МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ

Кафедра Комп'ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Ігор ЖУКОВ
«___» _____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»
ЗА СПЕЦІАЛЬНІСТЮ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

Тема: Телекомунікаційні протоколи в мережах «Інтернет речей»

Виконавець: Микола МАКСЮТЕНКО
Керівник: Валентин ЄФИМЕЦЬ

Нормоконтролер: Василь МАЛЯРЧУК

Засвідчую, що у дипломній роботі немає запозичень праць інших авторів без відповідальних посилань
Студент _____ Микола МАКСЮТЕНКО

КИЇВ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Інститут Комп'ютерних інформаційних технологій
Кафедра комп'ютерних систем та мереж
Спеціальність 123 "Комп'ютерна інженерія"

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних систем та мереж
_____Ігорь ЖУКОВ
«_____»_____2023 р.

ЗАВДАННЯ

на виконання дипломного проекту

Максютенко Микола Миколайович

(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломного проекту Телекомунікаційні протоколи в мережах «Інтернет речей»
затверджена наказом ректора від "08" серпня 2023р., № 1521/ст

2. Термін виконання проекту: з "02" жовтня 2023 р. по "31" грудня 2023 р.

3. Вихідні дані до проекту: Вимоги до змісту телекомунікаційних протоколів в мережах «Інтернет речей»

4. Зміст пояснювальної записки: Аналіз об'єкта дослідження, детальний огляд телекомунікаційних протоколів, дослідження ефективності телекомунікаційних протоколів в мережах інтернет речей, захист даних і безпека в мережах інтернет речей.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: презентація *PowerPoint.*

6. Календарний план-графік

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Оглянути літературу	02.10.23 – 06.10.23	
2.	Розглянути вимоги до протоколів в мережах «Інтернет речей»	06.10.23 – 10.10.23	
3.	Аналіз об’єкта дослідження	11.10.23 – 17.10.23	
4.	Розглянути застосування телекомунікаційних протоколів	18.10.23 – 26.10.23	
5.	Оглянути телекомунікаційні протоколи	26.10.23 – 05.11.23	
6.	Дослідити ефективность телекомунікаційних протоколів в мережах інтернет речей	06.11.23 – 14.11.23	
7.	Порівняння протоколів та виявлення їх переваг та недоліків	14.11.23 – 20.11.23	
8.	Проаналізувати захист даних і безпеку в мережах інтернет речей	23.11.23 – 27.11.23	
9.	Оформити пояснювальну записку	28.11.23 – 20.12.23	
10.	Підготовити графічний демонстраційний матеріал	21.12.23 – 31.12.23	

7. Дата видачі завдання “02” жовтня 2023 р.

Керівник дипломної роботи _____ Валентин ЄФІИМЕЦЬ
(підпис)

Завдання прийняв до виконання _____ Микола МАКСЮТЕНКО
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до магістерської роботи «Телекомунікаційні протоколи в мережах «Інтернет речей»»: 95 с., 7 рис., 4 табл., 45 використаних джерел.

МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ, ТЕЛЕКОМУНІКАЦІЙНІ ПРОТОКОЛИ, ЕФЕКТИВНІСТЬ, СПОЖИВАННЯ ЕНЕРГІЇ, ПРОПУСКНА ЗДАТНІСТЬ, ЗАТРИМКА ПЕРЕДАЧІ ДАНИХ, ВЗАЄМОДІЯ, МАРШРУТИЗАЦІЯ, БЕЗПЕКА.

Об'єкт дослідження – телекомунікаційні протоколи в мережах Інтернет речей.

Предметом дослідження – телекомунікаційні протоколи в мережах Інтернет речей (*IoT*).

Мета дипломної роботи – "Дослідження телекомунікаційних протоколів в мережах Інтернет речей" є аналіз, порівняння та оцінка ефективності різних телекомунікаційних протоколів, які використовуються у мережах Інтернет речей.

Метод дослідження – аналіз літератури та документів з телекомунікаційних протоколів в мережах *IoT*, проведення експериментів для оцінки ефективності цих протоколів.

Результати – дослідження показало, що різні телекомунікаційні протоколи в мережах *IoT* мають свої переваги та обмеження. Вони відіграють важливу роль у забезпеченні зв'язку між пристроями, керуванні мережею та забезпеченні безпеки даних. Аналіз показав, що ефективність та захищеність цих протоколів може змінюватися в залежності від умов використання.

Наукова новизна одержаних результатів – Дослідження підкреслило нові можливості та важливість вибору оптимальних телекомунікаційних протоколів для мереж Інтернету речей. Результати підтвердили, що різні протоколи мають унікальні особливості, які варто враховувати при розгортанні мереж *IoT*. Це відкриває можливості для покращення ефективності та безпеки мереж шляхом обізнаного вибору та використання відповідних протоколів.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT	—	*Internet of Things*
BLE	—	*Bluetooth Low Energy*
MQTT	—	*Message Queuing Telemetry Transport*
CoAP	—	*Constrained Application Protocol*
HTTP	—	*Hypertext Transfer Protocol*
VPN	—	*Virtual Private Network*
VLAN	—	*Virtual Local Area Network*
MAC	—	*Media Access Control*
DHCP	—	*Dynamic Host Configuration Protocol*
CSMA	—	*Carrier Sense Multiple Access*

ВСТУП

В останні десятиліття зростання технологій та підключення до Інтернету привело до розвитку нової парадигми під назвою Інтернет речей (*Internet of Things - IoT*). Інтернет речей відкриває безліч можливостей для сполучення фізичних пристроїв, сенсорів та систем у єдину мережу, що дозволяє збирати, обробляти та обмінювати даними без прямого взаємодії людей. Успішна реалізація Інтернету речей залежить від належного використання телекомунікаційних протоколів, які забезпечують зв'язок між різними пристроями та системами.

Розуміння та оптимізація телекомунікаційних протоколів у цій сфері є критично важливими. Протоколи, як правила та стандарти для обміну даними, визначають ефективність та безпеку цієї комунікації. Вони служать фундаментом для надійного з'єднання між пристроями, забезпечуючи важливі функції, від простого виявлення пристроїв до складного шифрування даних. У цьому контексті, дослідження протоколів, які підтримують *IoT*, відкриває важливі перспективи для покращення комунікаційних систем.

Актуальність дослідження телекомунікаційних протоколів в мережах Інтернет речей (*IoT*) не можна недооцінювати у сучасному світі, де цифрові технології стрімко розвиваються та впливають на всі аспекти нашого життя. *IoT*, як важливий компонент цього технологічного прогресу, перетворює спосіб взаємодії людей з технологіями, інтегруючи "розумні" пристрої в повсякденне життя, промисловість, медицину, транспорт та багато інших сфер.

Ключовим елементом ефективного функціонування *IoT* є телекомунікаційні протоколи, які забезпечують надійний обмін даними між різноманітними пристроями та системами. Вибір та оптимізація цих протоколів відіграють вирішальну роль у забезпеченні ефективності, надійності, швидкості та безпеки комунікаційних процесів. Оскільки *IoT* стає все більш розповсюдженим, важливо зрозуміти, як саме ці протоколи працюють, та які вони мають переваги та недоліки у різних сценаріях.

Наразі *IoT* знаходиться на етапі інтенсивного розвитку, і це створює потребу у детальному дослідженні протоколів, які лежать в основі цієї технології. Це дослідження надзвичайно актуальне, адже відповідно до стандартів та протоколів, які будуть використовуватися, залежить безпека, конфіденційність даних, а також загальна ефективність *IoT*-систем. Розвиток нових протоколів, а також оптимізація існуючих, може внести значний вклад у розв'язання актуальних проблем, пов'язаних з масштабованістю, енергоефективністю та безпекою *IoT*.

Крім того, актуальність дослідження підсилюється швидким розвитком технологій та зростанням кількості *IoT* пристроїв, що вимагає неперервного оновлення та адаптації комунікаційних протоколів. В цьому контексті, глибоке розуміння телекомунікаційних протоколів відіграє ключову роль у створенні стійких та безпечних *IoT*-систем, здатних ефективно масштабуватися та адаптуватися до зростаючих вимог сучасного світу.

Мета цього дослідження полягає у глибокому аналізі телекомунікаційних протоколів, які використовуються в мережах Інтернет речей (*IoT*), з метою зрозуміти їх ключові характеристики, функціональність та вплив на ефективність та безпеку *IoT*-систем. У світлі стрімкого розвитку цифрових технологій та зростаючої інтеграції *IoT* у повсякденне життя, важливо забезпечити, щоб системи зв'язку були не тільки ефективними та надійними, але й безпечними та стійкими до потенційних загроз.

Центральним елементом дослідження є детальний аналіз різних телекомунікаційних протоколів, включаючи їхні архітектури, протоколи зв'язку, протоколи з'єднання з мережею та протоколи керування мережею. Ми прагнемо визначити, як ці протоколи впливають на загальну продуктивність, надійність та безпеку *IoT*-систем, а також розглянути їхні сильні та слабкі сторони в різних сценаріях застосування.

Крім того, це дослідження має на меті оцінити ефективність різних протоколів у контексті сучасних вимог до *IoT*, таких як масштабованість, енергоефективність та інтегрованість. Особливу увагу буде приділено аналізу методів захисту даних та

безпеки в мережах *IoT*, оскільки це є критично важливим для забезпечення приватності та конфіденційності у все більш пов'язаному світі.

Мета цього дослідження також включає в себе розробку рекомендацій щодо вибору та оптимізації телекомунікаційних протоколів для різних застосувань *IoT*. Ми прагнемо надати цінні висновки, які можуть бути використані розробниками, інженерами та дослідниками для покращення існуючих та розробки нових *IoT*-систем, забезпечуючи їх високий рівень продуктивності, надійності та безпеки.

Предметом даного дослідження є телекомунікаційні протоколи в мережах Інтернет речей (*IoT*). Зосередження уваги на цих протоколах дає можливість детально розглянути та аналізувати різні аспекти комунікації, які відіграють вирішальну роль у функціонуванні *IoT*-систем. Основна увага приділяється дослідженню особливостей, структури, механізмів дії та застосування різних видів телекомунікаційних протоколів, включаючи, але не обмежуючись, протоколами зв'язку між пристроями, протоколами з'єднання з мережею, протоколами керування мережею, а також протоколами, які забезпечують безпеку даних.

