

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)

Кафедра автоматики та телекомунікацій
(повна назва кафедри)

«До захисту допущено»

В.о.завідувача кафедри автоматики та
телекомунікацій

(підпис) Поцєпєв В.В.
(ім'я та прізвище)

«___» _____ 2023 р.

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Дослідження використання технологій безпроводових сенсорних
мереж у зонах підвищеної небезпеки»

Виконав студент 3 курсу, групи ТКРп-20
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

Амерханян Варган Анатолійович
(Прізвище, Ім'я та По-батькові) (підпис)

Керівник асист. каф. АТ Дар'я ЖУКОВСЬКА
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Рецензент к.т.н., доц., доц. каф. ЕТ Олександр ШТЕПА
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Нормоконтроль:

Дар'я ЖУКОВСЬКА

23.06.2023 р.

*Засвідчую, що у цій випускній кваліфікаційній
роботі немає запозичень з праць інших авторів
без відповідних посилань.*

Студент _____
(підпис)

Луцьк – 2023 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)

Кафедра автоматики та телекомунікацій
(повна назва кафедри)

Захист відбувся _____
(дата)

з оцінкою _____

Секретар ЕК _____
(підпис)

Випускна кваліфікаційна робота
бакалавра

тема «Дослідження використання технологій безпроводових сенсорних мереж у
зонах підвищеної небезпеки»

Виконавець, студент

гр. ТКРП-20

Вартан АМЕРХАНЯН

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Керівник

Дар'я ЖУКОВСЬКА

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Консультанти:

Гліб СТУПАК

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Ганна ТЕЛИЧКО

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Валерій ПОЦЕПАЄВ

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Нормоконтроль

Дар'я ЖУКОВСЬКА

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Луцьк – 2023 р.

**Державний вищий навчальний заклад
"Донецький національний технічний університет"**

Інститут, факультет Комп'ютерно-інформаційних технологій та автоматизації
Кафедра Автоматика та телекомунікації
Освітньо-кваліфікаційний рівень бакалавр
Галузі знань 17 Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

**В.о. завідувача кафедри АТ
Валерій ПОЦЕПАЄВ**

«_____» _____ 2023 року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Амерханяну Вартану Анатолійовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) «Дослідження використання технологій безпроводових сенсорних мереж у зонах підвищеної небезпеки»

керівник проекту (роботи) Жуковська Дар'я
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від 05.05.2023 року № 175

2. Строк подання студентом проекту (роботи) _____

3. Вихідні дані до проекту (роботи)

Технічна документація та матеріали з переддипломної практики

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) технологічні аспекти сенсорних мереж; 2) способи використання засобів телекомунікаційної інфраструктури в зонах підвищеної небезпеки; 3) побудова структурної схеми; 4) вибір комунікаційного обладнання, побудова функціональної схеми.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

1) структурна схема мережі; 2) функціональної схема; 3) технічні характеристики обладнання;

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Поцєпаєв В.В., в.о.зав.каф.АТ		
2	Теличко Г.О., доц. каф. АТ		
3	Ступак Г.В., ст. викл каф. АТ		
нормоконтроль	Жуковська Д.О.	-	23.06.2023р.

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Дослідження безпроводових сенсорних мереж.	05.05.2023	
2	Характеристика зон підвищеної небезпеки.	08.05.2023	
3	Опис технологій та стандартів для проектування мережі.	13.05.2023	
4	Аналіз проблем при проектуванні безпроводових сенсорних мереж.	20.05.2023	
5	Аналіз технологій сенсорних мереж.	28.05.2023	
6	Вибір технології безпроводової сенсорної мережі у зонах підвищеної небезпеки.	03.06.2023	
7	Розробка структурної схеми проектованої безпроводової сенсорної мережі.	06.06.2023	
8	Вибір обладнання та розробка функціональної схеми.	10.06.2023	
9	Оформлення роботи.	14.06.2023	

Студент

(підпис)

Вартан АМЕРХАНЯН

(прізвище та ініціали)

Керівник роботи

(підпис)

Дар'я ЖУКОВСЬКА

(прізвище та ініціали)

ЛИСТ ЗАУВАЖЕНЬ

Посада, Ім'я та ПРІЗВИЩЕ	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Амерхян Вартан Анатолійович. Дослідження використання технологій безпроводових сенсорних мереж у зонах підвищеної небезпеки / Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» зі спеціальності 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Луцьк, 2023.

Пояснювальна записка: 58 стор., 17 рис., 9 табл., 11 посилань.

У випускній кваліфікаційній роботі дослідженні основних технологій безпроводових сенсорних мереж, проведенні аналізу їх використання в зонах надзвичайних ситуацій та внесенні пропозицій щодо реалізації безпроводових сенсорних мереж у таких зонах.

В даній роботі описується і аналізується вибір безпроводових технологій, які мають значні переваги і можуть бути використані у сенсорних мережах в зонах надзвичайних ситуацій. Також досліджуються та надаються пропозиції щодо технічної реалізації безпроводових сенсорних мереж.

Ключові слова: БЕЗПРОВОДОВА ТЕХНОЛОГІЯ, МЕРЕЖА, НАДЗВИЧАЙНА СИТУАЦІЯ, ДАТЧИК, ДБЖ, СЕНСОР, ТОПОЛОГІЯ, СТРУКТУРА, ПРОТОКОЛ.

ЗМІСТ

ВСТУП.....	7
1 АКТУАЛЬНІСТЬ ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ.....	10
1.1 Області досліджень у бездротових сенсорних мережах.....	10
1.1.1 Поняття «сенсорна мережа».....	10
1.1.2 Технологічні аспекти сенсорних мереж.....	11
1.2 Характеристика зон підвищеної небезпеки.....	14
1.2.1 Характеристика зон підвищеної небезпеки під час військових дій	15
1.3 Способи використання засобів телекомунікаційної інфраструктури в зонах підвищеної небезпеки.....	17
1.4 Актуальність використання телекомунікаційних вузлів для створення безпроводових сенсорних мереж в зоні надзвичайної ситуації.....	18
1.5 Проблеми при проектуванні безпроводових сенсорних мереж.....	20
Висновки до розділу 1.....	21
2 ХАРАКТЕРИСТИКА ТЕХНОЛОГІЙ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ У ЗОНАХ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ.....	23
2.1 Аналіз технологій сенсорних мереж.....	23
2.1.1 Різні види безпроводових мереж.....	23
2.1.2 Стандарт IEEE 802.11.....	25
2.1.3 Стандарт Bluetooth.....	30
2.1.4 Стандарт ZigBee.....	35
2.2 Вибір технології безпроводової сенсорної мережі у зонах підвищеної небезпеки.....	36
Висновки до розділу 2.....	38
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ У ЗОНАХ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ.....	40

3.1 Вибір топології для проектованої безпроводової сенсорної мережі	40
3.2 Структурна схема проектованої безпроводової сенсорної мережі.....	47
3.3 Вибір обладнання для проектованої безпроводової сенсорної мережі	48
3.4 Функціональна схема проектованої безпроводової сенсорної мережі	51
Висновки до розділу 3.....	53
ВИСНОВКИ.....	54
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	57

ВСТУП

Актуальність теми. Сучасне життя характеризується значним прогресом у технологічному розвитку в усіх сферах людської діяльності. Промисловий прогрес у галузях, таких як хімія, енергетика, металургія, військова справа тощо, забезпечує нам багато переваг і поліпшує якість життя. Але разом з цим, такий прогрес також несе в собі ризики, особливо в разі непередбачуваних обставин. Надзвичайні природні події, військові конфлікти та терористичні акти можуть викликати різного роду надзвичайні ситуації.

Зона підвищеної небезпеки – це територія або район, де існує підвищений ризик виникнення небезпеки або відбуваються певні небезпечні події. Ця зона може бути пов'язана з різними видами небезпек, такими як природні катастрофи (наприклад, землетруси, повені, лавини), техногенні аварії (наприклад, вибухи, руйнування, протікання небезпечних речовин) або зони конфліктів та воєнних дій.

Телекомунікації грають важливу роль у зонах підвищеної небезпеки, де швидкий обмін інформацією та зв'язок можуть бути життєво важливими. Ось кілька способів, якими телекомунікації використовуються у таких зонах:

Мобільний зв'язок: Мобільні телефони та мережі забезпечують зв'язок між людьми, що дозволяє швидко сповіщати про небезпеку, викликати допомогу та обмінюватись інформацією. У разі кризової ситуації мережі мобільного зв'язку можуть бути підсилені або встановлені тимчасові базові станції для забезпечення стабільного зв'язку.

Радіо та телебачення: Радіо та телевізійні мовлення можуть використовуватись для розповсюдження важливої інформації щодо небезпеки, евакуації, безпечних місць та інструкцій громадськості. Розповсюдження масової інформації може здійснюватись через трансляцію ефіром або за допомогою спеціальних систем виклику уваги на радіо та телевізорах.

Системи аварійного сповіщення: В деяких зонах підвищеної небезпеки встановлюються спеціальні системи аварійного сповіщення, такі як сирени,

гучномовці або системи масової розсилки повідомлень (наприклад, через SMS або мобільні додатки). Ці системи дозволяють оперативно сповістити населення про загрозу і надати конкретні інструкції щодо дій.

Супутникова зв'язок: Супутникові комунікаційні системи можуть бути особливо корисними у віддалених або важкодоступних зонах підвищеної небезпеки, де можуть бути пошкоджені традиційні інфраструктури зв'язку. Вони дозволяють забезпечувати зв'язок та передавати дані через супутникові сигнали.

Ці телекомунікаційні засоби допомагають владам та організаціям забезпечувати ефективний зв'язок, координацію дій, швидку передачу інформації та реагування на небезпеку в зонах підвищеної небезпеки. Вони допомагають покращити безпеку громадськості та забезпечити ефективну допомогу в надзвичайних ситуаціях.

Одним із засобів телекомунікаційної інфраструктури, що може активно використовуватись у зонах підвищеної безпеки є сенсорні мережі, що мають значний потенціал. Ці мережі базуються на розпізнаванні образів із використанням сенсорів, таких як камери, мікрофони, термальні сенсори та інші.

Однією з основних переваг сенсорних мереж є їх здатність спостерігати та аналізувати навколишнє середовище в реальному часі. У зонах підвищеної небезпеки, таких як промислові майданчики, пожежонебезпечні зони, райони з радіаційними загрозами або небезпечні зони через воєнні дії, сенсорні мережі можуть виявляти та реагувати на потенційні загрози швидше, ніж людський персонал.

Узагалі, сенсорні мережі можуть допомагати знижувати ризики та покращувати безпеку в зонах підвищеної небезпеки шляхом швидкого виявлення потенційних загроз, реагування на них та сповіщення відповідних служб. Вони можуть працювати в поєднанні з іншими системами безпеки та автоматичного управління, щоб забезпечувати надійний та ефективний моніторинг у небезпечних умовах.

Метою дипломного проекту є дослідження використання технологій безпроводових сенсорних мереж у зонах підвищеної небезпеки.

Щоб виконати роботу необхідно виконати **наступні задачі**:

- проаналізувати види сенсорних мереж;
- дослідити використання телекомунікаційної інфраструктури для створення безпроводових сенсорних мереж у зонах з підвищеною небезпекою;
- визначити особливості використання технологій безпроводових сенсорних мереж;
- запропонувати розробку реалізації безпроводових сенсорних мереж зонах з підвищеною небезпекою.

Об'єкт дослідження сенсорна мережа.

Предметом дослідження телекомунікаційна інфраструктура для реалізації технологій безпроводових сенсорних мереж у зонах з підвищеною небезпекою.

Структура та обсяг роботи. Випускна кваліфікаційна робота обсягом 58 машинописних сторінок, складається з вступу, трьох розділів, висновків, переліка використаних джерел, що складається з 11 найменувань. Робота містить 17 рисунків, 9 таблиць.

1 АКТУАЛЬНІСТЬ ПРОВЕДЕННЯ ДОСЛІДЖЕНЬ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

1.1 Области досліджень у бездротових сенсорних мережах

1.1.1 Поняття «сенсорна мережа»

Бездротові сенсорні мережі (WSN) привернули увагу дослідницьких спільнот протягом останніх кількох років через безліч теоретичних і практичних проблем. Цей зростаючий інтерес можна значною мірою пояснити розповсюдженням технології мікроелектромеханічних систем (MEMS) [1] і нових додатків, створених за допомогою великомасштабних мереж невеликих пристроїв, здатних збирати інформацію з фізичного середовища, виконуючи просту обробку на видобуті дані та передача їх у віддалені місця. Значні результати в цій галузі за останні кілька років спричинили сплеск цивільних і військових застосувань, таких як система відстеження та моніторинг навколишнього середовища.

