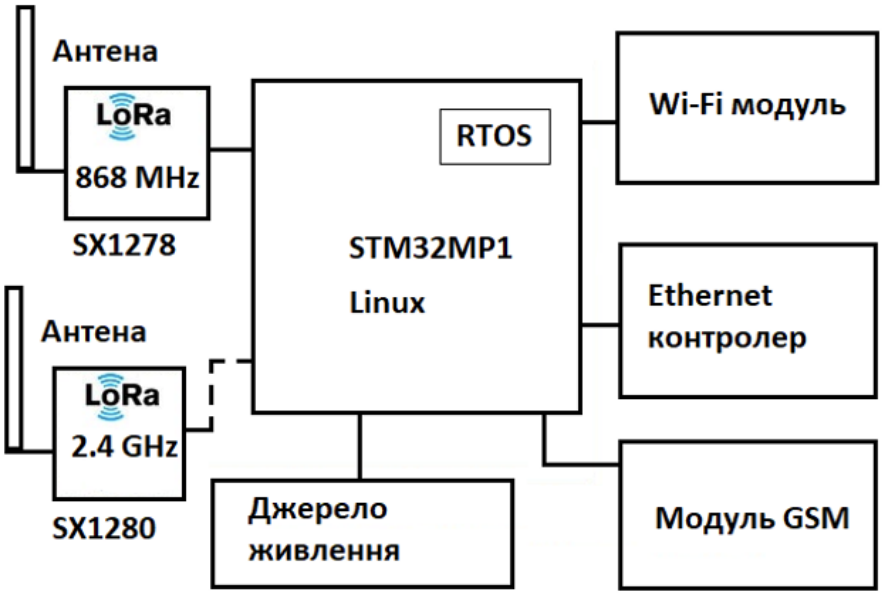


Рисунок 4.5 Високошвидкісний варіант шлюзу на мікроконтролері STM32MP1

Використання трансиверів з різними частотами дозволяє розширити функціональні можливості шлюзу. Наявність декількох каналів зв’язку та джерела живлення з резервним акумулятором робить роботу шлюзу більш надійною.

Окремо потрібно підкреслили що користуючись технологією LoRa можна використовувати як власний протокол передачі-прийому даних, так і протокол LoRaWAN, який об’єднує в мережі The Things Network понад 150 тисяч користувачів зі всього світу [26].

4.2.3. Датчики та виконавчі пристрої системи

Запропонована система має функціонувати з основними типами датчиків, які використовуються в системах безпеки. Перелік датчиків та

виконавчих пристроїв, які можуть бути використані у запропонованій системі наведено нижче.

- Датчик руху
- Датчик розбиття скла
- Датчик відчинення дверей або вікна
- Вуличний датчик руху
- Пожежний датчик
- Датчик протікання
- Тривожна кнопка з захистом від випадкових натискань
- Відеокамера
- Сирена або сповіщувач

Можливе поєднання декількох пристроїв у одній контрольній точці. Наприклад, відеокамера, яка оснащена датчиком руху, для фіксації об’єктів, що рухаються.

Рисунок 4.6 – Система безпеки з IP камерами, датчиками руху та ін.

4.3. Опис програмного забезпечення

Програмне забезпечення охоронної системи містить дві складові: *службові* програми та *користувацьке* програмне забезпечення.

Службові програми забезпечують

- обмін даними між користувацьким ПО та апаратними складовими системи;
- зберігання і обробку даних у хмарному сервісі;
- оновлення програмного забезпечення контрольних точок та шлюзів.

Користувацьке програмне забезпечення дає можливість

- здійснювати моніторинг стану безпеки вибраних та обладнаних територій
- виконувати зміну налаштувань контрольних точок та шлюзів;
- отримувати в режимі онлайн повідомлення про порушення безпеки або вторгнення

4.3.1 Склад користувацького програмного забезпечення

До складу користувацького ПО входять такі програми:

Desktop Control — комплексний додаток для монтажного та моніторингового бізнесу. Включає в себе наступні функціональні блоки: підключення та віддалене налаштування об'єктів, моніторинг та фотоверифікація тривог, адміністрування персоналу та детальний журнал.

Desktop Control дозволяє використовувати обліковий запис компанії, який об'єднує облікові записи співробітників. Керівник може будь-якої миті змінити роль співробітника, вимкнути або видалити його обліковий запис — навіть без фізичної присутності в офісі. Завдяки ролям співробітники мають

доступ тільки до тих модулів програми та інформації, яка їм необхідна для роботи. Кожна операція у програмі фіксується у журналі подій.