Протоколи, які розглядаються в цьому дослідженні, включають широко використовувані стандарти, такі як *HTTP, MQTT, CoAP, AMQP, WebSocket* та інші. Кожен з цих протоколів має свої унікальні характеристики та специфікації, які роблять їх придатними для певних сценаріїв використання в *IoT*. Основним завданням є вивчення того, як кожен протокол впливає на загальну ефективність, надійність, швидкість передачі даних та безпеку в мережах *IoT*.

Дослідження також звертає увагу на виклики та проблеми, пов'язані з інтеграцією та управлінням цими протоколами в різноманітних та часто складних екосистемах *IoT*. Це включає розгляд питань сумісності, масштабованості та енергоефективності, які є важливими для стабільної та ефективної роботи *IoT*-систем. Крім того, особлива увага приділяється питанням безпеки, зокрема, методам шифрування, аутентифікації та захисту конфіденційності, які є ключовими для захисту від зовнішніх загроз та забезпечення безпеки даних в *IoT*.

Об'єктом дослідження в цій магістерській роботі є мережі Інтернет речей (*IoT*). Цей вибір обумовлений важливістю та стрімким розвитком *IoT* у сучасному

світі. Мережі Інтернет речей унікальні своєю спроможністю інтегрувати велику кількість різноманітних пристроїв та датчиків, що здатні збирати, обробляти та передавати дані в автоматизований спосіб. Ці мережі відіграють ключову роль у формуванні сучасної цифрової інфраструктури, знаходячи застосування у різноманітних сферах – від побутових технологій до промислових систем.

У рамках цього дослідження особлива увага приділяється аспектам комунікації в мережах *IoT*, що охоплюють взаємодію між різними пристроями, обмін даними та їх обробку. Мережі *IoT* характеризуються своєю гетерогенністю, де різні пристрої та платформи вимагають взаємосумісності та ефективної інтеграції. Це створює складні виклики для проектування та управління мережами, особливо з точки зору вибору та налаштування телекомунікаційних протоколів.

Додатково, в контексті *IoT*, особливо актуальними є питання безпеки та конфіденційності. З огляду на те, що мережі *IoT* часто збирають та обробляють чутливі дані, забезпечення їх безпеки стає критично важливим. В цьому контексті, дослідження фокусується на аналізі протоколів та механізмів, які використовуються для захисту даних в мережах *IoT*, включаючи методи шифрування, аутентифікації та забезпечення цілісності даних.

Завдання практики:

1. Ознайомлення з концепціями та застосуванням Інтернету речей: Глибоке вивчення основних принципів *IoT*, його архітектури, ключових компонентів, та аналіз різноманітних областей застосування, включаючи домашнє автоматизування, промисловість, охорону здоров'я та транспортну систему.

2. Дослідження телекомунікаційних протоколів: Проведено детальний аналіз різноманітних протоколів, таких як *MQTT*, *CoAP*, *HTTP*, *AMQP*, їхніх особливостей та характеристик, із зосередженням уваги на їхній ролі в *IoT*.

3. Порівняння протоколів за ключовими критеріями: Виконано аналіз та порівняння цих протоколів за критеріями, такими як ефективність, споживання ресурсів, надійність, для оцінки їх придатності до різних застосувань в *IoT*.

4. Вивчення можливостей та обмежень протоколів для *IoT*-пристроїв: Детальний аналіз роботи протоколів в умовах обмежених ресурсів, характерних для *IoT*-пристроїв, з метою визначення їх ефективності та оптимальності.

5. Проведення практичних експериментів: Реалізація та оцінка протоколів на *IoT*-пристроях, щоб вивчати їх продуктивність та взаємодію з іншими пристроями в реальних умовах.

6. Аналіз результатів досліджень та формулювання висновків: Систематичний аналіз зібраних даних та висновків, що визначають важливість та вплив різних телекомунікаційних протоколів у мережах Інтернет речей, їх ефективність та безпеку.

РОЗДІЛ 1
АНАЛІЗ ОБ'ЄКТА ДОСЛІДЖЕННЯ

1.1 Особливості мереж Інтернет речей

IoT (Internet of Things) або **Інтернет речей** – система фізичних об'єктів («речей»), взаємопов'язаних між собою за допомогою вбудованих датчиків, програмного забезпечення та/або інших технологій. Цей зв'язок потрібний для того, щоб передавати дані на інші пристрої в системі або в інші системи через Інтернет. Простіше кажучи, фізичні об'єкти виходять в Інтернет, щоб відправити інформацію чи прийняти її [1].

Інтернет речей відноситься до концепції, за якою фізичні пристрої, об'єкти та системи здатні підключатися до Інтернету та обмінюватися даними між собою без прямого взаємодії людей. Основною ідеєю *IoT* є забезпечення зв'язку та обміну інформацією між різними об'єктами, що відкриває безліч можливостей для автоматизації, контролю та оптимізації різних процесів.

Основні компоненти:

- **Пристрої та датчики**: фізичні об'єкти, які можуть бути підключені до мережі Інтернет, такі як смартфони, домашні пристрої, автомобілі, електронні пристрої зі вбудованими сенсорами (наприклад, термометри, рухові датчики тощо) або спеціально розроблені *IoT*-пристрої.
- **Мережеве з'єднання**: технології та протоколи, які забезпечують зв'язок між пристроями та датчиками, такі як *Wi-Fi, Bluetooth, ZigBee, Z-Wave,* або провідні з'єднання, такі як *Ethernet*.
- **Хмарні платформи**: забезпечують обробку, зберігання та аналіз даних, зібраних від пристроїв *IoT*. Вони надають можливість доступу до даних з будь-якого місця, віддалене керування пристроями та виконання аналітичних операцій для отримання цінної інформації.

- **Додаткове програмне забезпечення**: включає додатки, алгоритми та інструменти, що дозволяють аналізувати та використовувати дані, зібрані з пристроїв *IoT*.
- **Аплікації та сервіси**: різноманітні програмні додатки та сервіси, які використовують дані, зібрані з пристроїв *IoT*, можуть включати розумні додатки для домашнього автоматизації, системи моніторингу здоров'я, системи безпеки, енергоефективні рішення та інші.
-

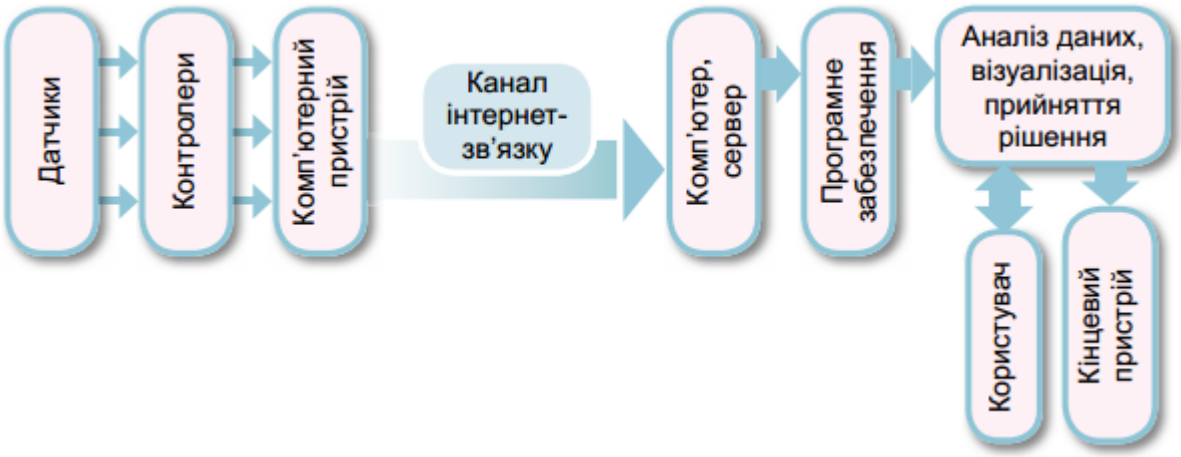

Рис. 1.1. Загальна схема функціонування мережі Інтернет речей

Фактично, Інтернет речей - це глобальна мережа різноманітних речей-приладів, які, за допомогою відповідної програми, здатні приймати рішення щодо різних дій без прямого участі людини [2] .

У цій мережі повинні брати участь різні типи датчиків (наприклад, ваги, вібрації, температури тощо), крім звичайних пристроїв, які ми використовуємо щодня (наприклад, конвеєрні стрічки, чайники, годинники, пилососи). Іншими словами, в цій мережі повинні бути пристрої, що зберігають зібрану інформацію, а також пристрої, що керують усіма цими процесами. Схематичне зображення пристроїв, які можуть бути підключені до мережі Інтернету речей, (рис.1.2):

Рис. 1.2. Пристрої Інтернету речей

Робота Інтернету речей базується на чотирьох основних етапах:

– Збір інформації з використанням датчиків;
– Передача отриманих даних від датчиків до хмарних сховищ;

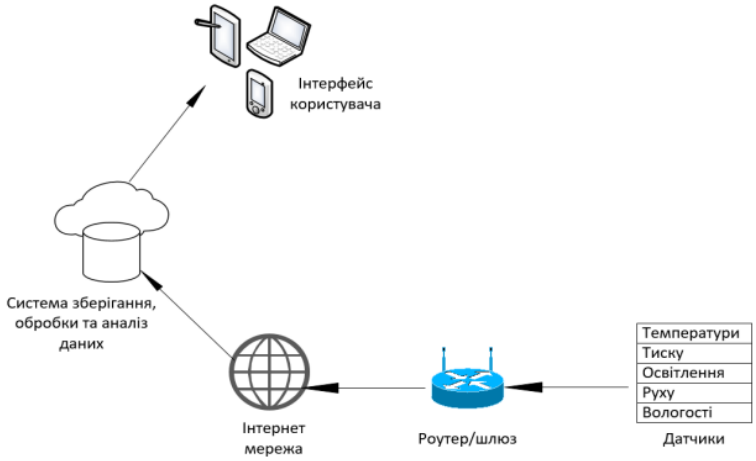

Рис. 1.3. Принцип роботи *IoT*

– Обробка зібраних даних, отриманих за допомогою датчиків;
– Передача обробленої інформації на інтерфейс користувача [3].

1.2 Основні телекомунікаційні протоколи

Телекомунікаційні протоколи відіграють ключову роль у мережах Інтернет речей, оскільки вони забезпечують комунікацію між різними пристроями та системами *IoT*.

Основні ролі телекомунікаційних протоколів в мережах Інтернет речей:

- Забезпечення зв'язку
- Управління мережею
- Синхронізація та координація
- Забезпечення безпеки
- Енергоефективність

Розглянемо основні телекомунікаційні протоколи, які широко використовуються в мережах Інтернет речей.