На сьогодні більшість розгорнутих бездротових сенсорних мереж вимірюють скалярні фізичні явища, такі як температура, тиск, вологість або розташування об'єктів. Загалом, більшість додатків мають низькі вимоги до пропускну здатності та, як правило, терпимі до затримок. Области досліджень у бездротових сенсорних мережах широкі, умовно дослідження в області використання сенсорних мереж можна розділити на 3 групи:

- Перша група – це системи, які складаються з сенсорних вузлів; сенсорні вузли можна назвати загальними вузлами або вузлами шлюзу. Загальні вузли беруть вимірювання з контрольованих середовищ, тоді як вузли шлюзу збирають дані від загальних вузлів і передають їх на базову станцію. Кожен сенсорний вузол є

індивідуальною системою. Щоб підтримувати різне прикладне програмне забезпечення на сенсорній системі, дослідникам необхідно розробити нові платформи, операційні системи та схеми зберігання.

- Друга група – протоколи зв'язку, які забезпечують зв'язок між додатком і датчиками. Вони також забезпечують зв'язок між сенсорними вузлами. Реалізація протоколів на різних рівнях у стеку протоколів може значно вплинути на енергоспоживання, наскрізну затримку та ефективність системи. Важливо оптимізувати спілкування і мінімізувати споживання енергії. Протоколи 2011 погано працюють у WSN, оскільки вони не розроблені для задоволення цих вимог. Отже, дослідники повинні шукати нові енергозберігаючі протоколи, хоча деякі з них були запропоновані для всіх рівнів стеку протоколів, щоб відповідати вимогам WSN.
- Остання група – це сервіси, які розроблені для покращення та вдосконалення програми продуктивності системи та ефективності мережі. Кожна з цієї групи ставить перед дослідниками унікальні завдання [1].

1.1.2 Технологічні аспекти сенсорних мереж

Безпроводові сенсорні мережі є складовою частиною Інтернету речей (IoT) і використовуються для збирання і передачі даних з фізичних об'єктів за допомогою бездротових з'єднань. Вони складаються з бездротових сенсорних вузлів, які можуть бути розташовані в різних місцях і збирають інформацію про навколишнє середовище, наприклад, температуру, вологість, освітленість або рух.

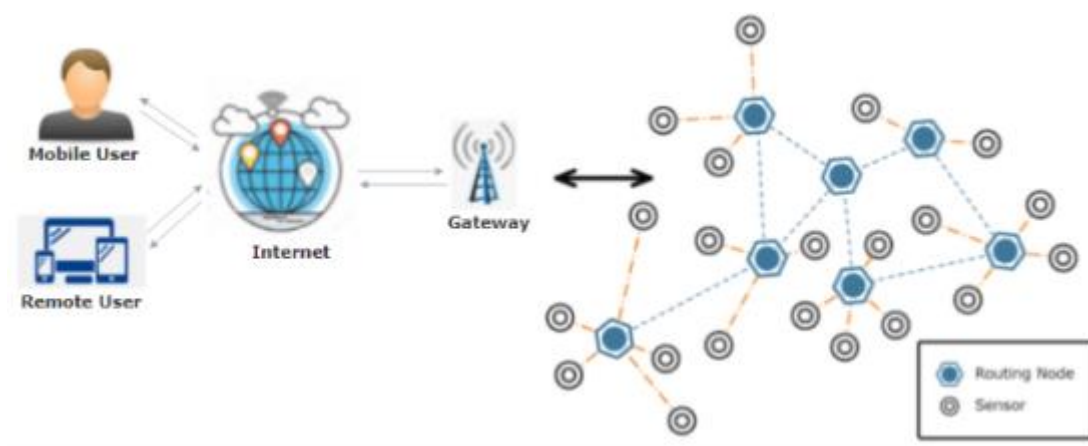


Рисунок 1.1 – Архітектура бездротової сенсорної мережі (WSN)

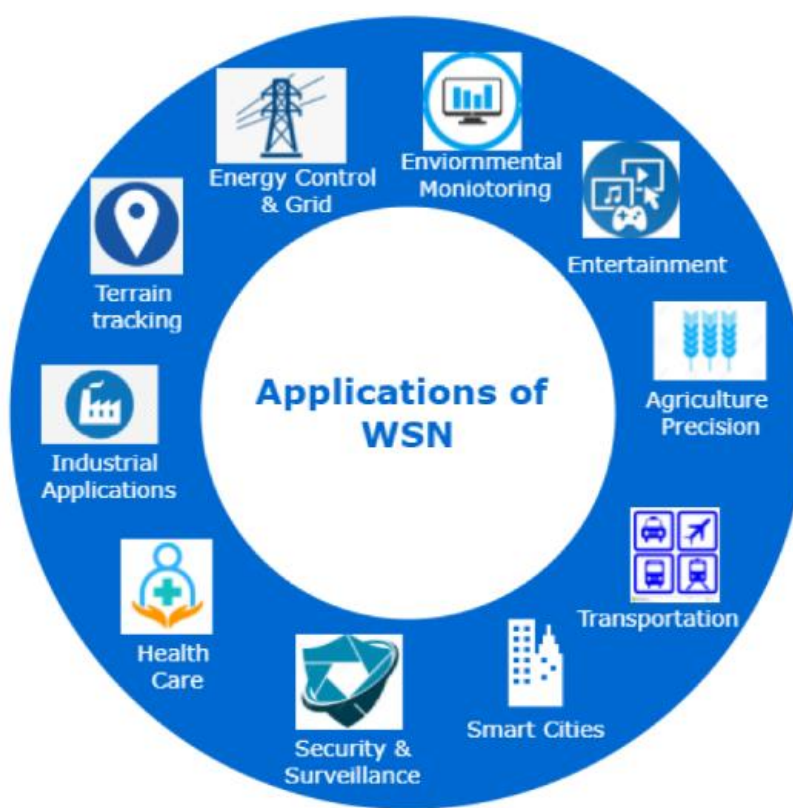


Рисунок 1.2 – Сфери застосування безпроводової сенсорної мережі (WSN) [5]

Основні технологічні риси безпроводових сенсорних мереж включають:

1. Бездротове з'єднання: Безпроводові сенсорні мережі використовують бездротові технології для передачі даних між сенсорними вузлами і базовою станцією або центральним вузлом. Такі технології включають Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN та

інші. Кожна з цих технологій має свої переваги та обмеження, що залежать від вимог до відстані передачі, енергоспоживання та пропускної здатності.

2. Енергоефективність: Оскільки багато сенсорних вузлів живляться від батарей або мають обмежені джерела живлення, енергоефективність є важливим аспектом безпроводових сенсорних мереж. Вони використовують різні стратегії для зменшення споживання енергії, такі як режими сну, призначені для збереження енергії у періодах неактивності, а також протоколи передачі даних, які мінімізують передачу зайвої інформації.

3. Масштабованість: Безпроводові сенсорні мережі можуть включати велику кількість сенсорних вузлів, розташованих на великій території. Вони повинні бути масштабовані, щоб дозволяти додавання нових вузлів або зменшення їх кількості залежно від потреби. Також важливо забезпечити ефективну маршрутизацію даних із сенсорних вузлів до базової станції.

4. Розподіленість: Безпроводові сенсорні мережі побудовані на принципі розподіленості, де кожен сенсорний вузол працює автономно та може спілкуватися безпосередньо з іншими вузлами у мережі. Це робить їх гнучкими та витривалими до відмов окремих вузлів, оскільки інші вузли можуть продовжувати збирати та передавати дані.

5. Резистентність до відмов: Безпроводові сенсорні мережі повинні бути стійкими до відмов окремих сенсорних вузлів або збоїв зв'язку. Для цього вони використовують механізми автоматичного виявлення відмов, резервування шляхів передачі даних та маршрутизації, що дозволяє забезпечити неперервну передачу інформації.

6. Обробка даних на місці (Edge Computing): Безпроводові сенсорні мережі використовують концепцію обробки даних на місці

(Edge Computing). Вузли мережі можуть виконувати певну обробку та аналіз даних непосредствено на місці збору, що дозволяє зменшити обсяг передаваної інформації та оптимізувати використання мережі.

Безпроводові сенсорні мережі знаходять застосування в різних галузях, таких як моніторинг навколишнього середовища, контроль і управління виробничими процесами, транспортна система, медичні технології, сільське господарство та багато інших. Вони дозволяють збирати реальні дані, виконувати аналітику та реагувати на зміни у режимі реального часу, що сприяє покращенню ефективності, безпеки та зручності в різних сферах діяльності.

В даній роботі розглядатиметься використання безпроводових сенсорних мереж у зонах підвищеної небезпеки.

1.2 Характеристика зон підвищеної небезпеки

Зони підвищеної небезпеки – це території, де існує підвищений рівень ризику для життя, здоров'я та майна людей. Ці зони можуть бути пов'язані з різними небезпечними ситуаціями, такими як природні катастрофи, епідемії, техногенні аварії або конфлікти. Основні характеристики зон підвищеної небезпеки включають наступне:

1. Високий рівень ризику: Зони підвищеної небезпеки характеризуються значним ризиком для життя та здоров'я людей. Це може бути пов'язано з потенційними загрозами, такими як землетруси, повені, шторми, вулканічна активність, епідемії захворювань або військові дії.
2. Обмеження та евакуація: У зонах підвищеної небезпеки можуть бути встановлені обмеження на доступ людей та рух транспорту. У разі настання небезпечних ситуацій може бути оголошений режим евакуації, коли мешканці повинні залишити зону

для своєї безпеки.

3. Планування навколишнього середовища: Зони підвищеної небезпеки можуть мати обмеження на будівництво та розвиток інфраструктури. Це пов'язано з необхідністю збереження природних ресурсів та зменшення ризику для мешканців.

4. Системи попередження та захисту: У зонах підвищеної небезпеки можуть бути розроблені системи попередження та захисту, що допомагають сповіщати населення про небезпеку та надавати необхідні інструкції для поведінки в екстремальних ситуаціях.

5. Спеціальні заходи безпеки: Можуть бути встановлені спеціальні правила та процедури безпеки для жителів та відвідувачів зон підвищеної небезпеки. Це може включати вимоги до особистого захисту, проведення евакуаційних тренувань та надання першої допомоги.

Важливо зауважити, що характеристики зон підвищеної небезпеки можуть варіюватися залежно від конкретного контексту та типу небезпеки, що існує у даній зоні.

1.2.1 Характеристика зон підвищеної небезпеки під час військових дій

Окремо слід звернути увагу на проблематику сьогодення та характеристику зон підвищеної небезпеки під час військових дій.

Зони підвищеної небезпеки під час воєнних дій – це території, на яких існує високий рівень ризику для цивільного населення та інфраструктури через активні бойові дії та наслідки військових операцій. Ці зони відображають небезпеку, яка виникає внаслідок наявності бойових сил, зброї, вибухівки та інших елементів, які можуть призвести до поранень, смерті або матеріальних збитків [4].

Зони підвищеної небезпеки можуть включати такі елементи:

- Фронтową лінію: це лінія розмежування між ворожими військовими силами. На цій лінії відбуваються активні бойові дії, включаючи стрілянину, артилерійську обстріл, повітряні атаки та мінні поля. Це найбільш небезпечна зона, оскільки ризик поранень та втрати життя величезний.

- Військові бази та табори: ці об'єкти є ціллю для ворожих атак, оскільки містять велику кількість військової техніки, боєприпасів та військового персоналу. У разі атаки на такі об'єкти може відбутися значний вибуховий ефект, спалахи пожежі та руйнування, що призводять до серйозних наслідків для навколишнього середовища та мешканців.

- Густонаселені райони: міста, селища та сільські населені пункти, розташовані в непосредственной близькості до зон бойових дій, також потрапляють у зону підвищеної небезпеки. Ці райони зазвичай стають мішенями для ворожих обстрілів та повітряних атак. Цивільні особи, які залишаються в цих районах, знаходяться під загрозою життя та можуть стати жертвами бойових дій.

- Об'єкти критичної інфраструктури: зокрема, електростанції, водопостачання, газопроводи, мости, транспортні вузли та комунікаційні мережі. Руйнування або пошкодження цих об'єктів може призвести до переривання постачання електроенергії, води та інших життєво важливих ресурсів, що погіршує гуманітарну ситуацію та ускладнює надання допомоги постраждалим.

- Полігони та місця зберігання зброї: ці об'єкти містять значну кількість вибухових речовин, боєприпасів та інших небезпечних матеріалів. Вони можуть стати мішенями для ворожих атак або ж піддаватися пошкодженням під час бойових дій, що призводить до вибухів, пожеж та забруднення довкілля.

У зонах підвищеної небезпеки під час воєнних дій дуже важливо

дотримуватися заходів безпеки та слухатися інструкцій військових та цивільних організацій. Також важливо мати на увазі, що ці зони можуть зазнавати змін через рух військ та зміну стратегічних об'єктів, тому необхідно бути в курсі останньої інформації та оновлювати дані про зони підвищеної небезпеки для забезпечення безпеки всіх осіб, що перебувають в цих районах.