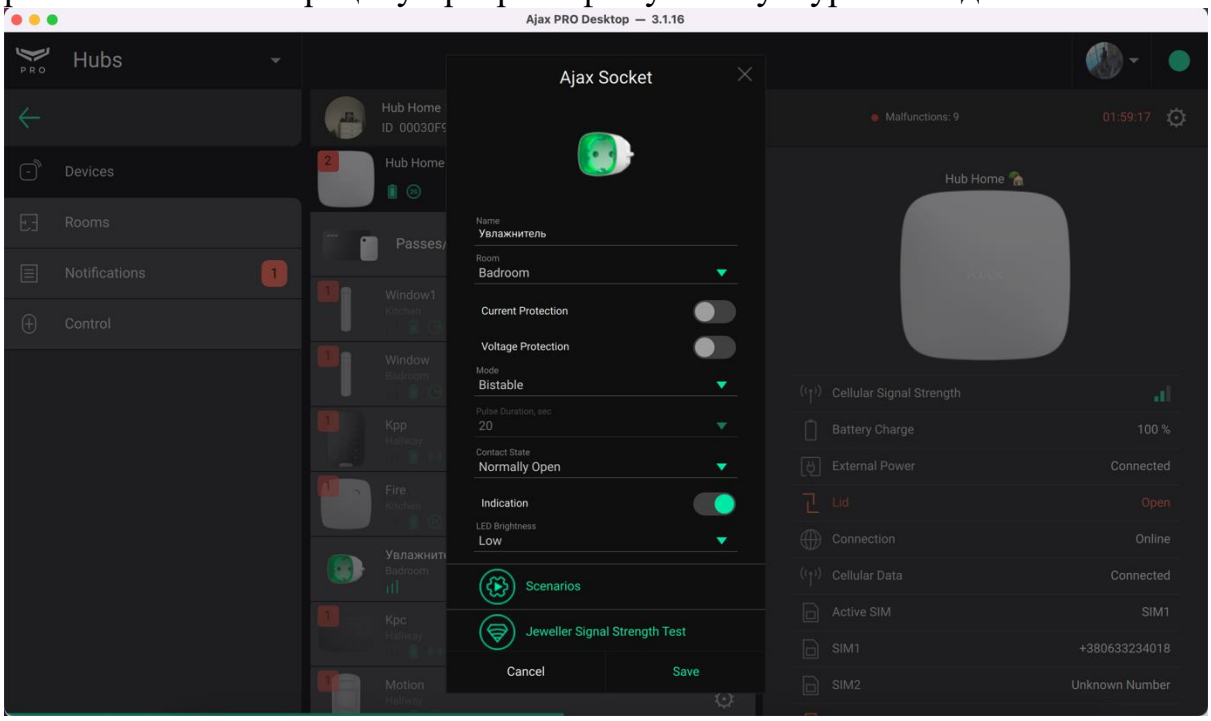


Рисунок 4.7 – Налаштування датчику Socket використовуючи програму Ajax PRO Desktop

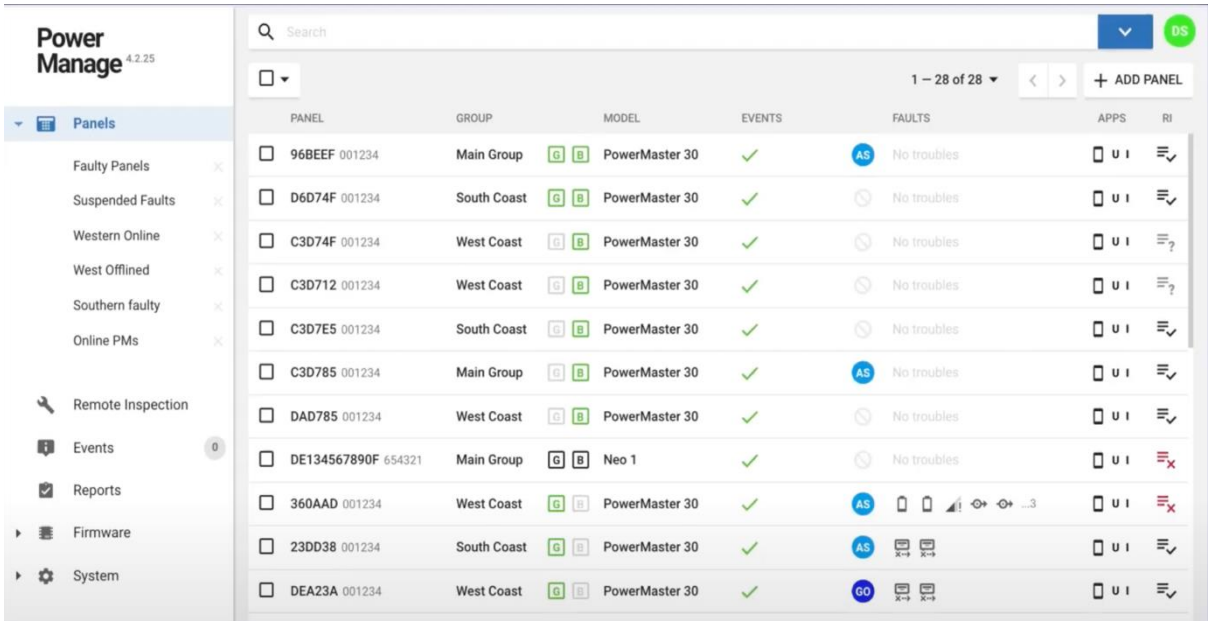


Рисунок 4.8 – Головна сторінка Power Manage зі списком всіх підключених централей

Дані ПО використовуються співробітниками охоронних компаній для надання якісних послуг кінцевим користувачам.

Користувачі, в свою чергу використовують мобільні додатки. Наприклад, аналогічні ConnectAlarm, Ajax Systems або Ring.