Bluetooth Low Energy (BLE)

Bluetooth є бездротовим протоколом для короткодійних з'єднань між пристроями. Він забезпечує надійну комунікацію в невеликому радіусі (зазвичай до 100 метрів).

В даний час існують два типи пристроїв з підтримкою *Bluetooth:*

Bluetooth Classic (BR/EDR), який використовується у бездротових динаміках, автомобільних системах розваг і навушниках;

Bluetooth Low Energy (BLE), тобто *Bluetooth* з низьким споживанням енергії, який з'явився у версії *Bluetooth* 4.0. Часто його застосовують у додатках, які чутливі до споживання енергії (наприклад, в пристроях з батарейним живленням) або у пристроях, що передають невеликий обсяг даних з великими інтервалами між передачами (наприклад, різноманітні датчики навколишнього середовища або бездротові перемикачі).

Ці два типи пристроїв несумісні один з одним, навіть якщо вони випущені під одним брендом чи специфікацією. Пристрої з підтримкою *Bluetooth Classic* не можуть безпосередньо з'єднуватися з пристроями, що використовують *BLE*. Тому деякі пристрої, такі як смартфони, підтримують обидва типи з'єднання (так звані

пристрої *Bluetooth Dual mode*), що дозволяє їм обмінюватися інформацією з обома типами пристроїв.

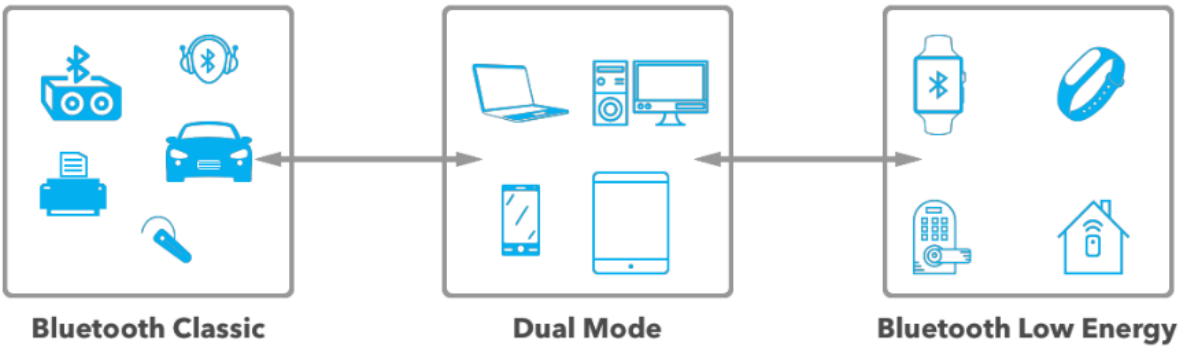

Рис. 1.4. Типи *Bluetooth*-пристроїв

Оскільки багато пристроїв Інтернету речей (*IoT*) використовують невеликі пристрої та датчики, *BLE* став найбільш поширеним протоколом зв'язку (порівняно з *Bluetooth Classic*) у додатках Інтернету речей.

Bluetooth Low Energy (BLE) є оптимізованою версією *Bluetooth*, яка споживає менше енергії та призначена для пристроїв з обмеженими ресурсами, таких як датчики, носимі пристрої та інші.

Wi-Fi* та *Wi-Fi Direct

WiFi Direct — це стандарт бездротової передачі даних, що особливо часто використовується на мобільних пристроях. В даний час цей стандарт є практично у всіх нових смартфонах і працює незалежно від моделі пристрою. *WiFi Direct* можна вважати наступником *Bluetooth* та конкурентом *AirDrop*. Передача даних відбувається за допомогою *WiFi* та може досягати швидкості до 250 Мбіт/с [4].

Wi-Fi є широко використовуваним бездротовим протоколом для мереж з великим радіусом дії та високою швидкістю передачі даних. *Wi-Fi Direct* дозволяє пристроям *IoT* безпосередньо підключатися один до одного без потреби в точці доступу *Wi-Fi*.

Стандарт прийшов на зміну більш повільному і складному з’єднанню під назвою *Bluetooth*. Він був здатний передавати дані на невеликій відстані і з відносно малою швидкістю.

Варто зауважити, що ввімкнення, використання і вимкнення бездротової мережі вай-фай відбувається набагато легше і швидше, ніж у попередника.

Налаштування дуже просте навіть для недосвідченого користувача. Набір цих факторів привів компанію *“Intel”* до впровадження першого подібного стандарту у вигляді платформи *Centrino* ще в 2008 році. Згодом застосування функції налагодили і багато інших виробників мережевого обладнання. Зараз підтримка *“ Wi-Fi Direct ”* доступна всім операційним системам, як *“Windows”*, так і *iOS* або *Android* [5].

Головною особливістю цієї функції є можливість обміну даними без використання точки доступу. Іншими словами, користувач отримує пряме підключення без посередницьких пристроїв. Робочий принцип схожий на *Ad-Hoc,* який також працює з прямими з'єднаннями, але має обмеження щодо швидкості до 11 Мегабіт на секунду.

ZigBee та Z-Wave:

ZigBee і Z-Wave є бездротовими мережевими протоколами, які використовуються в мережах Інтернет речей з низькою швидкістю передачі даних та низьким споживанням енергії.

ZigBee забезпечує мережеву топологію мережі з маршрутизацією та підтримує велику кількість пристроїв.

Z-Wave спеціалізується на домашніх автоматизаційних системах, забезпечуючи надійну комунікацію між пристроями в діапазоні до 100 метрів.

Як Z-Wave, так і *Zigbee* спрямовані на підключення в розумному домі. *Zigbee*, заснований на стандарті *IEEE*802.15.4, є більш гнучким і відкритим для розробки та налаштування специфічних програм. У порівнянні з *Zigbee, Z-Wave* дозволяє кожному вузлу спілкуватися з найближчими вузлами в діапазоні зв'язку, як прямо, так і опосередковано, завдяки бездротовій технології мережі типу "сітка". *3-Wave* є простішим за *Zigbee*, тому розробка на його основі ефективніша.

У відміну від *Wi-Fi*, де пристрої потребують підключення до *Wi-Fi* маршрутизатора, пристрої *Z-Wave* можуть бути підключені до мережі. Продукти *Z-Wave* все ж потребують центрального контролера для передачі даних до хмари, проте самі датчики та детектори не потребують *Wi-Fi*.

У порівнянні з *Z-Wave*, більшість *Bluetooth*-пристроїв не підтримують мережу типу "сітка" і не можуть бути підключені до різноманітних продуктів *Bluetooth* [6].

MQTT (Message Queuing Telemetry Transport)

MQTT є легковаговим протоколом повідомлень, спеціально розробленим для мереж Інтернет речей та сенсорних пристроїв. Він забезпечує надійну доставку повідомлень при низькому споживанні енергії та пропускній здатності.

Обмін повідомленнями в протоколі здійснюється між клієнтом (*client*), який може бути видавцем або передплатником (*publisher/subscriber*) повідомлень, та брокером (*broker*) повідомлень (наприклад, *Mosquitto MQTT*). Видавець відправляє дані на брокер, вказуючи в повідомленні певну тему (*topic*). Передплатники можуть отримувати різні дані від багатьох видавців залежно від підписки на відповідні теми. Учасник системи може взяти він роль видавця, передплатника чи обидві ролі відразу [7].

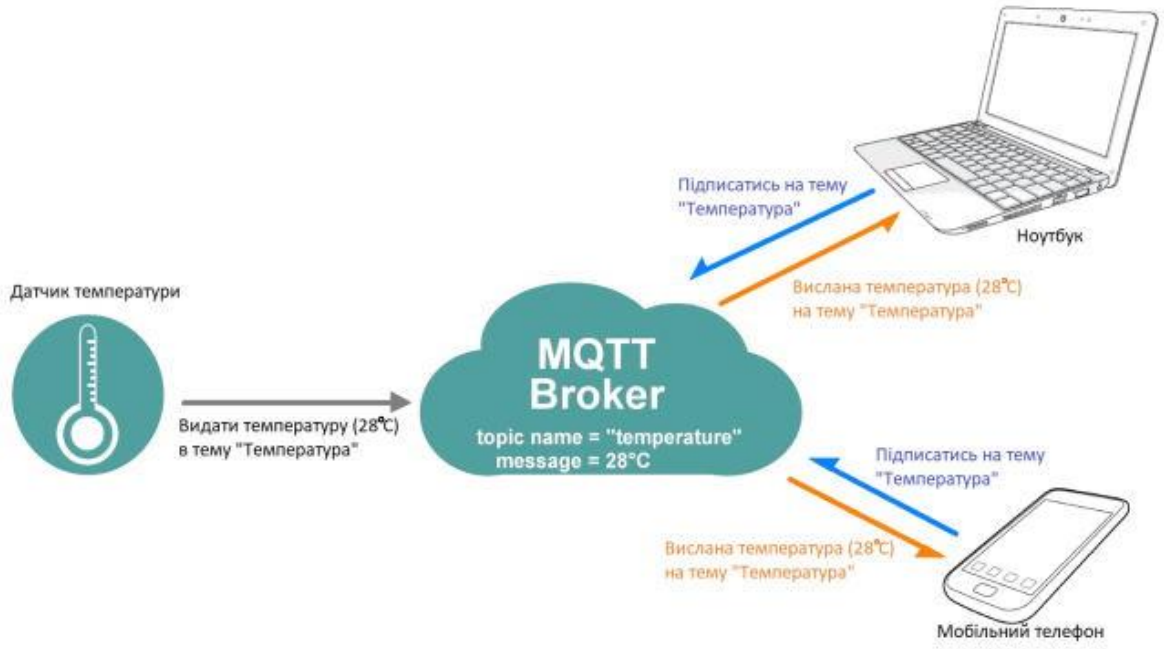

Рис. 1.5. Система зв’язку *MQTT*

Для взаємодії з брокером пристрої в протоколі використовують певні типи повідомлень, серед них:

– *Connect* – встановити з’єднання з брокером;
– *Disconnect* – розірвати з’єднання з брокером;
– *Publish* – опублікувати дані в топік на брокері;
– *Subscribe* – підписатися на топік на брокері;
– *Unsubscribe* – відписатися від топіка.