1.3 Способи використання засобів телекомунікаційної інфраструктури в зонах підвищеної небезпеки

Використання засобів телекомунікацій у зонах надзвичайних ситуацій має велике значення для забезпечення ефективної комунікації, координації дій та оперативного реагування в умовах кризових ситуацій. Телекомунікаційні технології можуть бути використані на різних етапах надзвичайних подій, починаючи з попередження про небезпеку до організації рятувальних та відновлювальних робіт.

Одним із основних аспектів використання телекомунікацій у надзвичайних ситуаціях є система екстреної інформаційної передачі (СЕІП). Ця система включає в себе телефонні мережі, радіокомунікаційні системи, мобільний зв'язок, супутникові засоби зв'язку, Інтернет та інші засоби передачі даних. Завдяки СЕІП можна швидко та ефективно розповсюджувати інформацію про небезпеку, інструкції з евакуації, організувати допомогу та координацію дій рятувальних служб [3-4].

У зонах надзвичайних ситуацій можуть бути використані спеціальні мобільні комунікаційні пункти, що дозволяють оперативно розгортати тимчасові мережі зв'язку. Ці пункти обладнані радіостанціями, супутниковими телефонами, комп'ютерами та іншою необхідною технікою для забезпечення зв'язку між рятувальними службами, лікарнями, штабами управління та іншими важливими точками.

Також важливим аспектом є використання безпілотних літальних

апаратів (дронів) з встановленими телекомунікаційними засобами. Дрони можуть бути використані для встановлення мобільних комунікаційних станцій у важкодоступних місцях, для забезпечення зв'язку з пошуковими загонами або для отримання візуальної інформації з небезпечних ділянок.

Крім того, телекомунікаційні засоби можуть бути використані для моніторингу та передачі даних про стан навколишнього середовища, виявлення хімічних, біологічних або радіаційних загроз, а також для координації дій груп рятувальників та виклику додаткової допомоги.

Загалом, використання засобів телекомунікацій у зонах надзвичайних ситуацій дозволяє покращити ефективність дій рятувальних служб, збільшити швидкість реагування на небезпеку та зменшити можливі наслідки кризових ситуацій. Це важливий елемент системи попередження та управління надзвичайними ситуаціями, який допомагає зберегти життя та майно людей [4].

1.4 Актуальність використання телекомунікаційних вузлів для створення безпроводових сенсорних мереж в зоні надзвичайної ситуації

На сьогоднішній день спостерігаються певні тенденції у розвитку засобів обробки та розподілення інформації, а також інформаційних систем взагалі. З одного боку, розвиток телекомунікаційних мереж потребує використання цифрових каналів та систем передачі даних, а також засобів обчислювальної техніки для обробки інформації під час її передачі. З іншого боку, розвиток засобів обробки інформації та обчислювальної техніки потребує все більшого застосування засобів зв'язку для організації обміну інформацією з метою вирішення прикладних задач. Цей процес інтеграції та зближення телекомунікаційних мереж і засобів інформатизації призводить до перетворення телекомунікаційних мереж у мережі інфокомунікації.

Згідно зі звичайними уявленнями, інфокомунікаційна система - це

комбінація інформаційної і телекомунікаційної систем, що включає в себе різноманітні компоненти. Інформаційна система включає в себе саму інформацію і користувачів, тоді як телекомунікаційна система відповідає за передачу інформації від джерела до споживача. Отже, інфокомунікаційна система складається з мережі телекомунікацій (телекомунікаційна підсистема), прикладної підсистеми (засоби зберігання і обробки інформації, прикладні процеси) і підсистеми джерел і споживачів інформації (користувацька підсистема).

Інфокомунікації – інформаційно-телекомунікаційна інфраструктура, яка розвивається згідно з техніко-економічними законами розвитку суспільства.

Вузли мережі є спеціальними пристроями, які з'єднуються з іншими пристроями, утворюючи структуровану систему. Їх можна класифікувати за ступенем мобільності на стаціонарні, рухомі та повітряні вузли. Стаціонарні вузли - це наземні пристрої, які не змінюють своє місце розгортання. Рухомі вузли, натомість, пов'язані з оперативним переміщенням мережі на певну відстань. Повітряні вузли, залежно від їх основного місця розташування, знаходяться в повітряному просторі, який забезпечує зв'язок з іншими вузлами мережі.

У бездротових сенсорних мережах основна обробка даних здійснюється на вузлі, що називається шлюзом. Шлюз - це потужний комп'ютер, як і сенсор, він має антену для отримання даних від сенсорів. Проте шлюз отримує інформацію лише від сенсорів, що знаходяться у безпосередній близькості до нього, а дані з інших сенсорів також потрібно доставити до шлюзу. Цю проблему вирішується шляхом обміну інформацією між сенсорами за допомогою прийомопередавачів, які працюють у радіодіапазоні. Сенсори обмінюються даними один з одним, включаючи інформацію про стан пристроїв та результати передачі даних. Інформація передається від одного сенсора до іншого, утворюючи ланцюжок, і найближчі до шлюзу сенсори передають йому всю зібрану інформацію. У разі виймання із ладу одного з сенсорів, всі сенсори мережі повинні переконфігуруватися, а передача даних

продовжується. Інформація, що проходила через несправні сенсори, змінює маршрут, виключаючи несправні сенсори і будуючи новий маршрут лише через робочі.

Для виконання цих завдань кожному сенсору встановлюється спеціальна операційна система. Ця операційна система дозволяє сенсорам автоматично встановлювати зв'язки з сусідніми сенсорами і формувати мережу з заданою топологією.

Найчастіше сенсорні мережі складаються з сотень або навіть тисяч сенсорів, і розробка схеми обміну даними між ними є дуже складною задачею. Крім того, потрібно враховувати той факт, що бездротові сенсорні мережі працюють в ISM-діапазоні (діапазоні промислового, наукового та медичного використання) – це діапазон загального призначення, який може використовуватися без спеціального ліцензування. Це може спричинити певні перешкоди з боку зовнішніх джерел радіосигналів.

Крім того, через обмежену енергоефективність або вплив зовнішніх перешкод сенсори можуть вийти з ладу на певний час або назавжди. У таких випадках схеми організації мережі та маршрутизації передачі даних повинні автоматично змінюватися. Цю функцію виконує операційна система, яка встановлена в кожен сенсор.

Часто сенсори повинні мати здатність самостійно визначати своє місцезнаходження відносно інших сенсорів. Це означає, що вони повинні визначити, до якого наступного сенсора вони передадуть дані, які в кінцевому підсумку мають надійти до шлюза. Отже, при розгортанні безпроводової сенсорної мережі першим етапом є ідентифікація всіх сенсорів, а потім встановлюється схема маршрутизації.

1.5 Проблеми при проектуванні безпроводових сенсорних мереж

Незважаючи на їх високу практичну корисність, існують деякі проблеми

в безпроводовій системі сенсорної мережі.

Масштабованість – існує величезна різниця в масштабі такої сенсорної мережевої системи, оскільки кількість сенсорних вузлів може варіюватися від кількох до кількох. Крім того, щільність розгортання регулюється відповідно.

Енергоефективність – оскільки бездротові сенсорні вузли мають працювати з обмеженим джерелом живлення, розробка програмного та апаратного забезпечення має бути настільки оптимізована, щоб вона могла ефективно виконувати призначену роботу.

Технічне обслуговування – WSN має кілька обмежень, таких як джерело живлення, зберігання, велика кількість алгоритмів, тому існує серйозна проблема в обслуговуванні всього цього.

Безпека – як і всі програми, що залежать від Інтернету, WSN також має проблему незахищеності. Для протидії крадіжці даних усіма можливими способами слід застосувати належне управління передачею даних.

Якість обслуговування. Дані мають надаватися вчасно, оскільки додатки в режимі реального часу значною мірою залежать від своєчасно поширених даних [6].

Отже, основною метою дослідження є аналіз функціонування безпроводових сенсорних мереж у зонах підвищеної небезпеки. Досліджуються основні безпроводові технології, які можуть бути використані в таких мережах, і вибирається найоптимальніша з них. Також проводиться практична реалізація експериментальної сенсорної мережі з наземними вузлами з інформаційно-комунікаційними можливостями, а також робляться пропозиції щодо їх технічної реалізації.

Висновки до розділу1

В даному розділі уваліфікаційної роботи бакалавра було обґрунтовано актуальність, тематику та проблематику застосування безпроводових

сенсорних мереж у зонах підвищеної небезпеки.

Досліджено, що у випадку надзвичайних ситуацій важлива якість роботи телекомунікаційних систем для ефективного сповіщення населення та проведення пошукових операцій. Сенсорні мережі, завдяки своїм особливостям, є одним з найкращих варіантів для роботи в екстремальних умовах.

Основними характеристиками безпроводових сенсорних мереж в умовах надзвичайних ситуацій є захищеність кожного вузла та всієї мережі від зовнішніх впливів. Навіть при відмові деяких елементів мережі інші мають бути здатні перебудуватися для забезпечення неперервної роботи системи. Швидкість розгортання мережі в надзвичайних умовах є важливою характеристикою, яка досягається завчасною настройкою і готовністю всіх компонентів мережі. Передавані дані повинні бути захищені від перехоплення та використання сторонніми особами.

Різномаїття датчиків, які можуть бути використані в сенсорних мережах дає змогу зрозуміти, що, такі мережі можуть застосовуватися не тільки в різних видах надзвичайних ситуацій (природних, техногенних, терористичних, соціальних), але й у промисловому виробництві, сільському господарстві, медицині тощо.

Основною метою цієї роботи є дослідження основних безпроводових сенсорних технологій, аналіз їх використання в умовах надзвичайних ситуацій, реалізація експериментальної безпроводової сенсорної мережі і, як наслідок, внесення пропозицій щодо впровадження безпроводових сенсорних мереж у надзвичайних ситуаціях.

Наступним завданням розділу є аналіз найпоширеніших безпроводових технологій, які можуть бути використані в сенсорних мережах у надзвичайних ситуаціях, а також вибір найоптимальнішої технології на основі порівняльної характеристики.

2 ХАРАКТЕРИСТИКА ТЕХНОЛОГІЙ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ У ЗОНАХ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ

2.1 Аналіз технологій сенсорних мереж

2.1.1 Різні види безпроводових мереж

Мережа означає групу пристроїв, з'єднаних між собою для виконання певного завдання. Для досягнення цієї мети у нас є дві різні технології, а саме «проводова мережа» та «безпроводова мережа». Між ними двома часто віддається перевага з точки зору гнучкості, мобільності користувача, доступу до мережі тощо саме безпроводовій. У «безпроводовій сенсорній мережі» дані передаються за допомогою радіочастот, на відміну від дротової мережі, де передача даних відбувається через фізичні кабелі. Існують різні типи безпроводових мережних систем залежно від швидкості передачі даних або зони покриття (рис.2.1).

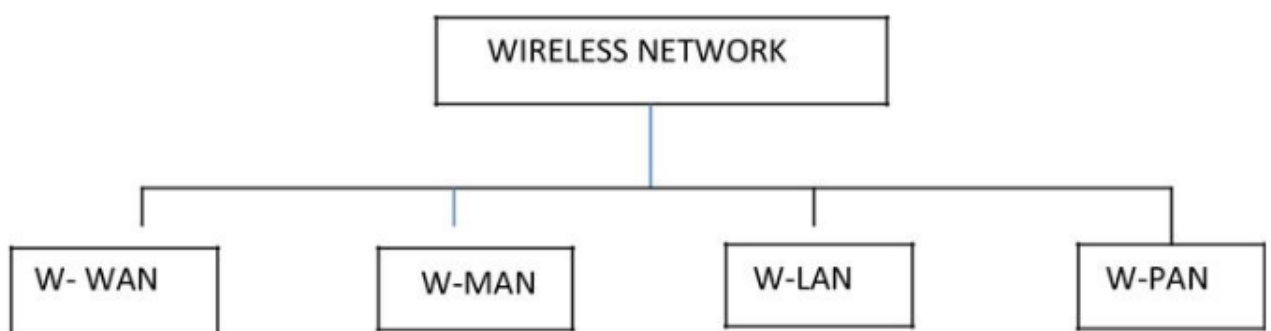


Рисунок 2.1 – Різні види WSN

W-WAN – безпроводова глобальна мережа. Як випливає з назви, це мережева система, яка може забезпечити передачу даних, голосу, зображень і відеоінформації на велику відстань у великій географічній зоні. Радіус дії W-

WAN перевищує 100 км. Цей тип мережі використовується для GSM, телефонних дзвінків, перегляду веб-сторінок тощо.