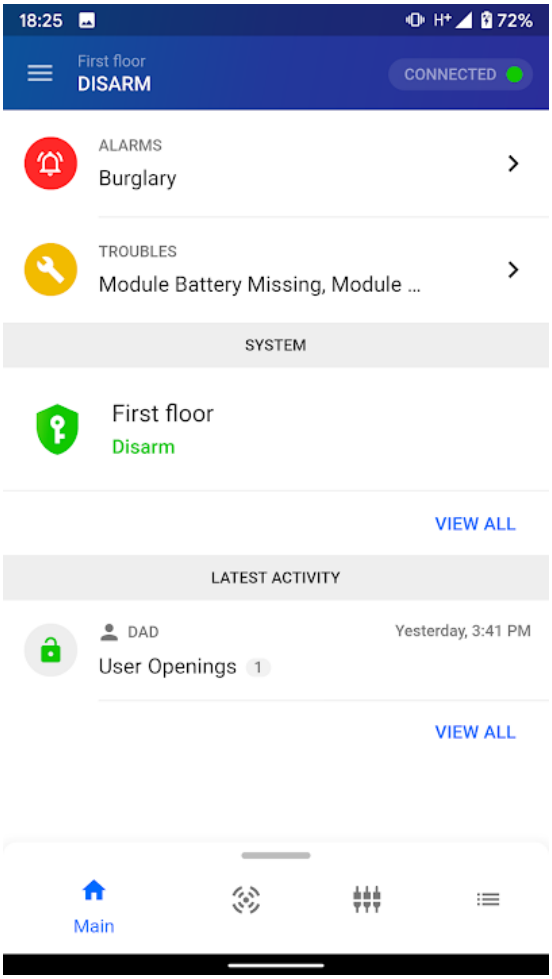
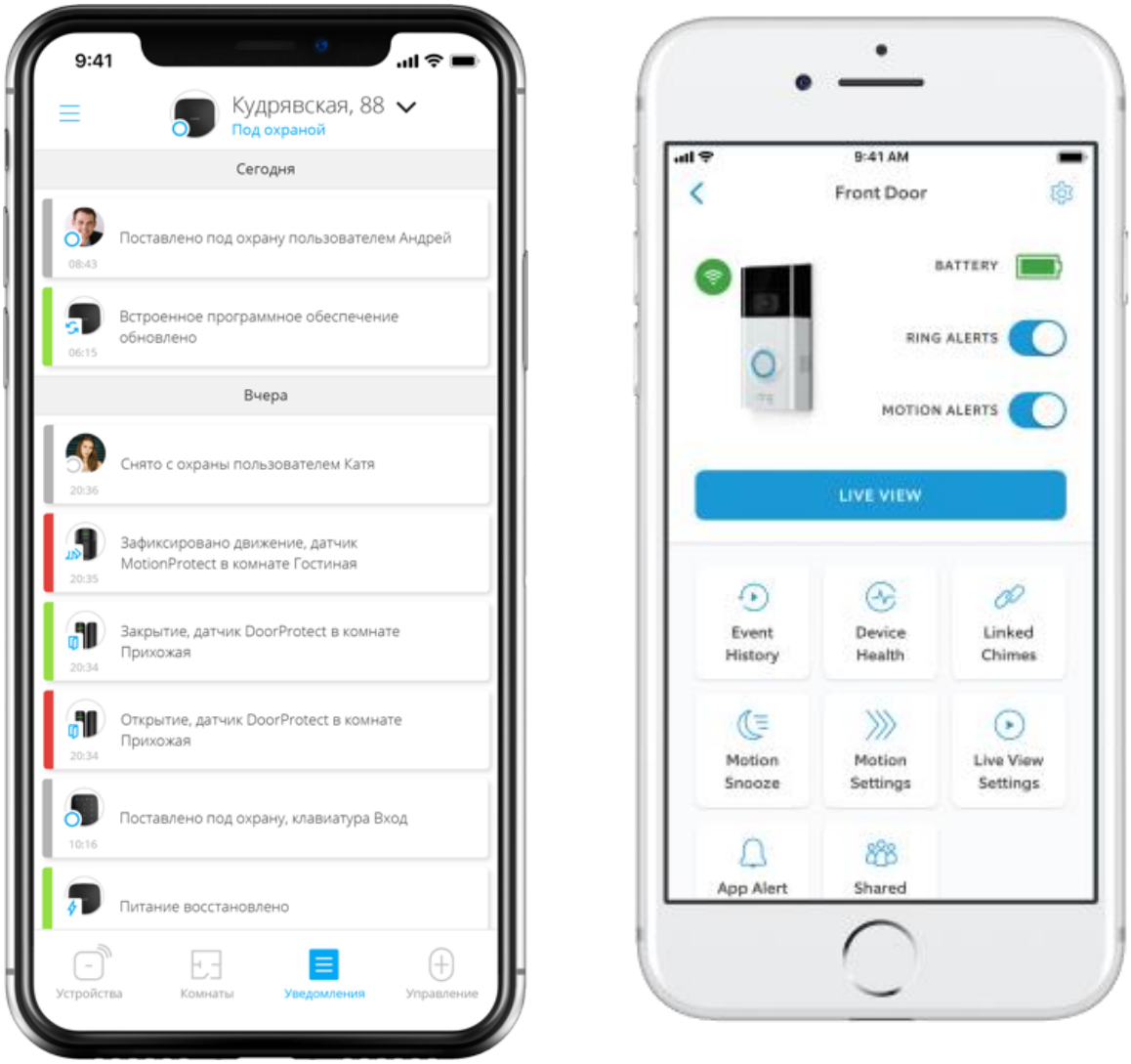


Рисунок 4.9 – Головна сторінка додатку ConnectAlarm



А) Б)

Рисунок 4.10 – А) Перелік повідомлень в додатку Ajax Systems, Б) Сторінка інформації про девайс в додатку Ring Alarm

Висновки до розділу 4

Технологія LoRa має ряд суттєвих переваг над іншими технологіями передачі даних і має дуже хороші перспективи використання у безпроводових системах безпеки. Мікроконтролер STM32WL з вбудованою технологією передачі даних LoRa дає можливість отримати наступні характеристики кінцевої точки:

Можливість використання у широкому діапазоні робочих частот від 150 до 960 МГц, що забезпечує підтримку всіх основних субгігагерцових промислових, наукових та медичних (ISM) діапазонів у всьому світі.