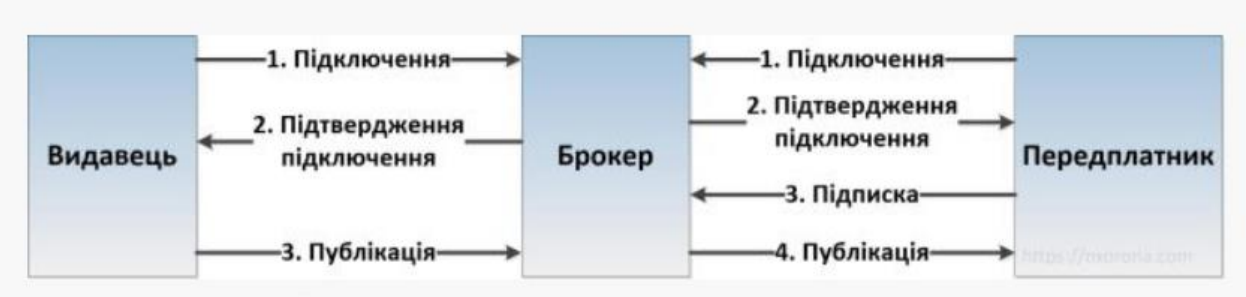

Рис. 1.6. Взаємодія з брокером

CoAP (Constrained Application Protocol)

CoAP є протоколом, розробленим для обміну даними в обмеженому середовищі, такому як мережі Інтернет речей. Він працює на базі протоколу *HTTP*, але з меншими вимогами до ресурсів.

Ось як функціонує *CoAP*:

1. Клієнт надсилає запит: Клієнт *CoAP* відправляє запит на сервер *CoAP* для доступу до ресурсу. Запит включає в себе метод *(GET, POST, PUT, DELETE), URI,* що ідентифікує ресурс, і будь-які додаткові параметри.

2. Сервер обробляє запит: Сервер *CoAP* отримує запит і обробляє його. Якщо запит дійсний, сервер генерує відповідь і відправляє його назад клієнтові. Якщо запит недійсний, сервер відправляє відповідь з помилкою.

3. Сервер відправляє відповідь: Сервер відправляє відповідь назад клієнтові. Відповідь містить код стану (наприклад, вміст 2.05, 4.04 Не знайдено), корисне навантаження (якщо застосовно) та будь-які додаткові параметри.

4. Клієнт одержує відповідь: Клієнт одержує відповідь від сервера і обробляє його. Якщо відповідь містить корисну навантаження, клієнт може використовувати ці дані для виконання бажаної операції [8].

HTTP (Hypertext Transfer Protocol)

HTTP є широко використовуваним протоколом для передачі даних в Інтернеті. В контексті мереж Інтернет речей він використовується для комунікації між пристроями та хмарними платформами.

HTTP протокол (*HyperText Transfer Protocol* «протокол передачі гіпертексту») – це протокол прикладного рівня гіпермедійних документів, таких як *HTML*. Протокол був розроблений для зв'язку між веб-браузерами і веб-серверами, але також використовується і для інших цілей. *HTTP* протокол використовується не тільки для передачі гіпертекстових документів, але і для передачі зображень та відео або для відправки контенту на сервери. Також *HTTP* використовується, щоб отримати частину документа для оновлення веб-сторінки за вимогою [9].

Рис. 1.7. Складові *HTTP*

1.3 Аналіз особливостей та переваг

Кожен з цих протоколів має свої переваги та обмеження і використовується залежно від вимог конкретної системи Інтернету речей. Обрання відповідного протоколу залежить від розміру мережі, вимог до швидкості передачі даних, енергоефективності, потреб у маршрутизації, топології мережі та інших факторів.

Стандартизація та сумісність з іншими пристроями

Bluetooth та *BLE*: *Bluetooth* є широко стандартизованим протоколом і майже всі сучасні смартфони, планшети та комп'ютери підтримують його. *BLE* також отримав широку підтримку та є сумісним з багатьма пристроями *IoT*.

Wi-Fi та *Wi-Fi Direct*: *Wi-Fi* є глобальним стандартом, і більшість пристроїв *IoT* можуть бути підключені до *Wi-Fi* мереж. *Wi-Fi Direct* зазвичай потребує спеціальної підтримки на пристроях для безпосереднього з'єднання.

ZigBee та *Z-Wave*: *ZigBee* та *Z-Wave* є стандартизованими протоколами, але їх підтримка може варіюватись серед пристроїв. Перед покупкою пристроїв потрібно переконатися, що вони сумісні з мережевим контролером або мережовим мостом.

MQTT, *CoAP* та *HTTP*: Ці протоколи є відкритими стандартами і мають реалізації для різних платформ. Вони можуть бути використані в широкому спектрі пристроїв *IoT*, але сумісність може варіюватись залежно від конкретної реалізації.

Захист даних та приватність користувачів

Bluetooth та *BLE*: *Bluetooth* має механізми шифрування та аутентифікації для захисту даних. *BLE* також надає можливості обмеження доступу до пристроїв.

Wi-Fi та *Wi-Fi Direct*: *Wi-Fi* має підтримку шифрування *WPA*2/*WPA*3, що забезпечує захист даних. Приватність може бути контрольована через механізми автентифікації та авторизації.

ZigBee та *Z-Wave*: Ці протоколи використовують шифрування та аутентифікацію для захисту даних передачі.

MQTT, *CoAP* та *HTTP*: Захист даних у цих протоколах залежить від використаної безпеки, такої як *TLS* (*Transport Layer Security*) або *SSL* (*Secure Sockets Layer*).

Вартість реалізації та розгортання

Bluetooth та *BLE: Bluetooth* має низькі витрати реалізації, а *BLE* забезпечує ще більшу економію ресурсів, що робить їх доступними для широкого кола пристроїв.

Wi-Fi та *Wi-Fi Direct: Wi-Fi* є досить доступним та встановленим протоколом, але вимагає більше ресурсів для реалізації та розгортання порівняно з іншими протоколами.

ZigBee та *Z-Wave*: Витрати на реалізацію і розгортання мережі *ZigBee* та *Z-Wave* можуть бути високими, оскільки вони вимагають спеціальних чіпів та контролерів.

MQTT, CoAP та HTTP: Ці протоколи мають високу вартість реалізації та розгортання, оскільки вони частіше використовуються у великих системах та потребують багато ресурсів.

Варто враховувати, що вартість реалізації та розгортання може варіюватись в залежності від розміру мережі, кількості пристроїв та особливостей вибраних протоколів.

Таблиця 1.1

Аналіз особливостей телекомунікаційні протоколів

Назва протоколу	Особливості		
	Пропускна здатність	Дальність	Енергоефективність
Bluetooth та *Bluetooth Low Energy* (*BLE*)	висока пропускну здатність для передачі даних, а *BLE* має низьку пропускну здатність, призначену для низькопотужних пристроїв.	має обмежену дальність передачі (до 100 метрів), а *BLE* зазвичай досягає 30 метрів	*BLE* споживає набагато менше енергії, що робить його популярним для датчиків та носимих пристроїв з обмеженими ресурсами
Wi-Fi та *Wi-Fi Direct*	висока пропускну здатність для швидкої передачі великого обсягу даних.	велика дальність дії (залежно від потужності точки доступу), але може бути обмеженою в мережах Інтернет речей через перешкоди	вимагає більше енергії порівняно з іншими протоколами, що може бути неоптимальним для пристроїв з обмеженими джерелами живлення

Продовження таблиці 1.1

Назва протоколу	Особливості		
	Пропускна здатність	Дальність	Енергоефективність
ZigBee та *Z-Wave*	помірна пропускну здатність, якої вистачає для передачі даних в мережах Інтернет речей	дальність передачі до 100 метрів, залежно від умов середовища та використання маршрутизації.	є енергоефективними протоколами, спеціально розробленими для пристроїв з низьким споживанням енергії
MQTT (*Message Queuing Telemetry Transport*)	Низька пропускна здатність, орієнтовану на ефективну передачу повідомлень в мережах Інтернет речей	Залежить від використовуваного протоколу транспорту (наприклад, *TCP*/*IP* або *UDP*).	*MQTT* може бути енергоефективним, оскільки його протоколи транспорту можуть бути оптимізовані для малопотужних пристрої
CoAP (*Constrained Application Protocol*):	помірна пропускна здатність, призначену для передачі обмеженої кількості даних в мережах Інтернет речей	залежить від використовуваного протоколу транспорту (наприклад, *UDP* або *SMS*)	спроектований для пристроїв з обмеженими ресурсами, що дозволяє досягти енергоефективності
HTTP (*Hypertext Transfer Protocol*):	висока пропускна здатність для передачі даних в Інтернеті.	залежить від доступності мережі Інтернет та точок доступу	може бути менш енергоефективним, оскільки вимагає додаткових ресурсів для передачі даних

1.4 Застосування телекомунікаційних протоколів

Застосування телекомунікаційних протоколів в різних сферах має значний вплив на розвиток технологій Інтернету речей. В кожній з нижче перелічених сфер використовуються різні протоколи, залежно від потреб та характеристик пристроїв та систем.

Смарт-хоми та розумні будинки:

Bluetooth та *Wi-Fi* використовуються для підключення різних пристроїв у домашній мережі, таких як освітлення, системи безпеки, термостати, розетки та інші.

ZigBee та *Z-Wave* широко використовуються для створення мережевої інфраструктури в розумних будинках, дозволяючи пристроям взаємодіяти між собою.

Здоров'я та медичні технології:

Bluetooth та *BLE* використовуються для підключення медичних пристроїв, таких як пульсометри, глюкометри, фітнес-трекери до мобільних пристроїв або облікових систем здоров'я.

MQTT та *CoAP* застосовуються для передачі даних в реальному часі з медичних датчиків до віддалених серверів або систем моніторингу.

Промисловість та автоматизація:

MQTT, *CoAP* та *HTTP* використовуються для збору даних з датчиків, контролю та керування у промислових системах.

ZigBee та *Z-Wave* застосовуються для створення бездротових мереж для моніторингу та керування промисловими пристроями.

Транспортні системи:

Wi-Fi та *Bluetooth* використовуються для забезпечення бездротового підключення в автомобілях, автобусах, поїздах та інших транспортних засобах.

MQTT та *CoAP* використовуються для передачі даних з сенсорів автомобілів, систем моніторингу та дистанційного керування транспортними системами.

Сільське господарство та "розумна" агротехнологія:

ZigBee та *Z-Wave* використовуються для створення мережевої інфраструктури для моніторингу ґрунту, вологості, рослин та автоматизації поливу.