Технології, які використовуються в W-WAN:

- ISDN (цифрова мережа з інтегрованими послугами) – це одна з технологій, яка використовується для передачі даних, голосу та сигналізації, і це система телефонної мережі з комутацією каналів. Він добре відомий тим, що забезпечує кращу швидкість і якість, ніж традиційні з'єднання.
- SMDS (Switched Multimegabit Data Service) – це телекомунікаційна послуга з комутацією пакетів і розроблена для технології високошвидкісної широкосмугової мережі.
- SONET (синхронна оптична мережа) – це протокол зв'язку, який використовується для передачі великої кількості даних на великі відстані.
- HDLC (High Data Link Control) – це протокол передачі даних, і дані організовані в кадри, які передаються через мережу до пункту призначення, який підтверджує їх успішне надходження.
- SDLC (Контроль синхронного каналу передачі даних) – за допомогою цього протоколу можливий безпомилковий рух даних між мережевими адресними пристроями в даній мережі зв'язку.

W-MAN – безпроводова міська мережа. Це система безпроводової мережі, яка має здатність покривати територію розміром приблизно з місто, і вона знаходиться десь між W-LAN і W-WAN. З'єднання можуть бути «точка-точка» або «точка-точка» до кількох мереж.

W-LAN – безпроводова локальна мережа. Безпроводова локальна мережа – це безпроводова комп'ютерна мережа двох або більше пристроїв, які використовують бездротове з'єднання для створення локальної мережі в межах обмеженої території, наприклад у домі, школі, комп'ютерній лабораторії, кампусі чи офісній будівлі.

W-PAN – безпроводова персональна мережа. Персональна мережа – це

комп'ютерна мережа для з'єднання електронних пристроїв на робочому місці окремої людини. PAN забезпечує передачу даних між такими пристроями, як комп'ютери, смартфони, планшети та персональні цифрові помічники [6].

2.1.2 Стандарт IEEE 802.11

Усі стандарти Wi-Fi підпадають під егіду IEEE 802 для локальних і міських мереж, LAN / MAN. Стандарти Wi-Fi належать до серії IEEE 802.11.

Коли в 1997 році був випущений перший стандарт Wi-Fi, буква суфікса не була додана. Однак у міру випуску нових варіантів додано літеру-суфікс для позначення фактичної варіації. Ця літера була малою.

Різноманітні стандарти під егідою IEEE 802.11 охоплюють усе: від каналів до елементів системи, необхідних для взаємодії, наприклад, безпеки, гарячих точок, якості обслуговування, роумінгу тощо.

Нижче наведено основні стандарти IEEE 802.11:

802.11a: це був перший стандарт Wi-Fi у серії 802.11. Випущений у 1999 році, він визначив канал бездротової мережі, що працює в діапазоні ISM 5 ГГц, використовуючи ортогональне частотне мультиплексування зі швидкістю передачі даних до 54 Мбіт/с.

Незважаючи на те, що 802.11a використовувався, він був настільки ж широко поширений, як і версія 802.11b. Незважаючи на те, що діапазон 5 ГГц був набагато ширшим і вміщував набагато більше каналів, на той час технологія була дорожчою, і це значно скоротило її використання.

802.11b: стандарт 802.11b використовувався набагато ширше, ніж 11a. Хоча максимальна швидкість необроблених даних була набагато нижчою – 11 Мбіт/с, стандарт використовував діапазон ISM 2,4 ГГц, а технологія для цього на той час була набагато дешевшою. Крім того, використання Wi-Fi було набагато меншим, і перешкоди не були проблемою, яка була б сьогодні.

802.11e: однією з ключових областей надсилання даних через будь-яке

середовище є те, що називається якістю обслуговування або QoS, і пріоритезацією даних. IEEE 802.11e розглядає цю тему, щоб можна було застосувати певний підхід.

802.11f: IEEE 802.11f – це рекомендація, яка описує додаткове розширення до IEEE 802.11 для забезпечення безпроводового зв'язку точок доступу між системами різних виробників. IEEE 802.11 f був випущений для випробування його використання, але він не був прийнятий у всій галузі, тому його було відкликано в 2006 році.

802.11g: стандарт з'явився в результаті попиту на швидший Wi-Fi із використанням діапазону 2,4 ГГц. 802.11g використовує технологію OFDM і підтримує швидкість передачі необроблених даних 54 Мбіт/с.

Він також мав зворотну сумісність, дозволяючи спілкуватися з DSSS, але на нижчій швидкості 802.11b. Зворотна сумісність була вимогою з огляду на кількість старих точок доступу та комп'ютерів, які могли мати доступний лише старий стандарт. Ця вимога завжди важлива.

802.11h: Специфікація IEEE 802.11h-2003 визначає контроль живлення, необхідний для Wi-Fi. Він регулює розширення спектру та керування потужністю передачі та вирішує проблеми, зокрема можливі перешкоди супутникам і радарам, які також використовують діапазон ISM 5 ГГц. Стандарт спочатку передбачав динамічний вибір частоти (DFS) і керування потужністю передачі (TPC) для 802.11a PHY, але він також був інтегрований у повний стандарт IEEE 802.11-2007.

802.11i: безпека є основною проблемою для Wi-Fi, оскільки багато точок доступу Wi-Fi розташовані в громадських місцях і відкриті для хакерів, які можуть отримати небажаний доступ до пристроїв людей, які використовують цю точку доступу. Стандарт IEEE 802.11i використовується для забезпечення безпечного наскрізного зв'язку для бездротових локальних мереж. Стандарт IEEE 802.11i покращує механізми бездротової автентифікації, шифрування, керування ключами та детальної безпеки.

802.11j: IEEE 802.11j-2004 – це поправка до базового стандарту, яка

розширює бездротовий зв'язок і передачу сигналів для роботи в діапазоні 4,9 ГГц і 5 ГГц у Японії.

802.11k: стандарт IEEE 802.11 розширює механізми вимірювання радіоресурсів (RRM) для безпроводови локальних мереж. Він містить деякі рекомендації щодо оптимізації продуктивності WLAN.

802.11n: 802.11n або більш повно IEEE 802.11n-2009 – це стандарт Wi-Fi, який працює в діапазонах ISM 2,4 і 5 ГГц зі швидкістю передачі даних до 600 Мбіт/с. Він використовує технологію MIMO разом із агрегацією кадрів, а також забезпечує покращення безпеки порівняно з попередніми стандартами бездротового каналу. Wi-Fi Alliance також позначив технологію стандарту як Wi-Fi 4.

802.11s: Ця поправка до стандарту IEEE 802.11 стосується теми сітчастої мережі. У ньому детально описано, як пристрої Wi-Fi можуть з'єднуватися між собою для створення сітчастої мережі WLAN, яка може використовуватися для відносно фіксованих – немобільних топологій і безпроводових спеціальних мереж.

802.11u: IEEE 802.11u-2011 є поправкою до стандарту IEEE 802.11-2007. Він додає функції, які використовуються для взаємодії із зовнішніми мережами. Він використовується для роумінгу, а також для ініціативи Hotspot2.0.

802.11ac: IEEE 802.11ac зробив значний стрибок у плані продуктивності, коли він був представлений. Стандарт був випущений у 2013 році, але навіть незважаючи на те, що багато компаній бачили стандарт під час його випуску, пройшов деякий час після його випуску, перш ніж продукти побачили та стали широко використовувати. Стандарт визначає «носія безпроводової мережі» Wi-Fi, яка працює на частоті нижче 6 ГГц і забезпечує швидкість передачі даних щонайменше 1 Гбіт/с для роботи з кількома станціями та 500 Мбіт/с для одного каналу. Стандарт був позначений як Wi-Fi 5 Wi-Fi Alliance з огляду на його функції та продуктивність.

802.11ad: 802.11ad також відомий як WiGi або Gigabit Wifi, і він

розроблений для надання даних із надзвичайно високою пропускнуою здатністю та використовує для цього міліметрові діапазони хвиль, де є велика пропускна здатність. Він визначається як стандарт багатогігібної безпроводової системи (MGWS) і працює на частотах до 60 ГГц – це мережевий стандарт для мереж WiGig.

З огляду на дуже високі частоти, що використовуються, діапазони дуже обмежені – часто лише кілька метрів, і вони сильно послаблюються об'єктами, як стіни тощо, які пропускають сигнали з нижчих частот.

802.11af: у регіонах, де для телевізійних передавачів потрібні охоронні зони, часто є багато того, що називається білим простором, щоб передавачі, що використовують ту саму частоту, не створювали перешкод. У цих регіонах, де є пробіл, сигнали низької потужності можна використовувати для низки інших послуг, оскільки рівень їхньої потужності означає, що вони не поширюватимуться надто далеко та створюватимуть перешкоди основним користувачам. Одним із способів використання цього білого простору є Wi-Fi, і IEEE 802.11af визначено для роботи в цих регіонах. Зважаючи на його застосування та спосіб використання частоти, його часто називають White-Fi.

802.11ah: хоча діапазони 2,4 і 5 ГГц найбільш широко використовуються для Wi-Fi, є також деякі розподіли ISM нижче 1 ГГц. IEEE 802.11ah прагне використовувати неліцензований спектр нижче 1 ГГц. Одна з переваг полягає в тому, що він зможе забезпечувати зв'язок на великі відстані і, отже, підтримувати Інтернет всього. Недоліком цих діапазонів є те, що вони відносно вузькі, і це може обмежити швидкість передачі даних.

802.11ax: 802.11ax розглядається як майбутній наступник 802.11ac. Використовуючи технології, включаючи OFDMA, MU-MIMO та інші, його метою є підвищення спектральної ефективності, а отже, загальної зручності використання.

Табл. 2.1 демонструє порівняння стандартів IEEE 802.11.

Таблиця 2.1 – Порівняння стандартів IEEE 802.11

Стандарт IEEE 802.11	Максимальна швидкість передачі даних, Мбіт/с	Частотний діапазон	Приблизна дальність дії, м
802.11a	54 Мбіт/с	5 ГГц	до 50
802.11b	11 Мбіт/с	2,4 ГГц	до 150
802.11g	54 Мбіт/с	2,4 ГГц	до 150
802.11n	600 Мбіт/с (при використанні 4 антен)	2,4 або 5 ГГц	до 150
802.11ac	6,933 Гбіт/с (при 8х MU-MIMO- антенах)	5 ГГц	до 50

Захист безпроводової мережі в технології Wi-Fi є важливим аспектом забезпечення приватності та безпеки інформації, яка передається через бездротовий канал зв'язку. Недостатньо захищена безпроводова мережа може стати легкою мішенню для несанкціонованого доступу, перехоплення даних, атаки злому інформації або розповсюдження шкідливого програмного забезпечення.

Основних методи захисту безпроводової мережі Wi-Fi:

- Захищений доступ Wi-Fi (WPA2/WPA3): Використання протоколів захищеного доступу Wi-Fi, таких як WPA2 або більш нового стандарту WPA3, є важливим кроком у забезпеченні безпеки мережі. Вони забезпечують шифрування даних, яке унеможливорює простий перехоплення інформації.
- Сильний пароль: Встановлення складного та унікального пароля для мережі є необхідним. Він повинен містити комбінацію букв, цифр і символів, а також бути достатньо довгим. Такий пароль ускладнює завдання зловмисникам при спробах перебору або вгадування паролю.
- Вимкнення WPS: Wi-Fi Protected Setup (WPS) - це функція,

яка спрощує підключення нових пристроїв до мережі. Однак вона може бути вразлива до атак злому, тому рекомендується вимкнути WPS у налаштуваннях маршрутизатора.

- Зміна ідентифікатора мережі (SSID): За замовчуванням маршрутизатори надають мережам загальнодоступні ідентифікатори (SSID). Рекомендується змінити SSID на щось унікальне та не пов'язане з особистою інформацією, щоб зробити мережу важкодоступною для несанкціонованих користувачів.

- Фільтрація MAC-адрес: Можна ввести обмеження на доступ до мережі, дозволяючи лише підключення пристроїв з певними MAC-адресами. Це не повністю захищає мережу, але може бути додатковим шаром безпеки.

- Використання віртуальної приватної мережі (VPN): Використання VPN дозволяє шифрувати весь трафік, який проходить через безпроводову мережу, забезпечуючи додатковий рівень безпеки. Це особливо важливо, коли ви підключаєтесь до незахищених громадських Wi-Fi мереж.

- Часті оновлення програмного забезпечення: Важливо періодично оновлювати програмне забезпечення маршрутизатора і підключених до нього пристроїв. Виробники випускають оновлення для виправлення виявлених уразливостей та покращення безпеки.

Ці методи допоможуть вам захистити безпроводову мережу Wi-Fi від потенційних загроз і зберегти вашу інформацію в безпеці. Пам'ятайте, що безпека мережі - постійний процес, і важливо слідкувати за оновленнями та рекомендаціями забезпечення безпеки вашого маршрутизатора та пристроїв.