Кількість точок теоретично не обмежена. На практиці - більше 1000

Максимальна відстань передачі даних у зоні прямої видимості - більше 15 км

Термін роботи точки від однієї батареї – більше 10 років

Чутливість приймача: –148 дБм

Перевищення рівня шуму над рівнем сигналу – до 16 дБ

Трансивер LoRa SX1280 з робочою частотою 2,4 ГГц забезпечує швидкість передачі даних до 250 кБіт/с.

Наявність мікроконтроллера STM32WL з вбудованим трансивером LoRa дозволяє знизити собівартість модулів системи.

Таким чином, запропонована охоронна система на основі технології LoRa має вагомі технічні, функціональні та вартісні переваги перед конкуруючими системами.

Розділ 5. Стартап проект

5.1. Опис стартап ідеї бездротової системи безпеки

Таблиця 5.1 – Ідея стартап-проекту бездротової системи безпеки

Зміст ідеї стартапу	Можливості застосування	Вигоди для користувача системи безпеки
Використання технології LoRa для системи безпеки	1.Системи безпеки	велика дальність дії, тривалий час автономної роботи пристроїв.
	2.Автоматизована система розумного будинку	проста у встановленні та експлуатації

Таблиця 5.2 – Характеристики ідеї бездротової системи безпеки

		(потенційні)					
№ п/п	Техніко-економічні характеристики ідеї	Конкуруючі системи			недолік	Схожі характеристики	перевага
		Запропонована система	Ajax Systems	Visonic			
	Протокол обміну даними	Дає змогу	Не дає змогу	Не дає змогу			
2	Тривалий час автономної роботи	Дає змогу	Не дає змогу	Не дає змогу			+
3	Завадостійкість	Дає змогу	Дає змогу	Не дає змогу		+	

5.2. Аналіз технологічної складової проекту

У таблиці 5.3 надано оцінку технологічних можливостей реалізації бездротової системи безпеки та наведено пропоновані технології.

Таблиця 5.3 - Технологічна оцінка стартап-проекту

№ п/п	Стартап	Технології її реалізації	Наявність технологій	Доступність технологій
1	Бездротова система безпеки	Протокол LoRa	Наявний	Доступна
2		Датчики	Наявний прототип	Доступна
3		Програмне забезпечення для віддаленої взаємодії з системою	Необхідно розробити	Доступна

Обрана технологія реалізації бездротової системи безпеки: радіочастотна технологія LoRa.

5.3. Ринковий аудит можливостей стартап-проекту

У таблиці 5.4 надано наближену характеристику потенційного ринку стартап-проекту.

Таблиця 5.4. - Попередня характеристика потенційного ринку бездротової системи безпеки з технологією LoRa

№ п/п	Найменування показника	Значення
1	Кількість основних конкурентів	9
2	Загальний обсяг продаж, грн/ум.од	30000000
3	Вектор зміни ринку	Зростає
4	Потенційні перепони виходу на ринок	Донести інформацію про велику відстань дії та високу енергоефективність
5	Специфічні вимоги до стандартизації та сертифікації	Є
6	Середня норма рентабельності в галузі (або по ринку), %	61%

У таблиці 5.5 наведено опис характеристик потенційних клієнтів бездротової системи безпеки.

Таблиця 5.5. - Характеристика потенційних користувачів бездротової системи безпеки

№ п/п	Ринкова потреба	Користувачі	Вимоги користувачів до бездротової системи безпеки
1	Забезпечити підвищений рівень безпеки	Мешканці будинків/квартир, власники або адміністратори офісів/підприємств	Зрозумілий інтерфейс, велика відстань дії, енергоефективність та спрощений монтаж обладнання

2	Забезпечення функціоналу Розумного будинку	Користувачі, які налаштовують Розумний будинок	

У табл. 5.6 наведено фактори загроз реалізації стартап-проекту.

Таблиця 5.6. - Загрози реалізації бездротової системи безпеки

№ п/п	Загрози	Причина загроз	Спосіб реагування
1	Незацікавленість клієнтів	Внаслідок невдалого маркетингу клієнт може не зацікавитись послугами	Демонстрація можливостей створеного продукту
2	Втрата конкурентоспроможності	Втрата рангу надійного постачальника	Грамотна цінова політика

У табл.5.7 показано фактори можливостей при реалізації стартап-проекту.

Таблиця 5.7. - Можливості для реалізації бездротової системи безпеки

№ п/п	Тип можливості	Зміст можливості	Спосіб реалізації

1	Перехід до домінування на ринку охоронного обладнання	Зростання попиту	Якісне та кількісне нарощування потужностей
2	Перехід до домінування на ринку обладнання для Розумного будинку	Зростання попиту внаслідок зростання клієнтів	Якісне та кількісне нарощування потужностей

Особливості конкурентних бездротових систем безпеки та їх вплив на реалізацію проекту визначено в таблиці 5.8.