MQTT та *CoAP* застосовуються для передачі даних зі сільськогосподарських датчиків до систем моніторингу та керування, щоб покращити врожайність та ефективність сільського господарства.

Висновки за розділом

Проведений аналіз особливостей мереж Інтернет речей показав, що такі мережі характеризуються великою кількістю різноманітних пристроїв, які можуть взаємодіяти та обмінюватися даними. Ці пристрої можуть мати обмежені ресурси, такі як потужність батареї, обчислювальні можливості та пам'ять, що вимагає використання ефективних та оптимізованих телекомунікаційних протоколів.

Вивчений огляд основних телекомунікаційних протоколів показав, що існує широкий спектр протоколів, які використовуються для забезпечення зв'язку і передачі даних у мережах Інтернет речей. Вони включають *MQTT, CoAP, Zigbee, Z-Wave, Bluetooth, LoRaWAN* та *NB-IoT*, кожен з яких має свої унікальні характеристики та специфікації.

Детальний аналіз особливостей та переваг кожного протоколу дав змогу з'ясувати, що кожен з них має свої сильні сторони та обмеження. Наприклад, *MQTT* є легким та ефективним для обміну повідомленнями, *CoAP* забезпечує можливість взаємодії з ресурсами пристроїв за допомогою *RESTful*, *Zigbee* та *Z-Wave* забезпечують низьке споживання енергії, а *LoRaWAN* має великий радіус покриття. Вибір протоколу залежить від конкретних вимог і характеристик проекту.

Висвітлений огляд застосування телекомунікаційних протоколів в різних сферах, таких як розумні будинки, промисловість, здоров'я та інші, показав їх широкий потенціал. Кожен протокол має свої переваги в певних застосуваннях, і вибір оптимального протоколу допоможе забезпечити ефективне та стабільне функціонування мереж Інтернет речей у різних сценаріях.

Узагальнюючи результати аналізу, ми розуміємо, що вибір телекомунікаційного протоколу є важливим кроком при проектуванні та розробці мереж Інтернет речей. Кожен протокол має свої переваги та обмеження, які необхідно враховувати при плануванні та реалізації проекту.

РОЗДІЛ 2
ДЕТАЛЬНИЙ ОГЛЯД ТЕЛЕКОМУНІКАЦІЙНИХ ПРОТОКОЛІВ

2.1. Протоколи зв'язку між пристроями

Протоколи зв'язку між пристроями в мережах Інтернет речей (IP) відіграють важливу роль у забезпеченні безперервного та ефективного обміну даними між різними пристроями, які належать до цієї мережі. Ці протоколи враховують особливості обмежених ресурсів, таких як обмежена пропускна здатність, енергоспоживання та обчислювальні можливості пристроїв, що працюють у мережі IP. Дозволяють забезпечити безпечну та надійну комунікацію, а також гарантують сумісність між різними пристроями.

***MQTT* (*Message Queuing Telemetry Transport*)** є легким, простим у використанні та масштабованим протоколом передачі повідомлень, спеціально розробленим для обміну даними в умовах обмежених ресурсів мереж Інтернет речей (IP). Він став популярним в мережах IP завдяки своїй ефективності, низькому споживанню енергії та здатності працювати при обмеженій пропускній здатності.

Основним принципом *MQTT* є модель публікації-підписки (*publish-subscribe*), де пристрої можуть публікувати повідомлення на тематичні канали (топіки), а інші пристрої можуть підписатися на ці канали для отримання повідомлень. Це дозволяє ефективно організувати спілкування між пристроями без необхідності встановлення прямого з'єднання між ними.

Однією з головних переваг *MQTT* є його легкість і простота використання.

Іншою важливою перевагою *MQTT* є його масштабованість. Він може працювати як в малому, локальному розподіленому середовищі, так і великій глобальній мережі. *MQTT* забезпечує надійну доставку повідомлень, дозволяє розподіляти навантаження та може масштабуватися від кількох пристроїв до тисяч і навіть мільйонів.

Крім того, *MQTT* підтримує різні рівні якості обслуговування (*Quality of Service - QoS*), що дозволяє контролювати надійність та доставку повідомлень.

***CoAP* (*Constrained Application Protocol*)** є легким та ефективним протоколом, спеціально розробленим для обмежених пристроїв та мереж Інтернет речей (IP). Він використовує *RESTful* (*Representational State Transfer*) підхід для взаємодії з пристроями та надає можливість виконання операцій зчитування, запису та видалення ресурсів.

Однією з ключових особливостей *CoAP* є його легкість та простота використання. Він має малу вагу та низький рівень накладних витрат, що дозволяє ефективно використовувати обмежені ресурси пристроїв, такі як обсяг пам'яті та пропускна здатність. Це особливо важливо в мережах IP, де пристрої можуть мати обмежені обчислювальні та енергетичні можливості.

CoAP використовує *RESTful* архітектуру, яка базується на принципах веб-сервісів. Це означає, що він використовує стандартні *HTTP*-подібні методи, такі як *GET*, *POST*, *PUT* та *DELETE*, для взаємодії з ресурсами пристроїв. Протокол дозволяє клієнтам зчитувати стан ресурсів, змінювати їх та виконувати дії, пов'язані з ресурсами.

Одна з ключових особливостей *CoAP* - це підтримка механізму низькорівневої надійності зв'язку. Протокол надає рівні якості обслуговування (*QoS*) для керування доставкою повідомлень, забезпечуючи надійну комунікацію в умовах незадовільної або змінної якості зв'язку. Це дозволяє гарантувати доставку повідомлень в обмежених мережах IP, де сполучення можуть бути ненадійними або недоступними.

Zigbee є стандартним протоколом мережі низької споживання енергії (*Low-Power*, *Low-Rate WPAN*), який спеціально розроблений для мереж Інтернет речей (IP). Він використовує бездротові технології на радіочастоті для забезпечення низького споживання енергії, широкого покриття та міжоператорської сумісності.

Однією з головних переваг *Zigbee* є його низьке споживання енергії. Протокол оптимізований для праці на батарейно-живлених пристроях, що дозволяє їм працювати на протязі довгого часу без необхідності постійної заміни або заряджання батарей. Це особливо важливо в контексті мереж IP, де пристрої можуть бути розташовані віддалено або важкодоступних місцях.

Зігбі також забезпечує широке покриття, що робить його ідеальним протоколом для мереж *IP*. Завдяки використанню радіочастотних технологій, *Zigbee* може працювати в різних проміжках частот, що дозволяє забезпечити надійне покриття приміщень або навіть великих територій. Це дозволяє створювати масштабовані мережі IP, які можуть включати в себе велику кількість пристроїв.

Ще одною перевагою *Zigbee* є його міжоператорська сумісність. Протокол стандартизований і підтримується різними виробниками, що дозволяє створювати мережі *IP* з пристроями від різних вендорів. Це робить *Zigbee* універсальним і зручним варіантом для інтеграції різних типів пристроїв в єдину мережу.

Зігбі дозволяє побудувати надійні та енергоефективні мережі *IP*, особливо в контексті додатків у розумних будинках та промисловості. У розумних будинках.

Bluetooth Low Energy (BLE) є протоколом зв'язку, спеціально розробленим для низькопотужних пристроїв з обмеженими ресурсами, включаючи мережі Інтернет речей (*IP*). Він використовується для передачі даних з низьким споживанням енергії, має невеликий радіус дії та підтримує широкий спектр додаткових сервісів, що робить його досить розповсюдженим у різних додатках *IP*.

Однією з ключових переваг *BLE* є його низьке споживання енергії. Протокол оптимізований для роботи на пристроях з обмеженими джерелами живлення, таких як сенсори, носимі пристрої та інші малий станції. Це дозволяє пристроям працювати на батарейках протягом тривалого періоду без необхідності їх постійної заміни або заряджання. Благодаря низькому споживанню енергії *BLE* став популярним протоколом для розумних пристроїв, особливо в галузях здоров'я та фітнесу, де пристрої постійно взаємодіють з користувачем і передають його біометричні дані.

Ще однією перевагою *BLE* є його невеликий радіус дії. Це означає, що пристрої можуть встановлювати бездротове з'єднання на невеликій відстані, що підтримує мобільність і гнучкість використання. Наприклад, це дозволяє розумним годинникам або фітнес-браслетам підключатися до смартфона чи планшета користувача, а також забезпечує точність і надійність передачі даних в обмеженому просторі.

Thread є відкритим стандартом для мереж Інтернет речей, який забезпечує надійний та енергоефективний зв'язок між пристроями. Він базується на мережевому стеку *IPv6*, що дозволяє кожному пристрою мати унікальну *IP*-адресу та забезпечує прямий доступ до Інтернету. *Thread* використовує механізм маршрутизації, що дозволяє побудувати стабільне з'єднання з мережею, навіть при зміні топології або додаванні нових пристроїв.

Однією з ключових переваг *Thread* є його масштабованість. Протокол дозволяє побудувати мережу Інтернет речей, яка може включати в себе велику кількість пристроїв. Кожен пристрій може бути як маршрутизатором, так і кінцевим пристроєм, що дозволяє передавати дані через декілька проміжних вузлів, забезпечуючи надійну доставку і збільшуючи покриття мережі.

Безпека є ще однією важливою характеристикою *Thread*. Протокол надає захист від несанкціонованого доступу та забезпечує шифрування даних, що передаються в мережі. Крім того, *Thread* має вбудовані механізми аутентифікації та авторизації, що дозволяють контролювати доступ до пристроїв та ресурсів мережі.

Thread також надає енергоефективність, що є критично важливим фактором для батарейно-живлених пристроїв. Протокол оптимізований для роботи в умовах обмежених ресурсів, забезпечуючи мінімальне споживання енергії пристроями.

Ці протоколи представляють лише деякі з численних варіантів протоколів зв'язку між пристроями, які використовуються у мережах IP. Вибір протоколу залежить від вимог конкретного застосування, таких як обсяг передаваних даних, вимоги до енергоспоживання, масштабованість та безпека.

2.2. Протоколи з'єднання з мережею

Протоколи з'єднання з мережею є важливою складовою інфраструктури Інтернету речей, які забезпечують зв'язок та взаємодію між пристроями, дозволяючи передавати дані та керувати пристроями. У мережах Інтернет речей використовуються різні протоколи з'єднання, кожен з яких має свої особливості, переваги та обмеження.