2.1.3 Стандарт Bluetooth

Bluetooth є бездротовим протоколом зв'язку, який дозволяє обмінюватися

даними між різними електронними пристроями через радіохвилі. Стандарт Bluetooth розроблений з метою створення надійного та простого у використанні способу підключення пристроїв без необхідності проводів.

Основні характеристики стандарту Bluetooth включають:

1. Передачу даних: Bluetooth може передавати дані зі швидкістю до 3 Мбіт/с, що зазвичай є достатньою для передачі аудіо, відео та інших типів файлів.
2. Частотний діапазон: Bluetooth використовує безліч радіочастотних діапазонів, включаючи 2,4 ГГц для Bluetooth Classic та 2,4 ГГц або 5 ГГц для Bluetooth Low Energy (LE).
3. Режими роботи: Bluetooth підтримує різні режими роботи, такі як режим передачі даних, режим голосового зв'язку та режим сполучення з точкою доступу до Інтернету (Internet Gateway).
4. Зона покриття: Зона покриття Bluetooth може варіюватися в залежності від версії протоколу та класу пристрою. Зазвичай це відстань до 10 метрів, але деякі пристрої можуть мати більший радіус дії.
5. Парування та безпека: Bluetooth використовує процес парування для встановлення зв'язку між пристроями. Це забезпечує безпеку та запобігає несанкціонованому доступу до даних.
6. Стандарт Bluetooth розподіляється на кілька версій, таких як Bluetooth 1.0, Bluetooth 2.0, Bluetooth 3.0, Bluetooth 4.0 (включаючи Bluetooth Low Energy), Bluetooth 5.0 та більш нові версії. Кожна нова версія протоколу вводить покращення, такі як збільшення швидкості передачі даних, зниження споживання енергії, покращену якість звуку тощо.

Bluetooth став широко використовуваним стандартом для підключення бездротових пристроїв, таких як навушники, гарнітури, клавіатури, миші, динаміки, смартфони, планшети та інші пристрої. Його використовують у різних галузях, включаючи домашню автоматизацію, звукові системи в

автомобілях, медичні пристрої та інші сфери життя.

Узагальнюючи, стандарт Bluetooth є важливою технологією бездротового зв'язку, яка дозволяє пристроям обмінюватися даними без необхідності використання проводів, що забезпечує зручність і легкість використання для користувачів.

Зв'язок за допомогою стандарту Bluetooth відбувається за допомогою радіохвиль у діапазоні від 2,4 ГГц до 2,4835 ГГц для Bluetooth Classic і 2,4 ГГц або 5 ГГц для Bluetooth Low Energy (LE). Цей діапазон розділений на 79 каналів, кожен з яких має ширину 1 МГц. Ширина каналу дозволяє передавати дані зі швидкістю до 1 Мбіт/с для Bluetooth Classic і до 2 Мбіт/с для Bluetooth Low Energy. У Bluetooth 5.0 швидкість передачі даних може сягати 2 Мбіт/с, а у Bluetooth 5.2 досягає 2 Мбіт/с з можливістю розширення до 5 Мбіт/с або 10 Мбіт/с у режимі двоканального даних.

Bluetooth має дві основні версії: Bluetooth Classic і Bluetooth Low Energy (LE). Bluetooth Classic був оригінальним варіантом, який надає широкий спектр функцій із підтримкою різних профілів, таких як Hands-Free Profile (HFP), Advanced Audio Distribution Profile (A2DP), File Transfer Profile (FTP) тощо. Ця версія використовує більше енергії, але забезпечує високу якість звуку і велику швидкість передачі даних.

Bluetooth Low Energy (LE) був впроваджений з версії Bluetooth 4.0 і призначений для пристроїв з низьким споживанням енергії, таких як фітнес-трекери, сенсори IoT, медичні пристрої тощо. Bluetooth LE пропонує меншу швидкість передачі даних, але значно економить енергію, що дозволяє пристроям працювати на одній батареї протягом довгих періодів часу.

Bluetooth також підтримує різні режими роботи. Найпоширенішими режимами є режим передачі даних, режим голосового зв'язку (для гарнітур і мікрофонів), режим сполучення з точкою доступу до Інтернету (Internet Gateway), режим мережі та режим ретрансляції сигналу. Це дає пристроям різноманітні можливості залежно від їх функціональних потреб.

Для забезпечення безпеки з'єднання Bluetooth використовує процес

парування. Парування може відбуватися за допомогою коду доступу, який вводится на обидва пристрої, або шляхом обміну криптографічними ключами. Це забезпечує захист від несанкціонованого доступу і забезпечує безпечний обмін даними між пристроями.

Загалом, стандарт Bluetooth є потужним засобом бездротового зв'язку, який забезпечує зручність і простоту використання. Його широке застосування в різних галузях дозволяє пристроям підключатися один до одного та обмінюватися даними з високою швидкістю і ефективністю [8].

У табл. 2.2 наведено класи пристроїв стандарту Bluetooth у вигляді порівняльної характеристики.

Таблиця 2.2 – Порівняльна характеристика класів пристроїв стандарту Bluetooth

Клас	Максимальна потужність, мВт	Максимальна потужність, дБм	Радіус дії (приблизно), м
1	100	20	100
2	2,5	4	10
3	1	0	1

Основні особливості Bluetooth 4.0:

- Низьке споживання енергії: Bluetooth 4.0 був спеціально розроблений для пристроїв з обмеженим живленням, таких як фітнес-трекери, сенсори IoT, медичні пристрої тощо. Це досягнуто шляхом зниження швидкості передачі даних і використання спеціальних режимів сну, що дозволяють значно зменшити споживання енергії.
- Короткий діапазон передачі: Зона покриття Bluetooth 4.0 зазвичай обмежена до відстані близько 10 метрів, хоча це може варіюватися в залежності від пристроїв та умов оточення. Це дозволяє пристроям економити енергію, оскільки зв'язок може бути

підтриманий на низькій потужності.

- Висока сумісність: Bluetooth 4.0 є зворотно сумісним з попередніми версіями Bluetooth, що дозволяє йому взаємодіяти з іншими Bluetooth-пристроями. Це означає, що пристрої, які підтримують Bluetooth 4.0, можуть працювати з раніше випущеними пристроями, що використовують Bluetooth Classic.

- Підтримка профілів: Bluetooth 4.0 підтримує різні профілі, які визначають функціональні можливості підключених пристроїв. Наприклад, профіль Health Device Profile (HDP) дозволяє зв'язувати медичні пристрої, такі як пульсометри або глюкометри, зі смартфонами або комп'ютерами.

- Широке застосування: Bluetooth 4.0 застосовується в різних галузях, включаючи фітнес і здоров'я, домашню автоматизацію, IoT, розумні годинники та багато інших. Його низьке споживання енергії та можливість працювати з малими батареями роблять його особливо популярним у сферах, де важлива довготривала автономність пристроїв.

За допомогою цього стандарту, різноманітні сенсори, такі як температури, тиску, вологості, швидкості та інші, мають можливість передавати дані на різні пристрої управління, такі як мобільні телефони, КПК, ПК та інші.

Усе вищесказане дає змогу звести характеристики двох стандартів IEEE 802.15.4 та Bluetooth, порівняння яких наведено в таб.2.3.

Таблиця 2.3 – IEEE 802.15.4 і Bluetooth

Параметр	IEEE 802.15.4	Bluetooth
Частота	2,4 ГГц / 868 МГц / 915 МГц	2,4 ГГц
Швидкість передачі	20...250 кбіт/с	1000 кбіт/с
Розмір мережі	До 65536 вузлів	До 8 вузлів
Дальність дії	10...100 м	10...100 м

2.1.4 Стандарт ZigBee

ZigBee – це безпроводовий комунікаційний протокол, розроблений для мереж низької потужності, що використовують малоенергетичні радіочастоти. Він створений з метою забезпечення надійного, низькопотужного та енергоефективного зв'язку між різними електронними пристроями, які використовуються в різних областях, включаючи домашню автоматизацію, мережі сенсорів, освітлення, медичні пристрої та інші.

Основні характеристики стандарту ZigBee включають наступне:

- Низька споживання енергії: ZigBee працює на низьких радіочастотах та використовує малу кількість енергії для передачі даних. Це дозволяє пристроям, які використовують ZigBee, працювати на батарейках протягом тривалого часу без необхідності заміни або зарядки.
- Мале дальнодіючий радіус: ZigBee призначений для створення мереж, які охоплюють невеликі відстані, зазвичай до 100 метрів в прямому видимості. Це робить його ідеальним варіантом для використання в приміщеннях або в обмежених просторах, де потрібен надійний бездротовий зв'язок.
- Мережева топологія "зірка": Заснована на технології "зірка", мережа ZigBee має центральний вузол, який координує комунікацію з усіма підключеними пристроями. Це забезпечує швидкий та ефективний обмін даними між пристроями в мережі.
- Висока стійкість до перешкод: За допомогою технології прямої послідовної частотної демодуляції (DSSS), ZigBee забезпечує високу стійкість до перешкод, таких як шуми, інші бездротові пристрої або металеві перешкоди. Це дозволяє мережам ZigBee працювати надійно навіть в складних електромагнітних середовищах.
- Безпека: Забезпечення безпеки є важливим аспектом ZigBee. Він використовує шифрування AES-128 для захисту передачі даних в

мережі. Крім того, ZigBee має вбудовану функцію ідентифікації та автентифікації пристроїв, що дозволяє створювати безпечні мережі.

– Велика кількість пристроїв: За допомогою протоколу ZigBee можна підключати до 65 000 пристроїв до однієї мережі, що дозволяє створювати великі та розширені мережі для різних застосувань.

Загалом, ZigBee є енергоефективним, надійним та безпечним протоколом, який забезпечує низькопотужний бездротовий зв'язок для різних пристроїв. Його характеристики роблять його популярним в області "розумного дому", мереж сенсорів та інших схожих застосувань, де важлива низька споживання енергії та висока надійність зв'язку.

2.2 Вибір технології безпроводової сенсорної мережі у зонах підвищеної небезпеки

Після огляду основних безпроводових технологій, які використовуються в ISM діапазоні, можна порівняти деякі характеристики цих технологій (табл.. 2.4) для визначення найбільш доцільного використання певної технології при проектуванні безпроводової сенсорної мережі. Також варто зауважити, що ранні стандарти IEEE 802.11, такі як 802.11b, 802.11a, 802.11g, не включені в таблицю. Нові стандарти Wi-Fi, такі як 802.11n та 802.11ac, замінили їх.

Одним з головних недоліків мобільних Wi-Fi мереж є обмежений час роботи акумуляторних батарей. Однак цю проблему можна легко вирішити, використовуючи акумулятори різної ємності. Менш потужні акумулятори можуть бути достатніми для безпроводового функціонування сенсорної мережі з Wi-Fi. Але треба враховувати, що потужніші акумулятори зазвичай мають більші об'єми.

Ультраширокопasmогова (UWB) технологія також має свій недолік – дуже обмежений радіус дії. У сенсорних мережах відстань між сенсорами може бути декілька десятків метрів, тому використання UWB може бути неефективним.

Такий же недолік притаманний технології Bluetooth, де енергоефективність пристроїв забезпечується лише на відстані до 10 метрів. При збільшенні відстані зростає потреба в більшій потужності передавача і, відповідно, збільшуються енергозатрати.

Таблиця 2.4 – Порівняльна характеристик технологій безпроводових мереж

Стандарт	802.11n	802.11ac	Bluetooth (802.15.1)	ZigBee (802.15.4)	UWB (802.15.3)
Частота	2,4 / 5 ГГц	5 ГГц	2,4 ГГц	868 МГц / 915 МГц / 2,4 ГГц	3,1...10,6 ГГц
Максимальна швидкість	600 Мбіт/с	6,93 Гбіт/с	1, 3, 24 Мбіт/с (дод. 55 Мбіт/с)	20 кбіт/с / 40 кбіт/с / 250 кбіт/с	480 Мбіт/с
Дальність дії	До 150 м	До 50 м	До 100 м	До 100 м	До 10 м
Енергозбереження	Низьке	Низьке	Високе	Дуже високе	Дуже високе
Розмір мережі	Не рекомендується більше 40	Не рекомендується більше 40	Майстер + 7	65536 (16-бітні адреси), 264 (64-бітні адреси)	До 127/хост
Основні переваги	Відносно висока швидкість	Висока швидкість	Енергозбереження	Енергозбереження, розміри мережі, вибір частотних діапазонів	Висока швидкість, енергозбереження

Тому, щоб вирішити практичні завдання щодо впровадження безпроводових сенсорних мереж у зонах з підвищеною небезпекою, найбільш доцільним вибором є використання технології Wi-Fi як основної безпроводової технології для передачі даних.