Таблиця 5.8. - Аналіз конкурентного середовища

Особливості конкуренції	Як проявляється	Що вимагає від компанії
Конкуренція технологій	Використання подібних технологій	Високий рівень стандартизації
Конкуренція постачальників	Відсутність єдиного постачальника обладнання	Індивідуальний підхід до клієнтів. Сервісна підтримка
Міжгалузева конкуренція	немає	немає
Товарна конкуренція	Використання стандартних технологій	використання доступного ПО та апаратного забезпечення

конкуренція цін	Робота з компаніями, які пропонують значно нижчу ціну	Зниження собівартості компонентів системи
Брендова конкуренція	Для кожного типу забезпечення потрібна команда розробників	Отримання переваги на ринку охоронних систем

У табл. 5.9 показано фактори конкурентоспроможності запропонованої системи безпеки та їх обґрунтування.

Таблиця 5.9. - Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування вибору такого фактору
1	Продумані ціни	Зниження собівартості апаратних компонентів системи
2	Надання сервісних послуг	При бажанні клієнта, можлива технічна підтримка

У табл. 5.10 наведено сильні та слабкі сторони запропонованої бездротової системи безпеки.

Таблиця 5.10. - Порівняльний аналіз переваг та недоліків запропонованої бездротової системи безпеки

№ п / п	Конкурентні показники	Бали 1-20	Рейтинг конкуруючих систем у порівнянні						
			–3	–2	–1	0	+1	+2	+3
1	Обґрунтовані цінові показники	18	+						
2	Надання сервісних послуг	14		+					
3	Необхідність самостійної роботи клієнта	6				+			

У табл.5.11 наведено SWOT-аналіз стартап-проекту.

Таблиця 5.11. - SWOT- аналіз стартап-проекту бездротової системи безпеки

Сильні сторони: знижені цінові показники, покращення технічних характеристик, сервіс	Слабкі сторони: частину робіт клієнт має виконувати самостійно
Можливості: створення свого сегменту ринку	Загрози: Продукт не цікавий клієнту

Інші варіанти випуску на ринок бездротової системи безпеки наведені у табл.5.12.

Таблиця 5.12. - Альтернативи впровадження бездротової системи безпеки на ринку

№ п/п	Альтернативні варіанти впровадження	Можливість залучення ресурсів	Терміни реалізації
1	Укладення договорів з охоронними компаніями та поширення нової системи на ринку	висока	незначні
2	Реалізація через торгові мережі	середня	незначні

Обрана альтернатива - укладення договорів з охоронними компаніями та швидке захоплення сегменту ринку при використанні нового рішення.

5.4. Ринкова стратегія просування проекту

Обґрунтування вибору цільових груп потенційних споживачів наведено у табл. 5.13.

Таблиця 5.13. - Цільові групи потенційних споживачів

№ п/п	Опис потенційних споживачів	Готовність до використання продукту	Очікуваний попит в цільовій групі	Конкуренція в групі	Простота запуску продукту
1	Охоронні компанії	Середня	Високий	Середня	Висока

2	Торгівельні мережі	Висока	Високий	Середня	Низька

У табл. 5.14 наведено базову стратегію розвитку бездротової системи безпеки.

Таблиця 5.14. - Визначення базової стратегії розвитку

№ п/п	Інші варіанти розвитку системи	Стратегія виходу на ринок	Основні позиції, які складають конкуренцію до обраної альтернативи	Основна стратегія розвитку системи
1	Використання окремо мікроконт-роллера та трансивера	Пропозиція кращого співвідно-шення ціна/якість	Зацікавлення та залучення найбільш популярних охоронних компаній	Стратегія диференціації
2	Здешевлення проекту	Здешевлення процесу виробництва	Застосування економічних апаратних рішень	Стратегія мінімальних витратах

У табл.5.15 наведено визначення основної стратегії конкурентної поведінки.

Таблиця 5.15. - Основна стратегія конкурентної поведінки

№ п/п	Чи є проект принципово новим на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1	Ні	Забирати існуючих та шукати нових	Буде. Фіксація тривог від різних охоронних датчиків і сповіщення користувачів	Стратегія конкуренції з лідером

У табл. 5.16 наведено основні критерії позиціонування бездротової системи безпеки на ринку.

Таблиця 5.16. - Критерії стратегії позиціонування

№ п/п	Вимоги цільової аудиторії до товару	Основна стратегія розвитку	Ключові позиції системи безпеки які забезпечують конкуренцію	Основні критерії привабливості (три ключових)
1	Кращі споживацькі характеристики	Стратегія диференціації	Новизна, гарант якості, точність дослідження	Якість, надійність, функціональність

2	Мінімальні витрати	Стратегія лідерства по витратах	Ціна	Дешевизна

5.5. Маркетингова програма просування проекту

Ключові переваги запропонованої бездротової системи безпеки наведено у табл. 5.17.

Таблиця 5.17. - Визначення ключових переваг бездротової системи безпеки

№ п/п	Перевага	Вигода, яку пропонує товар	Основні переваги перед конкурентами
1	Завадостійкість	Кращий функціонал	Кращі технічні характеристики
2	Нижча ціна	Економія коштів, більша функціональність	Нижча ціна

Визначення меж встановлення ціни на послугу наведено у табл. 5.18.