***Wi-Fi* (*Wireless Fidelity*)** є одним з найпопулярніших бездротових протоколів з'єднання, який широко використовується для передачі даних у безпроводових мережах. Він забезпечує високу швидкість передачі даних, широкий охоплення та зручність встановлення з'єднання, що робить його ідеальним в домашніх мережах Інтернет речей, офісних середовищах та громадських місцях.

Основна перевага *Wi-Fi* полягає в бездротовому з'єднанні, що дозволяє пристроям підключатися до мережі без необхідності фізичних кабелів. Це дозволяє зручно розташовувати та переміщувати пристрої в межах покритої зоны, забезпечуючи гнучкість і зручність використання.

Wi-Fi працює на різних частотах, таких як 2,4 ГГц та 5 ГГц, що дозволяє використовувати різні канали для передачі даних. Це дозволяє зменшити перешкоди та інтерференцію, що можуть впливати на якість з'єднання.

Щодо швидкості передачі даних, *Wi-Fi* забезпечує високу пропускну здатність, що дозволяє передавати великі обсяги інформації. Наприклад, *Wi-Fi* стандарту 802.11*ac* (також відомий як *Wi-Fi* 5) може досягати швидкості до 1 Гбіт/с, тоді як останній стандарт 802.11*ax* (*Wi-Fi* 6) підтримує ще більшу швидкість передачі даних.

Широкий охоплення є ще однією важливою перевагою *Wi-Fi*. Залежно від мережевих налаштувань та використаного обладнання, *Wi-Fi* може покривати значну площу, дозволяючи пристроям знаходитися на відносно великій відстані від маршрутизатора чи точки доступу і все ж отримувати стабільне з'єднання.

Wi-Fi також має різні режими роботи, включаючи інфраструктурний режим, де пристрої підключаються до центрального маршрутизатора або точки доступу, та безпроводовий режим "ад-хок", де пристрої можуть підключатися один до одного без проміжного обладнання.

Забезпечення безпеки є ще одним важливим аспектом *Wi-Fi*. Для захисту передачі даних через *Wi-Fi* використовуються різні методи шифрування, такі як *WPA* (*Wi-Fi Protected Access*) та *WPA*2. Це дозволяє забезпечити конфіденційність та недоступність даних для несанкціонованого доступу.

Ethernet є провідним протоколом з'єднання, який широко використовується для передачі даних по кабелях у мережах Інтернет речей. Він надає стабільне, надійне та швидке з'єднання, що робить його популярним у промислових системах, офісних середовищах та мережах передачі даних.

Основна перевага *Ethernet* полягає в його надійності та стабільності з'єднання. Провідне з'єднання дозволяє уникнути проблем, пов'язаних з бездротовим зв'язком, такими як інтерференція, втрати сигналу або незадовільна якість з'єднання, що можуть впливати на передачу даних. *Ethernet* забезпечує стабільний потік даних та мінімальну втрату пакетів, що робить його ідеальним для завдань, де надійність є критичною, наприклад, у промислових автоматизованих системах або важливих мережах передачі даних.

Щодо швидкості передачі даних, *Ethernet* забезпечує велику пропускну здатність, що дозволяє передавати значні обсяги інформації з високою швидкістю. Стандартні варіанти *Ethernet*, такі як 100*BASE-TX* і 1000*BASE-T*, підтримують швидкості передачі даних до 100 Мбіт/с і 1 Гбіт/с відповідно. Останні розширення, такі як 10*GBASE-T*, навіть дозволяють досягати швидкостей до 10 Гбіт/с. Це дозволяє ефективно передавати великі обсяги даних, такі як відео, аудіо або великі файли, що є важливим для багатьох застосувань Інтернету речей, включаючи відеоспостереження, потокову передачу медіа або обробку великих обсягів даних.

Ethernet також є дуже гнучким протоколом з'єднання, оскільки його можна використовувати як в малих локальних мережах (*LAN*), так і в більших об'єднаних мережах (*WAN*) з використанням різних технологій передачі даних, наприклад, *Ethernet over Fiber* або *Ethernet over Coaxial Cable*.

Bluetooth є бездротовим протоколом з'єднання короткого діапазону, який використовується для забезпечення з'єднання та обміну даними між близько розташованими пристроями. Він широко використовується в різних персональних пристроях, таких як розумні годинники, навушники, клавіатури, миші, динаміки та інші пристрої, що дозволяють користувачам зручно з'єднувати та обмінюватися даними між ними.

Одна з ключових переваг *Bluetooth* полягає в його бездротовому характері. Він дозволяє підключати пристрої один до одного без необхідності використовувати фізичні кабелі. Це робить *Bluetooth* зручним для використання, оскільки користувачі можуть безпосередньо з'єднувати свої пристрої без зайвих зусиль.

Bluetooth має обмежений діапазон дії, який зазвичай становить до 10 метрів. Це означає, що пристрої повинні бути в непосредственной близкості один до одного для забезпечення стабільного з'єднання. Однак, існує ряд новіших версій *Bluetooth*, таких як *Bluetooth* 5, які можуть забезпечувати більшу відстань з'єднання та покращену стабільність сигналу.

Щодо швидкості передачі даних, *Bluetooth* забезпечує високу пропускну здатність, що дозволяє передавати різноманітні типи даних, включаючи аудіо, відео, фотографії та інші медіа. Новіші версії *Bluetooth* можуть досягати високої швидкості передачі даних, такої як *Bluetooth* 5 з максимальною швидкістю до 2 Мбіт/с. Це дозволяє користувачам швидко обмінюватися файлами та стрімити медіа на віддалені пристрої.

Одна з особливостей *Bluetooth* є його спроможність підтримувати різні профілі та служби, які визначають специфічні можливості пристрою. Наприклад, існують профілі для бездротового передавання аудіо (*A2DP*), гарнітури та гарнітури (*HFP*), передачі файлів (*OPP*), керування презентацією (*HID*) та багато інших. Це робить *Bluetooth* універсальним протоколом для різних типів пристроїв та застосувань.

Z-Wave є протоколом мережі з низьким споживанням енергії, який використовується для забезпечення зв'язку між різними розумними пристроями. Цей протокол знаходить широке застосування в домашніх системах автоматизації, безпеки та контролю, де потрібно надійне та безпечне з'єднання.

Однією з ключових переваг *Z-Wave* є його низьке споживання енергії. Це дозволяє пристроям, підключеним до *Z-Wave* мережі, працювати на батареї або інших джерелах живлення протягом тривалого часу без необхідності частої заміни або заряджання. Це особливо важливо для розумних домашніх систем, де багато пристроїв працюють постійно і мають бути доступними в будь-який момент.

Надійність є ще однією перевагою *Z-Wave*. Цей протокол використовує механізми повторювачів сигналу, що забезпечують широкий охоплення та стабільність зв'язку. Якщо один пристрій не може безпосередньо спілкуватися з контролером, існують інші пристрої, які можуть служити повторювачами сигналу і передавати команди до віддалених пристроїв. Це дозволяє створювати великі мережі з високою надійністю та масштабованістю.

Захист від несанкціонованого доступу є ще однією важливою характеристикою *Z-Wave*. Цей протокол використовує шифрування та аутентифікацію для захисту передачі даних між пристроями. Це дозволяє забезпечити конфіденційність і цілісність даних, а також запобігти несанкціонованому доступу до системи. З-*Wave* протокол використовує спеціальні ключі для ідентифікації пристроїв та забезпечення безпеки комунікації.

Ще одною перевагою *Z-Wave* є його велика сумісність з різними пристроями. Цей протокол стандартизований і підтримується широким спектром виробників. Це означає, що ви можете використовувати пристрої різних брендів, які підтримують *Z-Wave*, і вони зможуть взаємодіяти між собою. Це забезпечує великий вибір пристроїв та можливість розширення вашої системи без обмежень.

***LoRaWAN* (*Long Range Wide Area Network*)** є протоколом мережі широкого охоплення та довгого діапазону, призначеним для передачі даних в мережах Інтернет речей. Він базується на технології *LoRa* (*Long Range*), яка дозволяє передавати дані на великі відстані з використанням низької потужності.

Однією з ключових переваг *LoRaWAN* є його великий радіус покриття. Завдяки використанню низької частоти, *LoRaWAN* може передавати дані на значно більшу відстань порівняно з іншими бездротовими протоколами, такими як *Wi-Fi* або *Bluetooth*. Це дозволяє створювати мережі, які покривають великі території, такі як міста, сільські райони або промислові комплекси, зменшуючи витрати на розгортання та підтримку інфраструктури.

Низьке споживання енергії є ще однією перевагою *LoRaWAN*. Протокол оптимізований для використання в батарейно-живлених пристроях, що дозволяє їм працювати протягом довгого часу без необхідності заряджання або заміни батарей.

Технологія *LoRa* дозволяє пристроям входити в режим сну, споживаючи дуже малу потужність, і переходити в активний режим тільки для передачі або прийому даних. Це особливо важливо для застосувань, де пристрої розташовані в важкодоступних або віддалених місцях.

Захист від несанкціонованого доступу є ще однією важливою характеристикою *LoRaWAN*. Протокол використовує шифрування та аутентифікацію для захисту передачі даних, що забезпечує конфіденційність і цілісність даних.

***NB-IoT* (*Narrowband Internet of Things*)** є стандартом мережі передачі даних з низьким потужністю передавального каналу (*LPWA*), який розроблений спеціально для підключення малопотужних пристроїв до мереж Інтернет речей. Використовуючи існуючу інфраструктуру мобільного зв'язку, *NB-IoT* забезпечує широкий охоплення, глибоку проникність сигналу та довгий термін служби батареї, що робить його популярним в моніторингових системах, громадському здоров'ї та багатьох інших додатках Інтернету речей.

Однією з ключових переваг *NB-IoT* є його широкий охоплення. Використовуючи смужку зв'язку з низькими частотами, *NB-IoT* може забезпечити сильний сигнал навіть в труднодоступних місцях, таких як глибоко розташовані підземні приміщення або товсті стіни будівель.

Другою важливою характеристикою *NB-IoT* є його глибока проникність сигналу. Сигнал *NB-IoT* може проникати через перешкоди, такі як стіни будівель або розташовані глибоко під землею інфраструктури. Це робить його ідеальним вибором для застосувань, де пристрої розташовані у важкодоступних або затінених місцях, наприклад, вентиляційні системи, лічильники енергії або системи моніторингу середовища.

Третьою перевагою *NB-IoT* є його довгий термін служби батареї. Протокол оптимізований для низького споживання енергії, що дозволяє пристроям працювати на одній батареї протягом тривалого періоду часу.