При проектуванні безпроводової сенсорної мережі на основі Wi-Fi, цю мережу дуже легко масштабувати, що означає можливість збільшувати її

обсяги, не зменшуючи технічних характеристик мережі самої по собі. Для розширення мережі достатньо просто додати нову точку доступу, до якої можуть підключатися додаткові сенсори, і з'єднати її з іншими точками або з головним шлюзом.

При виникненні проблеми з будь-яким сенсором, це не вплине на роботу всієї мережі, оскільки кожен сенсор підключений до власної точки доступу. Є ризик лише у випадку відмови самої точки доступу або шлюзу, тому при проектуванні мережі необхідно приділити особливу увагу захисту даних вузлів.

Wi-Fi технологія забезпечує високий рівень безпеки мережі за допомогою нового стандарту захисту WPA2 та дотримання основних правил безпеки, таких як використання надійного пароля для доступу до мережі та його періодична зміна. Це запобігає несанкціонованому доступу сторонніх осіб до мережі з метою перехоплення інформації.

Усі недоліки Wi-Fi технології в проектуванні бездротових сенсорних мереж, які були описані вище, компенсуються. Наприклад, для забезпечення постійного живлення елементів мережі використовуються дві акумуляторні кислотні батареї (АКБ) з напругою 12 В і ємністю 33 А·год.

Висновки до розділу 2

В даному розділі випускної кваліфікаційної роботи бакалавра проведений аналіз сучасних безпроводових технологій і стандартів для використання під час проектування сенсорних мереж. Виходячи з проведених досліджень можна зробити висновок, що існує багато безпроводових технологій передачі даних, які можуть бути використані у сенсорних мережах. Найпопулярніші з них – Wi-Fi, Bluetooth та ZigBee.

У сучасному житті найбільш поширеною технологією у сенсорних мережах є 802.11.xx (Wi-Fi). Основна особливість цієї мережі полягає у

високій пропускній здатності та системі захисту переданої інформації. У бездротовій сенсорній мережі пристрої ієрархічно поділяються на координатор-шлюз, який отримує всю зібрану інформацію з мережі, обробляє її та може передавати її в зовнішню мережу; маршрутизатор - зазвичай, точка доступу, яка отримує інформацію від сенсорів, зберігає її та передає координатору; кінцевий пристрій – виконує функції збору та передачі інформації в напрямку до координатора. Бездротові сенсорні мережі є стійкими до виходу з ладу одного або декількох її елементів.

При проектуванні бездротових сенсорних мереж можна також використовувати інші технології бездротової передачі даних, залежно від потреб сенсорної мережі, враховуючи та компенсуючи їх недоліки.

Завданням наступного розділу є аналіз найпоширеніших топологій сенсорних мереж, практична реалізація експериментальної сенсорної мережі з інфокомунікаційними наземними вузлами, а також внесення пропозиції щодо її модернізації.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ У ЗОНАХ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ

3.1 Вибір топології для проектованої безпроводової сенсорної мережі

Існує сім основних типів топології мережі.

1. Топологія мережі «точка-точка».

Топологія мережі «точка-точка» є найпростішим методом. Цей тип мережевої топології передбачає з'єднання двох вузлів або пристроїв за допомогою загального каналу зв'язку. Два пристрої можуть бути двома комп'ютерами, серверами, маршрутизаторами або комутаторами, з'єднаними між собою кабелем. Топологія мережі «точка-точка» поширена в комп'ютерних мережах, комп'ютерній архітектурі та телекомунікаційних системах [10]. Деякі з переваг використання топології мережі «точка-точка» включають:

1. Висока пропускна здатність і швидкість.
2. Низька затримка.
3. Легке обслуговування.

2. Топологія шинної мережі

Топологія шинної мережі є основоположним методом, який використовують багато мережевих адміністраторів для підключення всіх пристроїв або вузлів до одного основного кабелю за допомогою різноманітних роз'ємних ліній і відводів. Лінії відводу – це кабелі, які з'єднуються з основним кабелем, також відомим як шина, тоді як відводи – це окремі роз'єми. Це створює один канал для зв'язку по всій мережі. Коли хтось використовує свій комп'ютер для надсилання повідомлення через цей тип мережі, усі підключені комп'ютери знають про цю дію [10].

Однак лише одержувач повідомлення може прийняти його, перевіривши його адресу, яка додається до кадру даних. Решта комп'ютерів у топології шинної мережі автоматично відхиляють повідомлення. Щойно повідомлення

досягає місця призначення, термінатор видаляє ці дані з лінії зв'язку, щоб запобігти перериванню потоку даних і відхиленню сигналу. Це налаштування часто є чудовим варіантом для невеликих мереж, оскільки кожен комп'ютер у мережі працює незалежно, маючи доступ до всіх можливостей мережі.

Використання топології шинної мережі дає такі переваги:

1. Легка установка та впровадження.
2. Мінімум кабелів.
3. Економічна ефективність.

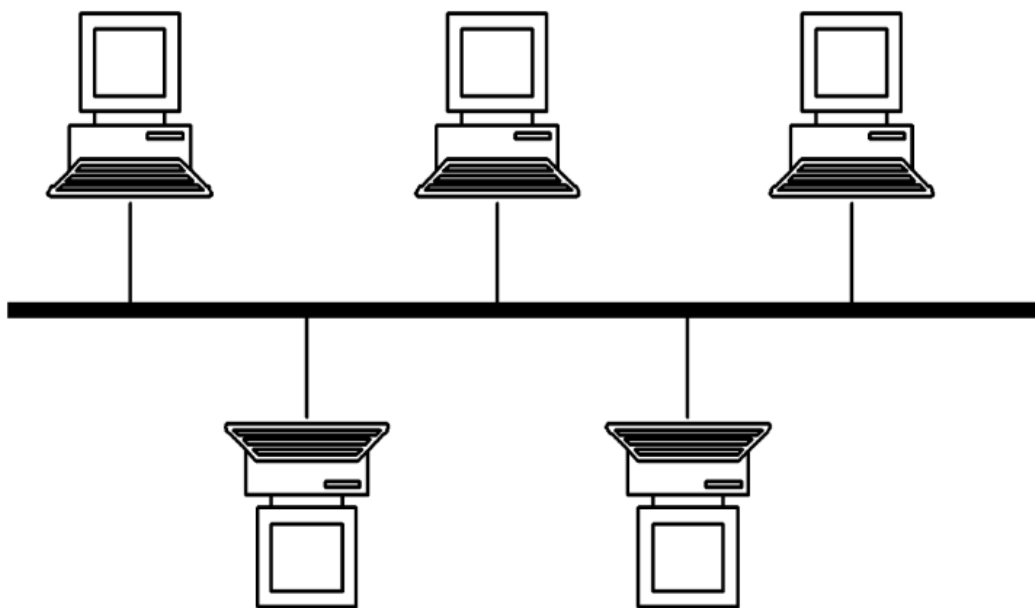


Рисунок 3.1 – Топологія шина

3. Кільцева топологія мережі.

Кільцева топологія мережі складається з двох основних каналів «точка-точка», які з'єднують один пристрій із двома іншими пристроями, розташованими з кожного боку від нього. Це створює кільце пристроїв, через які дані можуть проходити, поки вони не досягнуть цільового пристрою. У цій конфігурації шлях передачі повідомлень від одного пристрою до іншого є циклічним і односпрямованим. Кожен пристрій або комп'ютер у кільці має доступ до повідомлення протягом фіксованого періоду часу, щоб допомогти з передачею. Коли повідомлення досягає місця призначення, одержувач видаляє

дані [10]. Деякі з переваг використання кільцевої топології мережі включають:

1. Легкий монтаж.
2. Потрібна мінімальна кількість кабелів.
3. Зменшено зіткнення даних.

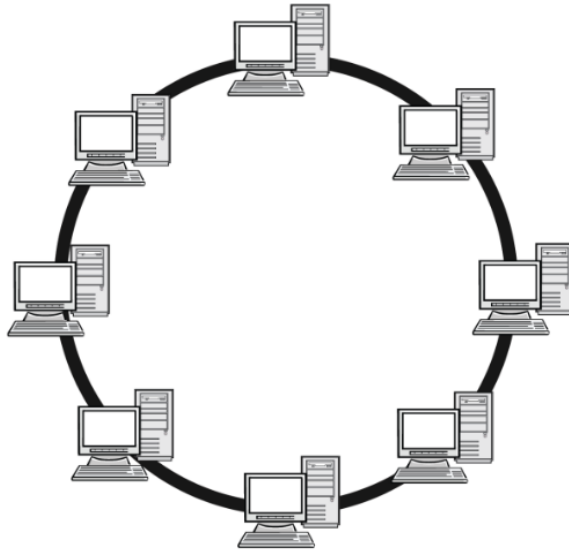


Рисунок 3.2 – Топологія кільця

4. Топологія мережі «зірка».

Зіркоподібна топологія мережі є найпоширенішою конфігурацією. У цій схемі кожен пристрій або вузол підключається до центрального мережевого концентратора. Пристрої використовують цей центральний концентратор для непрямого зв'язку один з одним. Якщо пристрій хоче надіслати або отримати повідомлення, він повинен спочатку зв'язатися з концентратором, щоб діяти як проміжне програмне забезпечення між пристроями. Коли концентратор розуміє, який тип повідомлення пристрій хоче надіслати, він передає його через широкомовну або одноадресну передачу призначеним одержувачам [10].

Щоб створити топологію мережі «зірка», мережеві адміністратори підключають кожен пристрій до концентратора за допомогою одного порту введення-виведення та одного кабелю. Основна причина такої популярності зіркової топології мережі полягає в тому, що вона покращує безпеку мережі, запобігаючи проходженню даних через усі пристрої. Серед інших переваг

використання зіркоподібної топології мережі:

1. Централізований контроль.
2. Легке масштабування та ре конфігурація.
3. Економічність.

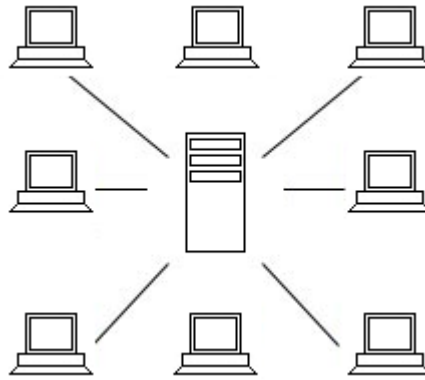


Рисунок 3.3 – Топологія зірки

5. Меш топологія мережі

Топологія сітчастої мережі передбачає створення спеціального зв'язку «точка-точка» між кожним пристроєм у мережі. Це дозволяє передавати дані безпосередньо між двома пристроями без проходження через інші пристрої в тій же мережі. Існує два основних типи мережевих топологій. Перший – це топологія повної сітки. У цій конфігурації кожен вузол підключається до будь-якого іншого вузла в мережі [10].

Друга – часткова сітчаста топологія мережі. У цій схемі деякі вузли можуть бути підключені не до кожного окремого вузла в мережі. Зв'язки між вузлами в обох типах сітчастої топології мережі зазвичай є симплексними зв'язками, що означає, що дані переміщуються лише в одному напрямку. Однак деякі мережеві адміністратори можуть замінити два симплексні зв'язки на дуплексні, щоб дозволити передавати дані між двома вузлами в обох напрямках одночасно. Деякі з переваг використання сітчастої топології мережі включають:

1. Швидкий зв'язок.
2. Більше конфіденційності та краща безпека.

3. Зменшення заторів на каналах.

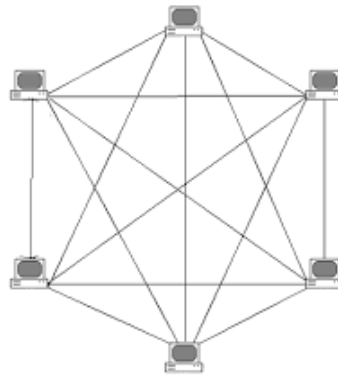


Рисунок 3.4 – Меш топологія

7. Деревоподібна топологія мережі.

Деревоподібна мережева топологія з'єднує зіркоподібні мережі шляхом об'єднання шинних мереж для створення ієрархії «батьківсько-начірній». У цій конфігурації кожен вузол прямо або опосередковано підключений до основного кабелю шини. Для цього адміністратори мережі ділять мережу на сегменти, що полегшує їх обслуговування. Кожен сегмент складається з основного концентратора, який з'єднує всі підхаби [10]. Деякі з переваг використання деревоподібної топології мережі включають:

1. Розширене покриття мережі.
2. Обмежена втрата даних.
3. Збільшена кількість прямих і непрямих вузлів.