Таблиця 5.18. - Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар

1	1500 у.о./од.	800 у. о./од	Середній	Н.400 у.о. – В.600 у.о.

Формування системи збуту запропонованої бездротової системи безпеки наведено у табл. 5.19.

Таблиця 5.19. - Формування збуту бездротової системи безпеки

№ п/п	Поведінка цільових клієнтів	Вимоги до постачальника системи	Можливості каналу збуту	Найкраща система збуту
1	Максимальна простота підключення	Поставки якісного та надійного обладнання	Значні	Договірна система збуту

Концепції маркетингових комунікацій наведено у табл. 5.20.

Таблиця 5.20. - Концепція маркетингових комунікацій

№ п/п	Особливості поведінки цільових клієнтів	Канали отримання інформації, цільовими клієнтами	Ключові позиції для просування	Мета рекламного повідомлення	Зміст рекламного звернення
1	Зацікавленість в якісному та простому для використання продукті	Інтернет, соціальні мережі, пошта, телебачення	Гарантованість якості, стандартизація, ціна	Зацікавити у підвищенні рівня безпеки	Представлення легкості підключення і можливостей системи безпеки

Висновки до розділу 5

У даному розділі запропоновано стартап-проект створення бездротової системи безпеки, яку можна використовувати в офісах та житлових будинках.

Досліджено доцільність та виконано аналіз рентабельності випуску бездротової системи безпеки на основі радіочастотної технології LoRa. Показано, що переваги, які надає вибрана технологія, надають можливість створити комерційний проект з кращими користувацькими та ціновими характеристиками.

ВИСНОВКИ

Для передачі невеликих обсягів даних і забезпечення терміну живлення від батареї у декілька років у системах безпеки найкраще підходять технології LPWAN.

Висока енергоефективність, що забезпечується технологією Sigfox і LoRa. Окрім того, завдяки високій чутливості LoRa забезпечує високу завадостійкість зв'язку на великих відстанях у порівнянні з системами іншими системами.

Для передачі великих обсягів даних у системах безпеки, у першу чергу відеоданих, гарну перспективу мають LoRa 2.4 ГГц і технології 5G.

Незважаючи на те, що проводові системи безпеки мають перевагу в швидкості передачі даних в надійності каналу зв'язку, на даний момент радіочастотні технології їх витісняють за рахунок відмови від необхідності прокладення кабелів.

Перехід систем безпеки на бездротовий зв’язок робить необхідними використання енергоефективних протоколів взаємодії елементів системи, котрі будуть сприяти низькому споживанню енергії, так як вони працюють виключно від батареї.

Бездротові системи безпеки поділяються на дві категорії: ті, які використовують загальнодоступні протоколи (наприклад Wi-Fi, Z-Wave, Bluetooth) або свої внутрішні протоколи (наприклад Power G або Jeweller).

Найбільш перспективними є змішані системи, котрі мають підтримку і загальнодоступних протоколів, і внутрішніх протоколів. Саме завдяки цьому користувач може досить гнучко налаштувати свою систему підключивши охоронні датчики використовуючи внутрішні протоколи, а датчики для автоматизації підключити використовуючи загальнодоступні протоколи.

Враховуючи те, що технологія LoRa забезпечує велику дальність дії, високу чутливість, можливість приймати сигнали, рівень яких може бути менше рівня завад до 20 dB та високу енергоефективність бездротові системи безпеки, побудовані на цій технології, можуть скласти конкуренцію існуючим системам за рахунок можливості розташування елементів системи на великих відстанях, підвищеної завадостійкості, довго тривалість автономної роботи пристроїв.

Використання мікроконтролера STM32WL з вбудованою трансивером LoRa дає можливість функціонування системи у широкому діапазоні робочих частот від 150 до 960 МГц, що забезпечує підтримку всіх основних субгігагерцових промислових, наукових та медичних (ISM) діапазонів у всьому світі, а також знизити собівартість модулів системи. Кількість точок такої системи теоретично не обмежена. Максимальна відстань передачі даних у зоні прямої видимості - більше 15 км. Термін роботи точки від однієї батареї – більше 10 років. Чутливість приймача: –148 дБм. Перевищення рівня шуму над рівнем сигналу – до 16 дБ. Швидкість передачі даних до 250 кБіт/с.

Таким чином, запропонована охоронна система на основі технології LoRa має вагомі технічні, функціональні та вартісні переваги перед конкуруючими системами, а сам проект є комерційно вигідним.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Harnessing the Internet of Things for Global Development - ITU, веб-сайт. URL: https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf (дата звернення 19.11.2021).

2. LoRa and LoRaWAN: A Technical Overview, Semtech Corporation URL: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/ (дата звернення 19.11.2021).

3. Alexander S. Gillis “What is 5G?”, TechTarget веб-сайт. URL: https://www.techtarget.com/searchnetworking/definition/5G (дата звернення 14.11.2021 р.)

4. IMT Vision – Framework and overall objectives of the future, itu.int: веб-сайт. URL: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf (дата звернення 19.11.2021).

5. Hoffman, Chris "What Is 5G, and How Fast Will It Be?" How-to Geek веб-сайт. URL: https://www.howtogeek.com/340002/what-is-5g-and-how-fast-will-it-be/ (дата звернення 14.11.2021 р.)