NB-IoT також забезпечує безпеку передачі даних. Використовуючи шифрування та аутентифікацію, протокол забезпечує конфіденційність та цілісність даних, переданих між пристроями та мережевою інфраструктурою.

Отже, протоколи з'єднання з мережею є важливим елементом Інтернету речей, оскільки вони дозволяють пристроям взаємодіяти з мережею та іншими пристроями. Вибір конкретного протоколу залежить від вимог до швидкості, споживання енергії, покриття та інших факторів.

2.3. Протоколи керування мережею

Протоколи керування мережею в мережах Інтернет речей (*IoT*) відповідають за управління та контроль над мережевими ресурсами, конфігурацію пристроїв, керування комунікаційними потоками та забезпечення надійності мережі. Вони забезпечують ефективну та оптимальну роботу мережі Інтернет речей, здатну виконувати потреби різноманітних застосувань. Деякі з найпоширеніших протоколів керування мережею включають такі:

6*LoWPAN* (*IPv*6 *over Low-Power Wireless Personal Area Networks*) є протоколом, який дозволяє підключати малопотужні пристрої до мереж Інтернет речей, використовуючи стек протоколів *IPv*6. Його основною метою є забезпечення сполучення та комунікації між малопотужними пристроями, такими як сенсори, монітори, актуатори та інші, через обмежені бездротові мережі, такі як *Zigbee, Bluetooth Low Energy* (*BLE*) або *IEEE* 802.15.4.

Одна з ключових особливостей 6*LoWPAN* полягає у здатності пристроїв до перетворення та стиснення *IPv*6-пакетів для передачі через обмежені мережеві технології. Оскільки малопотужні пристрої зазвичай мають обмежені ресурси, включаючи обчислювальну потужність, енергію та пам'ять, важливо ефективно використовувати ці ресурси при передачі даних. 6*LoWPAN* дозволяє зменшити розмір *IPv*6-пакетів шляхом стиснення заголовків та використання більш ефективного представлення даних. Це дозволяє зменшити навантаження на мережу та забезпечити більш ефективне використання бездротового каналу.

Ще однією важливою особливістю 6*LoWPAN* є підтримка *IPv*6. Це означає, що кожен малопотужний пристрій може мати унікальну *IP*-адресу, що спрощує ідентифікацію та комунікацію з ним.

6*LoWPAN* також забезпечує механізми маршрутизації та керування мережею. Протокол підтримує маршрутизацію на рівні мережі та мережевого рівня, що дозволяє побудувати оптимальні маршрути для передачі даних у мережі з обмеженими ресурсами.

***RPL* (*Routing Protocol for Low-Power and Lossy Networks*)** є протоколом маршрутизації, спеціально розробленим для мереж Інтернет речей (*IoT*) з обмеженими ресурсами. Він вирішує проблеми передачі даних в мережах з низькою пропускною здатністю, високою затримкою та непостійною доступністю зв'язку, які є характерними для мереж *IoT* з малопотужними пристроями, такими як сенсори, актуатори, розумні розетки та інші.

Однією з ключових особливостей *RPL* є його здатність вибирати оптимальні маршрути для передачі даних в мережі. Враховуючи обмежені ресурси малопотужних пристроїв, *RPL* використовує децентралізований підхід до маршрутизації, що означає, що прийняття рішення про маршрутизацію відбувається на самому пристрої.

RPL також надає механізми для керування топологією мережі. Він дозволяє пристроям динамічно оновлювати та підтримувати інформацію про мережу, зокрема про доступність сусідніх пристроїв та зміни топології. Це важливо в мережах *IoT*, де пристрої можуть бути мобільними або вимикатися з мережі, що може впливати на доступність маршрутів. *RPL* розроблений таким чином, щоб динамічно адаптуватися до змін у мережі, підтримуючи надійну та ефективну комунікацію між пристроями.

***CoAP* (*Constrained Application Protocol*)** є протоколом керування мережею, який надає зручний механізм взаємодії з пристроями та можливість зчитування, запису та видалення ресурсів у мережах Інтернет речей (*IoT*). Його основна мета полягає в тому, щоб забезпечити ефективну комунікацію між обмеженими

пристроями з низькими ресурсами, такими як сенсори або малопотужні мікроконтролери, та іншими пристроями або серверами.

CoAP використовує архітектуру *RESTful* (*Representational State Transfer*), що дозволяє пристроям взаємодіяти з ресурсами у мережі за допомогою стандартних *HTTP*-подібних методів, таких як *GET*, *POST*, *PUT* та *DELETE*. Це дозволяє зчитувати стан пристроїв, виконувати команди, змінювати параметри та отримувати відповіді на запити. *CoAP* дуже легкий та ефективний, оскільки він мінімізує розмір пакетів даних та використовує *UDP* для передачі даних, що дозволяє економити пропускну здатність та ресурси мережі.

Однією з особливостей *CoAP* є його простота використання та налаштування. Цей протокол легко інтегрується з різноманітними мережевими технологіями, такими як *Ethernet, Wi-Fi, Zigbee*, а також забезпечує взаємодію з різними платформами та пристроями. *CoAP* також підтримує механізми безпеки, такі як *DTLS* (*Datagram Transport Layer Security*), що дозволяють захистити передачу даних в мережі від несанкціонованого доступу та забезпечити конфіденційність і цілісність інформації.

Протокол *CoAP* широко використовується у різних сферах застосування *IoT*, зокрема в галузях, які вимагають обміну даними з обмеженими ресурсами, таких як моніторинг середовища, управління енергоефективними системами, автоматизовані будинки, розумні міста та інші.

***OMA DM* (*Open Mobile Alliance Device Management*)** є протоколом керування пристроями, розробленим для віддаленого управління пристроями Інтернет речей (*IoT*). Він надає набір стандартів та протоколів для ефективного керування пристроями, незалежно від їх типу та виробника.

OMA DM дозволяє виконувати різноманітні функції керування пристроями, зокрема керування конфігурацією, оновлення програмного забезпечення, збір статистики, моніторинг, діагностику та багато інших. Він дозволяє віддалено налаштовувати та керувати параметрами пристроїв, встановлювати та оновлювати програмне забезпечення, виконувати перевірку статусу пристроїв та відправляти команди віддаленого управління.

Один з ключових принципів *OMA DM* - це спрощення та стандартизація процесу керування пристроями. Використовуючи *OMA DM*, різні типи пристроїв можуть спілкуватися з управляючою платформою за допомогою спільних інтерфейсів та протоколів.

OMA DM також забезпечує механізми безпеки для захисту передачі даних між пристроями та управляючою платформою. Це включає аутентифікацію, шифрування та захист від несанкціонованого доступу.

OMA DM широко використовується в різних сферах застосування *IoT*, таких як автоматизовані системи, моніторинг промислових процесів, телематика, управління флотом транспорту та багато інших. Він дозволяє операторам та розробникам забезпечити ефективне управління великою кількістю пристроїв, знизити витрати на обслуговування та забезпечити безпеку та надійність роботи мереж Інтернет речей.

***TR*-069 (*Technical Report* 069),** відомий також як *CPE WAN Management Protocol* (*CWMP*), є протоколом керування мережею, розробленим для управління та налагодження мережевого обладнання в домашніх мережах і невеликих підприємствах. Цей протокол встановлює стандартні методи і процедури для взаємодії з мережевими пристроями, такими як маршрутизатори, маршрутизатори *Wi-Fi*, комутатори та інші обладнання, що використовується для підключення до Інтернету.

TR-069 дозволяє віддалено керувати та конфігурувати мережеве обладнання безпосередньо з централізованої управляючої платформи, яка може бути розташована в провайдерському центрі або в іншому віддаленому місці. Використовуючи *TR*-069, провайдери послуг або системні адміністратори можуть віддалено налаштовувати параметри мережевого обладнання, виконувати оновлення програмного забезпечення, контролювати його роботу та отримувати статистику про стан мережі.

Однією з ключових особливостей *TR*-069 є його здатність автоматично встановлювати зв'язок між управляючою платформою і мережевими пристроями. Протокол використовує механізм *Auto-Configuration Server* (*ACS*), який ініціює

взаємодію з пристроями та керує процесом налаштування та моніторингу. *TR*-069 використовує *HTTP* або *HTTPS* як транспортний протокол для передачі даних між управляючою платформою та мережевими пристроями.

Протокол *TR*-069 також включає механізми безпеки, що дозволяють захистити передачу даних та забезпечити автентифікацію між управляючою платформою та пристроями. Це гарантує конфіденційність та цілісність даних, а також запобігає несанкціонованому доступу до мережевого обладнання.

TR-069 є широко використовуваним стандартом у провайдерській індустрії для керування мережевим обладнанням, зокрема в постачальників інтернет-послуг, операторів мобільного зв'язку та постачальників послуг зв'язку.

Ці протоколи керування мережею допомагають управляти мережевими ресурсами, забезпечувати надійну передачу даних, виконувати налаштування та моніторинг пристроїв у мережі Інтернет речей. Кожен з них має свої особливості та застосування, і вибір протоколу залежить від конкретних потреб та вимог вашого застосування *IoT*.

Висновки за розділом

Детальний огляд протоколів зв'язку між пристроями показав, що існує широкий спектр протоколів, які використовуються для передачі повідомлень і даних між пристроями в мережах Інтернет речей. *MQTT* є ефективним та легким протоколом публікації-підписки, який ідеально підходить для обміну даними в обмежених умовах мереж IP. *CoAP* забезпечує можливість взаємодії з ресурсами пристроїв за допомогою *RESTful* і є ідеальним для обмежених пристроїв і мереж IP. *Zigbee* та *Z-Wave*, як стандарти мереж низької споживання енергії, використовуються в розумних будинках та промислових системах. *Bluetooth* та *LoRaWAN* використовуються для короткодіапазонного та довгодального зв'язку відповідно, а *NB-IoT* є стандартом для мереж інтернет речей з низькою потужністю.

Огляд протоколів з'єднання з мережею показав, що *Wi-Fi, Ethernet, Bluetooth* та *Zigbee* є популярними протоколами, які забезпечують з'єднання між пристроями і мережами IP. *Wi-Fi* є широко використовуваним бездротовим протоколом з високою швидкістю передачі даних для домашніх мереж та офісних середовищ. *Ethernet* забезпечує надійне з'єднання по проводам і широко використовується в промислових системах та офісних мережах. *Bluetooth* є популярним для з'єднання близькорозташованих пристроїв, таких як навушники та розумні годинники. *Zigbee* забезпечує низькопотужне і надійне з'єднання для розумних будинків та індустріальних застосувань.