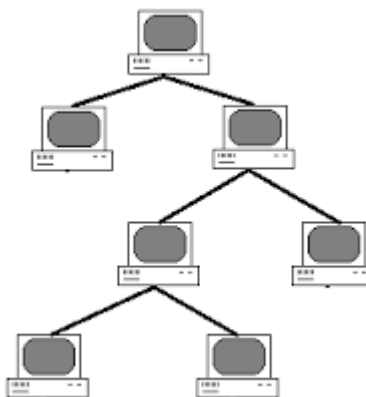


Рисунок 3.5 – Деревоподібна топологія

7. Топологія гібридної мережі.

Топологія гібридної мережі поєднує принаймні дві інші топології мережі. Цей тип конфігурації популярний, оскільки дозволяє мережевим адміністраторам створювати топології мережі, які є практичними та відповідають унікальним потребам кожної організації. Наприклад, мережевий адміністратор може використовувати топологію шинної мережі, щоб розмістити як топологію мережі «зірка», так і топологію кільцевої мережі, використовуючи роз'ємні лінії та відводи для з'єднання з ними [10].

Це полегшує мережевим адміністраторам вибір найкращих характеристик кожного типу топології мережі. Це також дозволяє їм налаштовувати мережеві топології для різних відділів організації, щоб покращити потік даних і підвищити безпеку за потреби. Деякі з переваг використання гібридної топології мережі включають:

1. Збільшений обсяг вузлів.
2. Покращена гнучкість.
3. Підвищена надійність.

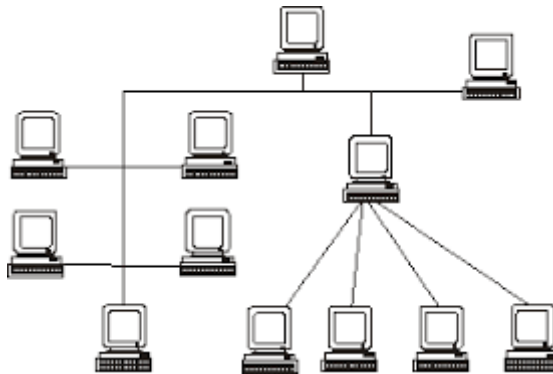


Рисунок 3.6 – Топологія гібридної мережі

Загалом, всі сенсори у класифікації за функціоналом і складністю можуть бути поділені на три категорії. Найскладніший клас включає найбільш складний сенсор за своєю будовою, який відповідає за управління всією бездротовою сенсорною мережею. Він зберігає дані про топологію мережі і виконує роль шлюзу для передачі даних, зібраних всією мережею, для

подальшої обробки. Цей тип сенсорів називається мережевим координатором або Network Coordination Device (NCD). Він має найбільший обсяг пам'яті та джерело живлення. Зазвичай в сенсорних мережах використовується лише один координатор.

Середньою за складністю категорією є маршрутизатор або повнофункціональний пристрій (FFD). Маршрутизатор може приймати і передавати дані, а також визначати напрямки передачі. Зазвичай він має додаткову пам'ять і джерело живлення порівняно зі звичайним сенсором.

Найпростішою категорією є звичайний сенсор або пристрій зі скороченим набором функцій (RFD). Найпростіший сенсор може лише передавати дані найближчому маршрутизатору.

Маршрутизатори, які отримують дані від сенсорів, утворюють кластер. Маршрутизатори різних кластерів передають дані один одному. В результаті, ці дані повинні бути доставлені до координатора. Координатор, що виступає шлюзом в сенсорній мережі, зазвичай має зв'язок з IP-мережею, куди відправляються дані для подальшої обробки.

Наведено приклад топології бездротової сенсорної мережі на рис. 3.7.

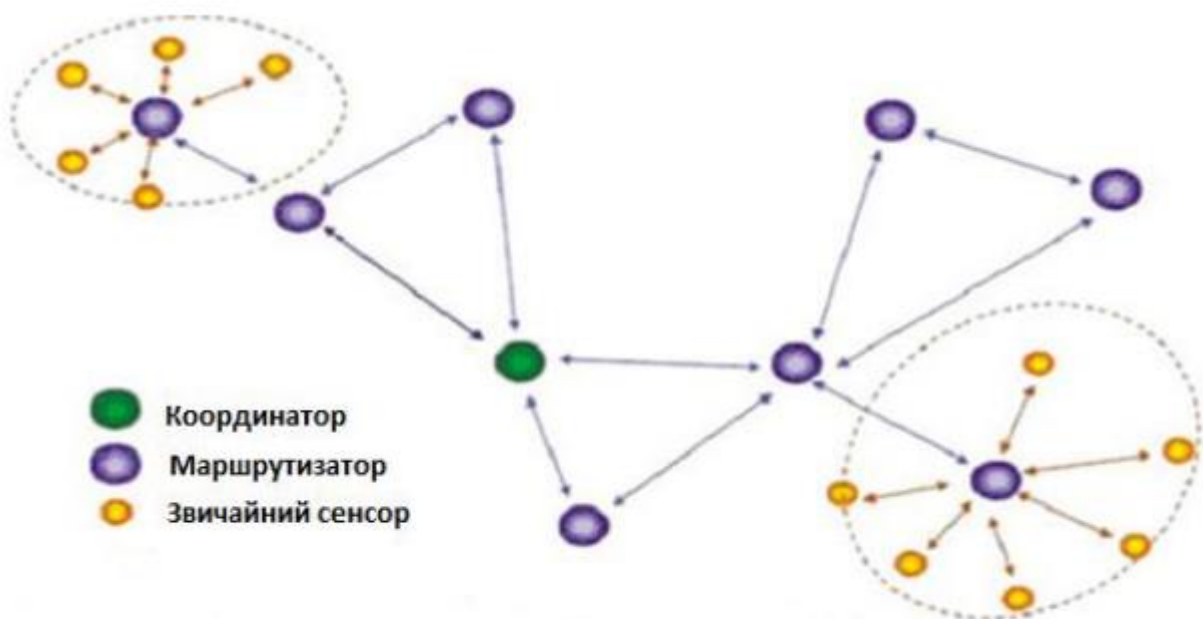


Рисунок 3.7 – Топологія безпроводової сенсорної мережі

3.2 Структурна схема проектованої безпроводової сенсорної мережі

Як було вказано раніше, фізична топологія визначає розташування вузлів і зв'язок між ними в мережі.

Проектована мережа складається з двох зон покриття – А і В. Є також персональний комп'ютер, який виконує роль центру керування мережею і має встановлений сервер для збору інформації з підключених до мережі сенсорів. Цей комп'ютер підключений до маршрутизатора за допомогою звичайного кабелю. Маршрутизатор може виступати шлюзом для з'єднання з глобальною мережею.

До маршрутизатора також підключена точка доступу, яка створює першу зону покриття. Ці точки доступу встановлені для забезпечення безпроводового зв'язку між зонами А і В.

В зоні В також є маршрутизатор, до якого підключена точка доступу, аналогічно зоні А разом це обладнання являє ще одну зону.

Роутер і точки доступу в зоні А живляться від акумуляторної батареї, що забезпечує неперервне живлення цих пристроїв. Аналогічно і у зоні В.

У зоні А підключені безпроводові пристрої: плата з Wi-Fi-інтерфейсом і відео-датчиком (сенсори), а також мобільний-пристрій з встановленим додатком клієнта. В зоні В також підключений Android-пристрій з клієнтом.

На рис. 3.8 зображена структурна схема проектованої сенсорної мережі.

Зони покриття А та В охоплюють відстань до 350 метрів (за теоретичними розрахунками – практично 500 метрів) і можуть розташовуватися на відстані до 1,75 кілометра одна від одної.

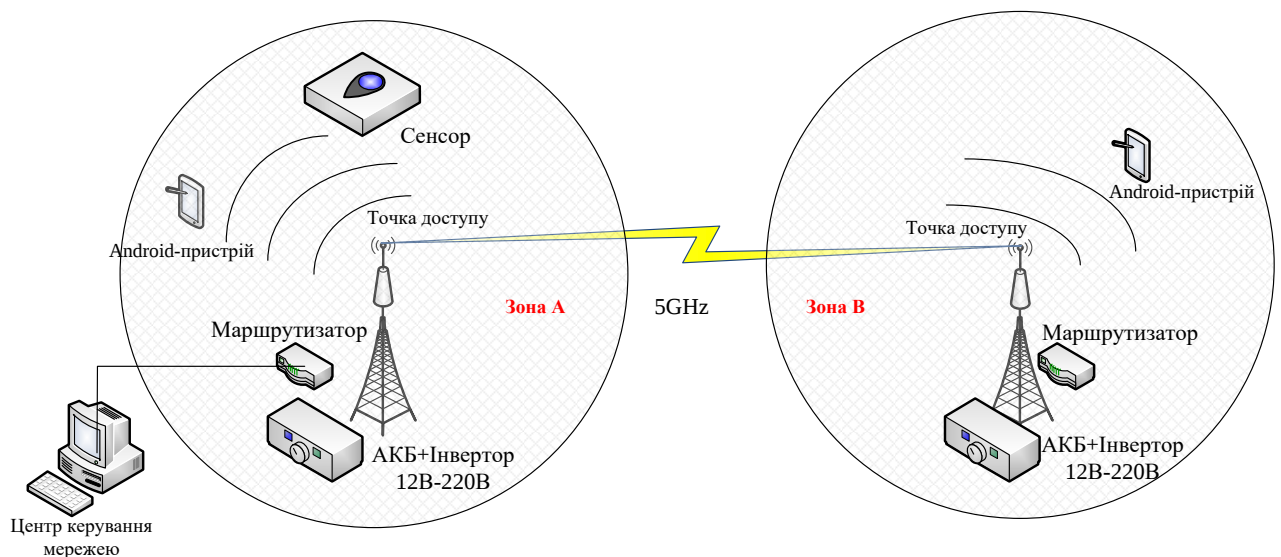


Рисунок 3.8 – Структурна схема проекрованої сенсорної мережі

3.3 Вибір обладнання для проекрованої безпроводової сенсорної мережі

У складі проекрованої проекрованої безпроводової сенсорної мережі є таке обладнання: маршрутизатори, точки доступу. Також використовується плата (сенсор), кілька Android-пристроїв з клієнтом і комп'ютер з сервером.

Маршрутизатори та точки доступу були обрані з урахуванням їх технічних характеристик, які ідеально підходять для виконання поставлених завдань. В таблицях 3.1, 3.2, 3.3, 3.4 наведено детальний опис технічних характеристик використовуваного обладнання.

В якості маршрутизаторів обрано маршрутизатори MikroTik RB2011iL-IN та MikroTik RB750r2 [11].

Таблиця 3.1 – Характеристики обраного маршрутизатора MikroTik RB2011iL-IN (рис.3.9)

Характеристика	Значення
Розміри	228x97x25 мм
Процесор	Atheros AR9344 600 МГц
Оперативна пам'ять (RAM)	64 MB DDR SDRAM
Роз'єми	5 × 10/100/1000 Mbit/s Ethernet RJ45 Auto-MDI/X 5 × 10/100 Mbit/s Ethernet RJ45 Auto-MDI/X
PoE вихід порт	№10 (500 mA)
Максимальна споживана потужність	до 6 Вт
Робоча температура	-35C to +65C



Рисунок 3.9 – Маршрутизатора MikroTik RB2011iL-IN

Таблиця 3.2 – Характеристики обраного маршрутизатора MikroTik RB750r2 (рис.3.10)

Характеристика	Значення
Розміри	113x89x28 мм
Процесор	Atheros QCA9531-BL3A-R 850 МГц
Оперативна пам'ять (RAM)	64 MB
Роз'єми	5 × 10/100 Mbit/s Ethernet RJ45
PoE вихід порт	Пасивний PoE (6-30 В)
Максимальна споживана потужність	до 2 Вт
Робоча температура	-40°C to 70°C

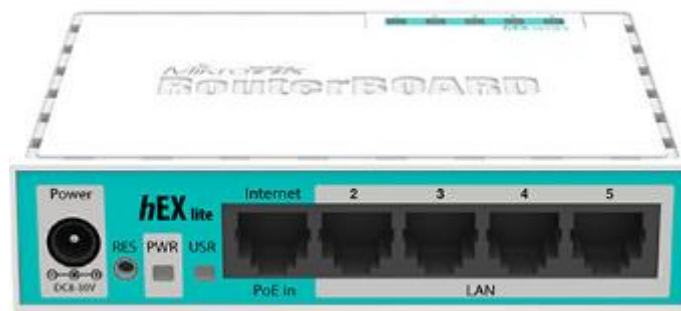


Рисунок 3.10 – Маршрутизатора MikroTik RB750r2

В якості точок доступу обрано точки доступу MikroTik Groove A-52HPn та MikroTik SXT Lite5 (рис.3.11).