6. 5G best choice architecture. White Paper – ZTE веб-сайт. URL: https://res-www.zte.com.cn/mediares/zte/Files/PDF/white_book/5g-best-choice-architecture.pdf (дата звернення 14.11.2021 р.)

7. Installer Guide INTEGRA 64, Satel Ltd. (2019) веб-сайт. URL: https://www.satel.eu/en/installer/man#en (дата звернення: 29.09.2021).

8. Axiom Security Control Panel Installation Guide, hikvision.com. URL: https://www.hikvision.com/content/dam/hikvision/products/S000000001/S000000601/S000000937/S000000938/OFR001809/M000010570/Installation_Guide/DS-PWA32_Axiom-Security-Control-Panel_Installation-Guide_20190126.PDF (дата звернення: 05.11.2021).

9. DSC from Tyco Security Products (2018): “Products catalog”: веб-сайт. URL: https://www.dsc.com/index.php?o=about_tyco (дата звернення: 29.09.2021).

10. D-303222 PowerMaster-10/30 G2 Installer's Guide, visonic.com. веб-сайт. URL: http://www.visonic.com/data/uploads/powermaster_10_30_installer_guide_english_d-303222.pdf (дата звернення: 29.09.2021).

11. Ajax Systems (2021), Starter Kit: веб-сайт. URL: https://ajax.systems/ua/products/starterkit/. (дата звернення: 27.09.2021).

12. ООО «Шериф». Види охоронних датчиків і як вони працюють: веб-сайт. URL: https://sheriff.com.ua/uk/7135/ . (дата звернення: 13.10.2021).

13. Ajax Systems (2021), “Захист на відстані дотику”: веб-сайт. URL: https://ajax.systems/ua/how-it-works/. (дата звернення: 08.11.2021).

14. Ajax Systems (2021), “Технології та можливості радіопротоколу Jeweller”: веб-сайт. URL: https://support.ajax.systems/uk/jeweller-radio-protocol/. (дата звернення: 29.10.2021).

15. Ajax Systems (2021), “Ajax HUB user guide”: веб-сайт. URL: https://ajax.systems/ua/products/hub/ (дата звернення: 19.10.2021).

16. S. Kartakis, B. D. Choudhary, A. D. Gluhak, L. Lambrinos, and J. A. McCann, “Demystifying low-power wide-area communications for city iot applications,” in Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization. ACM, 2016, pp. 2–8.

17. Cattani M, Boano CA, Römer K. An Experimental Evaluation of the Reliability of LoRa Long-Range Low-Power Wireless Communication. Journal of Sensor and Actuator Networks. 2017; 6(2):7. https://doi.org/10.3390/jsan6020007

18. Long-range wireless STM32WL microcontrollers. Overview.: веб-сайт. URL: https://www.st.com/en/microcontrollers-microprocessors/stm32wl-series.html#overview (дата звернення: 09.09.2021).

19. Semtech SX1280. Long range, low power 2.4 GHz Wireless RF Transceiver with ranging capability: веб-сайт. URL: https://www.semtech.com/products/wireless-rf/lora-24ghz/sx1280 (дата звернення: 21.10.2021).

20. Janssen T., BniLam N., Aernouts M., Berkvens R., Weyn M. LoRa 2.4 GHz Communication Link and Range. *Sensors* 2020, 20, 4366. https://doi.org/10.3390/s20164366

21. F. Rander Andersen, K. Dilip Ballal, M. Nordal Petersen and S. Ruepp, "Ranging Capabilities of LoRa 2.4 GHz," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2020, pp. 1-5, doi: 10.1109/WF-IoT48130.2020.9221049.

22. Wei, Ching-Chuan & Su, Pei-Yi & Chen, Shu-Ting. (2020). Comparison of the LoRa Image Transmission Efficiency Based on Different Encoding Methods. International Journal of Information and Electronics Engineering. 10. pp.1-4. 10.18178/IJIEE.2020.10.1.712 .

23. T. Chen, D. Eager and D. Makaroff, "Efficient Image Transmission Using LoRa Technology In Agricultural Monitoring IoT Systems," 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2019, pp. 937-944, doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00166.

24. Jebril AH, Sali A, Ismail A, Rasid MFA. Overcoming Limitations of LoRa Physical Layer in Image Transmission. Sensors. 2018; 18(10):3257. https://doi.org/10.3390/s18103257

25. Semtech SX1278. LoRa Core™ 137MHz to 525MHz Long Range Low Power Transceiver: веб-сайт. URL: https://www.semtech.com/products/wireless-rf/lora-core/sx1278 (дата звернення: 05.11.2021).

26. The Things Network: веб-сайт. URL: https://www.thethingsnetwork.org/ (дата звернення: 05.11.2021).

ДОДАТОК А

SUMMARY

Wireless security systems have a number of significant advantages, as the no need of wires greatly simplifies installation and allows users to place devices in any convenient location, and criminals will not be able to deactivate such surveillance cameras or sensors by cutting their cables. Due to these advantages, wireless security systems are getting more popular than for traditional security systems.

Wireless security systems use state-of-the-art data transmission and energy-saving technologies. Most components of the security system, such as security sensors, run on batteries. Terminal devices use radio frequency technology to communicate with the gates. The gate has access to the Internet.

However, industrial electromagnetic interference and buildings with their elements significantly reduce the maximum distance of wireless security systems and the operation of its individual elements. In such cases, the system may issue false alarms and send inaccurate information to the user. Therefore, it is necessary to increase the noise immunity of wireless security systems and increase the maximum distance of their components.

The above shortcomings can be corrected by a new system with advanced functionality, low cost and the ability to work over long distances in conditions of significant electromagnetic interference.

The aim of the work is to create a concept of wireless security system with advanced functionality, namely using a radio frequency communication channel based on LoRa technology.

The first section discusses radio frequency data transmission technologies for the Internet of Things. The basis for data transmission in wireless security systems are radio frequency technologies, which must provide a sufficiently long distance of data transmission and consume a small amount of energy.

LPWAN technology is best for transferring small amounts of data and ensuring battery life in a few years.

The high energy efficiency provided by Sigfox technology also depends on Sigfox semiconductor partners, as their chips consume from 10 mA to 50 mA in transmission - depending on the partner and the chip used.

Due to its high sensitivity (-148dbm) and high energy efficiency, LoRa is ideal for devices with low power consumption and high reliability over long distances. In addition, due to its high sensitivity, LoRa provides high noise immunity over long distances compared to other systems.

The most important thing in NB-IoT is the ability to work at lower signal levels and at high noise levels, as well as save battery.

5G technologies have good prospects in security systems. The disadvantages of such technologies are that the technology has a cellular network architecture, in which the coverage area is divided into small zones - cells. Data may be lost when moving between cells, or reconnecting from one base station to another takes some time when the sensor should have sent its data.

LoRa 2.4 GHz and 5G technologies have good prospects for the transmission of large amounts of data in security systems, primarily video data.

The second section discusses the principles of construction and components of security systems. Security systems, including security systems, are globally divided into two categories according to the method of data exchange between devices and control panel, namely: wired and wireless.

Wired systems had an advantage in data rate in the reliability of the communication channel. However, at the moment, radio technology is not inferior to the wired connection and more and more systems are beginning to use different technologies. Despite the advantages of wired security systems, wireless security systems are displacing them by eliminating the need for cabling.

The transition of security systems to wireless communication requires the use of energy-efficient protocols for the interaction of system elements, which will contribute to low energy consumption, as they run solely on battery power.

As systems switch to wireless communication between the device and the control panel, it is necessary to use energy-efficient devices and protocols that will promote low energy consumption, as they run exclusively on battery as opposed to connecting to the bus (through which the device is powered). Therefore, wireless security systems must be built based on these parameters.

The third section performs a comparative analysis of wireless security systems. According to the protocols used, wireless security systems can be divided into two categories: those that use public protocols (such as Wi-Fi, Z-Wave, Bluetooth) or their own internal protocols (such as Power G or Jeweler).

However, the most popular are mixed systems, which support both public protocols and internal protocols. This allows the user to flexibly configure their system by connecting security sensors using internal protocols, and to connect sensors for automation using public protocols.

The results of the comparison of Jeweler, LoRa, Power G radio protocols show that LoRa technology has a number of significant advantages. Namely:

- long range
- high sensitivity
- the ability to receive signals whose level may be less than the interference levels up to 20 dB
- high energy efficiency

Thus, a wireless security system based on LoRa technology can compete with existing systems due to the ability to locate system elements over long distances, increased noise immunity, long battery life.

The fourth section describes the proposed wireless security system based on the LoRa protocol. LoRa technology has a number of significant advantages over other data transmission technologies and has very good prospects for use in

wireless security systems. The STM32WL microcontroller with built-in LoRa data transmission technology makes it possible to obtain the following endpoint characteristics:

Ability to use in a wide operating frequency range from 150 to 960 MHz, providing support for all major sub-GHz industrial, scientific and medical (ISM) bands worldwide.

The number of points is theoretically not limited. In practice - more than 1000

The maximum data transmission distance in the line of sight is more than 15 km

The service life of a point from one battery is more than 10 years

Receiver sensitivity: –148 dBm

Exceeding the noise level above the signal level - up to 16 dB

The LoRa SX1280 transceiver with an operating frequency of 2.4 GHz provides data transfer speeds of up to 250 kbps.

The presence of STM32WL microcontroller with built-in LoRa transceiver allows you to reduce the cost of system modules. The use of the STM32WL microcontroller with built-in LoRa transceiver allows the system to operate in a wide operating frequency range from 150 to 960 MHz, supporting all major sub-GHz industrial, scientific and medical (ISM) bands worldwide and reducing system modules. The number of points of such a system is theoretically not limited. The maximum data transmission distance in the line of sight is more than 15 km. The service life of a point from one battery is more than 10 years. Receiver sensitivity: –148 dBm. Exceeding the noise level above the signal level - up to 16 dB. Data transfer rate up to 250 kBps.

The fifth section proposes a startup project based on the creation of a wireless security system that will be used in offices and residential buildings. A study of the feasibility and profitability of this business project and determined that the commercialization of the project is appropriate.

LPWAN technologies are best suited for security in transferring small amounts of data and ensuring a battery life of several years in security systems. Due to the fact that LoRa technology provides long range, high sensitivity, the ability to receive signals that can be less than the noise level up to 20 dB and high energy efficiency, wireless security systems based on this technology can compete with existing systems due to the location of elements long-distance systems, high noise immunity, long battery life.

Thus, the proposed security system based on LoRa technology has significant technical, functional and cost advantages over competing systems, and the project itself is commercially viable.