Таблиця 3.3 – Характеристики обраної точки доступу MikroTik Groove A-52HPn

Характеристика	Значення
Розміри	177 × 44 × 44 мм
Процесор	Atheros AR9342 600 МГц
Оперативна пам'ять (RAM)	64 MB DDR2
Роз'єми	1 × 10/100 Base-TX (Cat. 5, RJ-45) Ethernet 1 × N-type Male
PoE вихід	Пасивний PoE (9-30 В)
Стандарти	802.11a/b/g/n
Режими роботи	Точка доступу, станція, точка-точка
Пропускна здатність	150 Мбіт/с
Частоти	2,4 або 5 ГГц (обирається програмно)
Робоча температура	-40°C to 70°C

Таблиця 3.4 – Характеристики обраної точки доступу MikroTik SXT Lite5

Характеристика	Значення
Розміри	140x140x56 мм
Процесор	Atheros AR9344 600 МГц
Оперативна пам'ять (RAM)	64 MB SDRAM
Роз'єми	1 × 10/100 Base-TX (Cat. 5, RJ-45) Ethernet
PoE вихід	Пасивний PoE (8-32 В)
Стандарти	802.11a/n
Режими роботи	Станція, точка-точка
Пропускна здатність	300 Мбіт/с
Частоти	5 ГГц
Робоча температура	-40°C to 70°C



Рисунок 3.11 – Точки доступу MikroTik Groove A-52HPn та MikroTik SXT Lite5

Зовнішній вигляд плат та сенсорних вузлів представлено на рис. 3.12-3.13.



Рисунок 3.12 – Зовнішній вигляд плат



Рисунок 3.13 – Зовнішній вигляд сенсорних вузлів

3.4 Функціональна схема проектованої безпроводової сенсорної мережі

На рис. 3.14 предсталена функціональна схема проектованої безпроводової сенсорної мережі з вказаним обладнанням.

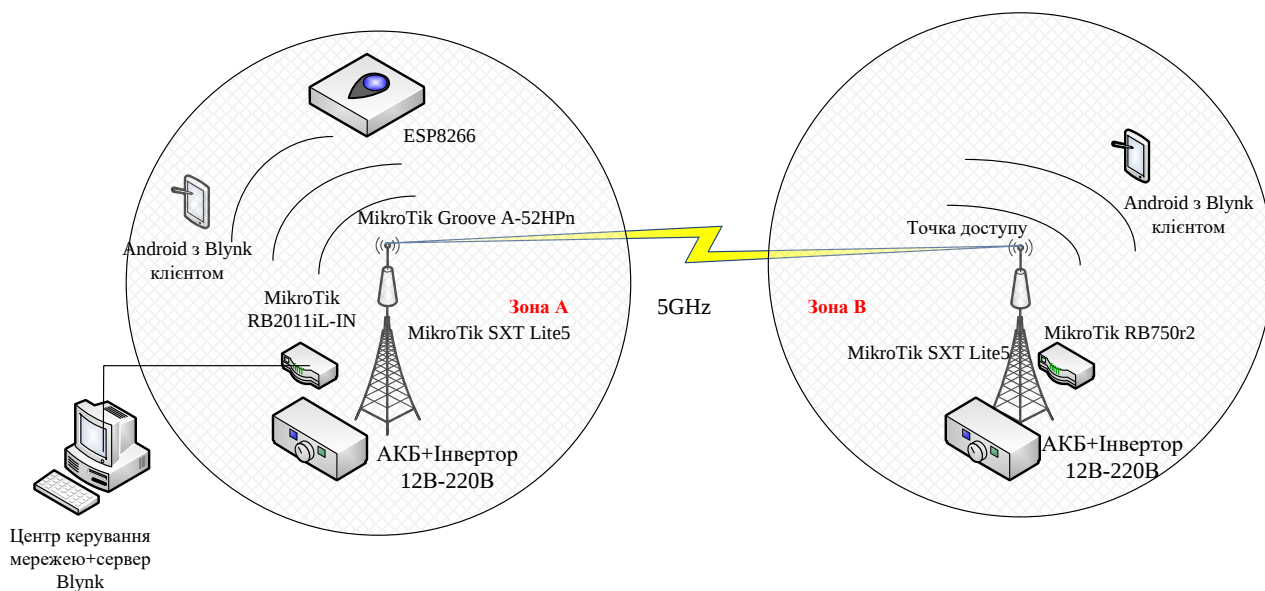


Рисунок 3.14 – 4Функціональна схема проектованої безпроводової сенсорної мережі

Розподіл адресного простору для обраного обладнання беручи до увагу знаходження в певній зоні проектованої безпроводової сенсорної мережі предстало в таблиці 3.5.

Таблиця 3.5 – Розподіл адресного простору

Пристрій	Розташування	ІР-адреса
MikroTik RB2011iL-IN	Зона А	192.168.88.10
MikroTik Groove A-52HPn	Зона А	192.168.88.52
MikroTik SXT Lite5	Зона А	192.168.88.21
ПК з сервером Blynk	Зона А	192.168.88.50
Плата ESP8266	Зона А	192.168.88.31
Android-пристрій з клієнтом Blynk	Зона А	192.168.88.33
MikroTik RB750r2	Зона В	192.168.88.2
MikroTik Groove A-52HPn	Зона В	192.168.88.25
MikroTik SXT Lite5	Зона В	192.168.88.22
Android-пристрій з клієнтом Blynk	Зона В	192.168.88.32

Висновки до розділу 3

В даному розділі випускної кваліфікаційної роботи бакалавра було проаналізовано найпоширеніші топологіями безпроводових сенсорних мереж є топологія "зірка", "дерево" та "комірка". Особливістю цих топологій є наявність єдиного головного вузла, відомого як шлюз, на який надходить вся зібрана інформація з сенсорів.

При проектуванні безпроводової мережі використовуються фізичні та логічні топології. Також розробляється процедура налаштування необхідного обладнання.

У результаті встановлюється зв'язок між пристроями, що знаходяться в різних зонах покриття мережі, і здійснюється керування сенсорами з мобільних пристроїв за допомогою спеціальної платформи.

Аналіз результатів дозволяє запропонувати шляхи модернізації сенсорної мережі, такі як розширення мережі шляхом збільшення зон покриття, збільшення кількості сенсорів та технічна модернізація елементів мережі.

ВИСНОВКИ

Мето роботи заключалась у дослідженні використання технологій безпроводових сенсорних мереж у зонах підвищеної небезпеки.

В першому розділі уваліфікаційної роботи бакалавра було обґрунтовано актуальність, тематику та проблематику застосування безпроводових сенсорних мереж у зонах підвищеної небезпеки.

Досліджено, що у випадку надзвичайних ситуацій важлива якість роботи телекомунікаційних систем для ефективного сповіщення населення та проведення пошукових операцій. Сенсорні мережі, завдяки своїм особливостям, є одним з найкращих варіантів для роботи в екстремальних умовах.

Основними характеристиками безпроводових сенсорних мереж в умовах надзвичайних ситуацій є захищеність кожного вузла та всієї мережі від зовнішніх впливів. Навіть при відмові деяких елементів мережі інші мають бути здатні перебудуватися для забезпечення неперервної роботи системи. Швидкість розгортання мережі в надзвичайних умовах є важливою характеристикою, яка досягається завчасною настройкою і готовністю всіх компонентів мережі. Передавані дані повинні бути захищені від перехоплення та використання сторонніми особами.

Різномаїття датчиків, які можуть бути використані в сенсорних мережах дає змогу зрозуміти, що, такі мережі можуть застосовуватися не тільки в різних видах надзвичайних ситуацій (природних, техногенних, терористичних, соціальних), але й у промисловому виробництві, сільському господарстві, медицині тощо.

Основною метою цієї роботи є дослідження основних безпроводових сенсорних технологій, аналіз їх використання в умовах надзвичайних ситуацій, реалізація експериментальної безпроводової сенсорної мережі і, як наслідок, внесення пропозицій щодо впровадження безпроводових сенсорних мереж у

надзвичайних ситуаціях.

Наступним завданням розділу є аналіз найпоширеніших безпроводових технологій, які можуть бути використані в сенсорних мережах у надзвичайних ситуаціях, а також вибір найоптимальнішої технології на основі порівняльної характеристики.

В другому розділі випускної кваліфікаційної роботи бакалавра проведений аналіз сучасних безпроводових технологій і стандартів для використання під час проектування сенсорних мереж. Виходячи з проведених досліджень можна зробити висновок, що існує багато безпроводових технологій передачі даних, які можуть бути використані у сенсорних мережах. Найпопулярніші з них – Wi-Fi, Bluetooth та ZigBee.

У сучасному житті найбільш поширеною технологією у сенсорних мережах є 802.11.xx (Wi-Fi). Основна особливість цієї мережі полягає у високій пропускній здатності та системі захисту переданої інформації. У бездротовій сенсорній мережі пристрої ієрархічно поділяються на координатор-шлюз, який отримує всю зібрану інформацію з мережі, обробляє її та може передавати її в зовнішню мережу; маршрутизатор - зазвичай, точка доступу, яка отримує інформацію від сенсорів, зберігає її та передає координатору; кінцевий пристрій – виконує функції збору та передачі інформації в напрямку до координатора. Бездротові сенсорні мережі є стійкими до виходу з ладу одного або декількох її елементів.

При проектуванні бездротових сенсорних мереж можна також використовувати інші технології бездротової передачі даних, залежно від потреб сенсорної мережі, враховуючи та компенсуючи їх недоліки.

Завданням наступного розділу є аналіз найпоширеніших топологій сенсорних мереж, практична реалізація експериментальної сенсорної мережі з інфокомунікаційними наземними вузлами, а також внесення пропозиції щодо її модернізації.

В третьому розділі випускної кваліфікаційної роботи бакалавра було проаналізовано найпоширеніші топологіями безпроводових сенсорних мереж є

топология "зірка", "дерево" та "комірка". Особливістю цих топологій є наявність єдиного головного вузла, відомого як шлюз, на який надходить вся зібрана інформація з сенсорів.

При проектуванні безпроводової мережі використовуються фізичні та логічні топології. Також розробляється процедура налаштування необхідного обладнання.

У результаті встановлюється зв'язок між пристроями, що знаходяться в різних зонах покриття мережі, і здійснюється керування сенсорами з мобільних пристроїв за допомогою спеціальної платформи.

Аналіз результатів дозволяє запропонувати шляхи модернізації сенсорної мережі, такі як розширення мережі шляхом збільшення зон покриття, збільшення кількості сенсорів та технічна модернізація елементів мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Research areas in Wireless Sensor Networks [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/344477013_Research_areas_in_Wireless_Sensor_Networks – Дата доступу: травень 2023. – Назва з титул. екрана.
2. Бездротові сенсорні мережі: опитування щодо моніторингу якості води [Електронний ресурс]. – Режим доступу: <https://www.elsevier.es/en-revista-journal-applied-research-technology-jart-81-pdf-S1665642317301037> – Дата доступу: травень 2023. – Назва з титул. екрана.
3. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/812-2004-%D0%BF#Text> – Дата доступу: травень 2023. – Назва з титул. екрана.
4. Про внесення змін до Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку у сфері цивільного захисту [Електронний ресурс]. – Режим доступу: https://www.drs.gov.ua/wp-content/uploads/2022/01/574_0_19-22.pdf – Дата доступу: травень 2023. – Назва з титул. екрана.
5. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review [Електронний ресурс]. – Режим доступу: <https://www.mdpi.com/1424-8220/22/6/2087> – Дата доступу: травень 2023. – Назва з титул. екрана.
6. Бездротові сенсорні мережі - проблеми дослідження та ефективні розумні рішення [Електронний ресурс]. – Режим доступу: <https://www.intechopen.com/online-first/86241> – Дата доступу: травень 2023. – Назва з титул. екрана.
7. Стандарти WiFi: IEEE 802.11 [Електронний ресурс]. – Режим доступу: <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802->

[11/standards.php](#) – Дата доступу: травень 2023. – Назва з титул. екрана.

8. Guide to Bluetooth Security [Електронний ресурс]. – Режим доступу: <https://www.nist.gov/publications/guide-bluetooth-security-2> – Дата доступу: травень 2023. – Назва з титул. екрана.

9. ZigBee vs Z-Wave [Електронний ресурс]. – Режим доступу: <https://www.smarty.ninja/zigbee/zigbee-vs-z-wave/> – Дата доступу: травень 2023. – Назва з титул. екрана.

10. 7 типів топології мережі (плюс визначення та ключові функції) [Електронний ресурс]. – Режим доступу: <https://www.indeed.com/career-advice/starting-new-job/network-topology-types> – Дата доступу: червень 2023. – Назва з титул. екрана.

11. MikroTik Routers and Wireless [Електронний ресурс]. – Режим доступу: <https://mikrotik.com/> – Дата доступу: червень 2023. – Назва з титул. екрана.