Детальний огляд протоколів керування мережею показав, що 6*LoWPAN* та *RPL* дозволяють підключати малопотужні пристрої до мереж Інтернет речей та забезпечують оптимальний механізм маршрутизації. *OMA DM* та *TR*-069 є протоколами для віддаленого управління та конфігурації пристроїв *IoT* у мережах. Враховуючи специфіку проекту, вибір певного протоколу керування мережею допоможе забезпечити ефективне та безперебійне функціонування мережі *IoT*.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ ПРОТОКОЛІВ В МЕРЕЖАХ ІНТЕРНЕТ РЕЧЕЙ

3.1 Методи оцінки ефективності протоколів

Для вимірювання споживання енергії ми плануємо використовувати спеціальні засоби та обладнання, призначені для точного вимірювання енергії, що споживається пристроями під час передачі даних в мережі Інтернет речей. Ці засоби дозволяють отримати детальні показники енергоспоживання та аналізувати його вплив на тривалість роботи батарейних пристроїв.

Експерименти будуть проведені в різних умовах, включаючи різні відстані між пристроями, різні швидкості передачі даних та різний обсяг передаваних повідомлень. Також будуть враховані різні типи даних, що передаються, наприклад, текстові повідомлення, зображення або сенсорні дані.

Під час експериментів будуть виміряні та збережені дані про споживання енергії для кожного протоколу та умови передачі даних. Далі будуть проведені аналіз та порівняння результатів для визначення найбільш енергоефективного протоколу в різних сценаріях використання.

Це дослідження дозволить нам зрозуміти, який протокол забезпечує кращу енергоефективність та має найменший вплив на ресурси батарейних пристроїв. Отримані результати стануть підґрунтям для обґрунтованого вибору оптимального телекомунікаційного протоколу для певних типів застосувань в мережах Інтернет речей.

Для досягнення точних результатів дослідження, ми будемо проводити кілька повторних вимірювань для кожного протоколу та умови передачі даних. Це дозволить зменшити вплив випадкових помилок та забезпечить достовірність наших висновків.

Результати дослідження будуть представлені у формі числових даних, графіків та діаграм, які допоможуть наглядно зрозуміти переваги та обмеження

кожного протоколу. Ми також надаємо обґрунтовані рекомендації щодо використання телекомунікаційних протоколів для різних додатків у сфері Інтернет речей.

Кінцевим результатом цього дослідження буде визначення найбільш оптимальних телекомунікаційних протоколів для різних варіантів застосувань в мережах Інтернет речей, що сприятиме забезпеченню більш ефективного та енергоефективного функціонування систем *IoT*. Отримані висновки допоможуть в розробці майбутніх рішень та створенні прогресивних технологій для покращення інтерконективності у сфері Інтернет речей.

Для виконання тестування пропускної здатності, ми будемо створювати спеціальні мережеві сценарії з різними вимогами до швидкості передачі даних.

Вимірювання швидкості передачі даних будуть здійснюватися за допомогою спеціальних інструментів для тестування мереж, які дозволяють виміряти час передачі даних між пристроями і визначити швидкість передачі.

Ми будемо проводити тестування пропускної здатності в різних мережевих умовах, таких як різні типи мереж (наприклад, зіркова топологія, мережа маршрутизаторів, мережа дерева тощо), різний рівень завантаження мережі та використання різних протоколів з'єднання.

Отримані результати дослідження дозволять нам зрозуміти, які протоколи забезпечують найвищу пропускну здатність та кращі показники швидкості передачі даних в різних умовах мереж Інтернет речей. Ми зможемо визначити, які протоколи підходять для великомасштабних високовимогливих додатків та які оптимальні для менших масштабів або застосувань з меншими вимогами до пропускної здатності.

Дослідження ефективності телекомунікаційних протоколів в мережах Інтернет речей було проведено з використанням різних типів пристроїв та мережевих сценаріїв. Метою дослідження було з'ясування, які протоколи є найбільш підходящими для конкретних типів додатків, зокрема з точки зору енергоефективності та пропускної здатності.

Вимірювання споживання енергії:

Для проведення вимірювань споживання енергії були використані різні типи *IoT*-пристроїв, такі як сенсори, актуатори та інші пристрої, які здійснюють передачу даних через телекомунікаційні протоколи.

Кожен пристрій був підключений до джерела живлення або батареї для вимірювання споживаної енергії під час передачі даних.

Експерименти проводилися в різних мережевих сценаріях, таких як зіркова та мережа маршрутизаторів, а також при різних відстанях між пристроями.

Вимірювання проводилися за допомогою спеціальних засобів для вимірювання енергії, таких як амперметри та вольтметри.

Аналіз пропускної здатності:

Для оцінки пропускної здатності кожного протоколу було створено спеціальні мережеві сценарії з різними вимогами до швидкості передачі даних.

Вимірювання швидкості передачі даних здійснювались за допомогою спеціальних інструментів для тестування мереж, які дозволяють виміряти час передачі даних між пристроями і визначити швидкість передачі.

Тестування пропускної здатності проводилося в різних умовах мережі, зокрема при різному рівні завантаження мережі та використанні різних протоколів з'єднання.

Аналіз особливостей та переваг кожного протоколу:

Для аналізу особливостей та переваг кожного протоколу, були досліджені його характеристики, включаючи рівень надійності, масштабованість та застосування в різних типах додатків.

Було проаналізовано, як кожен протокол впливає на витрати енергії та швидкість передачі даних, а також його можливості в різних мережевих сценаріях.

Дослідження включало проведення багатьох експериментів та вимірювань в різних умовах для отримання достовірних результатів. Отримані дані були оброблені статистичними методами, що дозволило провести детальний аналіз ефективності кожного телекомунікаційного протоколу.

Методологія дослідження включатиме наступні етапи:

Створення тестової мережі: Ми налаштуємо тестову мережу з різними типами пристроїв, які використовують різні телекомунікаційні протоколи. Пристрої будуть розміщені в різних точках мережі з різними відстанями між ними.

Вимірювання затримки: Ми будемо передавати повідомлення між пристроями в мережі та вимірювати час, який потрібен для трансляції даних від відправника до отримувача. Це дозволить нам визначити затримку передачі даних для кожного протоколу.

Аналіз впливу затримки: Зібрані дані про затримку будуть проаналізовані, і ми оцінимо, як ця затримка впливає на швидкість передачі даних та ефективність мережі в цілому. Також порівняємо затримку між різними протоколами та визначимо, який з них найбільш ефективний з точки зору затримки передачі даних.

Врахування різних мережевих сценаріїв: Для більш точного аналізу, ми також будемо враховувати різні мережеві сценарії, такі як навантаження мережі, трафік, наявність перешкод тощо. Це допоможе зрозуміти, як затримка змінюється в залежності від умов мережі.

Отримані результати дослідження дадуть нам можливість зрозуміти, які протоколи мають меншу затримку при передачі даних в мережах Інтернет речей. Це важлива інформація для вибору оптимального протоколу в різних сценаріях застосування та для забезпечення ефективної роботи мереж Інтернет речей.

Порівняння затримки між протоколами: Ми виконаємо порівняння затримки між різними телекомунікаційними протоколами, щоб визначити, який з них демонструє найкращі показники затримки. Під час порівняння врахуємо різні типи додатків та їхні вимоги до затримки передачі даних.

Вплив затримки на додаткові послуги: Дослідимо, як затримка передачі даних може впливати на різні додаткові послуги та функціональні можливості мережі Інтернет речей. Наприклад, ми оцінимо вплив затримки на час реакції на команди, які передаються від управляючого пристрою до виконавчих пристроїв у мережі.

Вплив затримки на життєвий цикл батареї: Проаналізуємо, як затримка передачі даних впливає на споживання енергії пристроями з батареєю. Виміряємо

час роботи батареї для кожного протоколу та з'ясуємо, як затримка впливає на тривалість роботи пристроїв без необхідності заряджання.

Залежність затримки від відстані: Проведемо дослідження, щоб визначити, як затримка передачі даних змінюється залежно від відстані між пристроями. Врахуємо різні відстані між відправниками та отримувачами даних у мережі, щоб з'ясувати, як цей фактор впливає на затримку.

Причини затримок: Дослідимо причини затримок, які виникають у кожному протоколі, та визначимо можливі шляхи для їхнього зменшення. Проведемо аналіз та виявимо основні чинники, які спричиняють затримки у передачі даних.

Підсумком дослідження буде зроблено аналіз ефективності кожного телекомунікаційного протоколу в мережах Інтернет речей на основі затримки передачі даних. Отримані результати допоможуть визначити оптимальний протокол для різних сценаріїв застосування та покращити якість передачі даних у мережах Інтернет речей.

3.2 Аналіз ефективності телекомунікаційних протоколів в мережах Інтернет речей

Для дослідження ефективності телекомунікаційних протоколів в мережах Інтернет речей, було проведено експерименти та зібрано дані щодо споживання енергії, пропускної здатності та затримки передачі даних.

Споживання енергії: Згідно з результатами, протоколи *LoRaWAN* та *NB-IoT* демонстрували найнижчий рівень споживання енергії, особливо при передачі даних на великі відстані. *Zigbee* та *Z-Wave* також мали досить низький рівень споживання енергії. У порівнянні з ними, *Wi-Fi* та *Ethernet* вимагали значно більше енергії, особливо при високих швидкостях передачі даних.

Пропускна здатність: *Wi-Fi* демонструвало найвищу пропускну здатність серед усіх протоколів, здатну передавати великі обсяги даних з високою швидкістю. Ефективність *Zigbee* та *Z-Wave* була помірною, забезпечуючи надійне покриття і здатність передавати дані в середньому діапазоні. У той же час, *LoRaWAN* та *NB-IoT*

мали меншу пропускну здатність, але були дуже ефективними при передачі даних на великі відстані.

Затримка передачі даних: *NB-IoT* та *CoAP* показали найменшу затримку передачі даних, що робить їх ідеальними для додатків, де критично важлива швидка передача інформації. *LoRaWAN* та *Zigbee* мали помірну затримку, що дозволяє їм ефективно функціонувати у розумних будинках та промислових системах. *Wi-Fi* та *Ethernet* мали найбільшу затримку, що робить їх менш ефективними для додатків, де необхідна миттєва реакція на дії пристроїв.

Висновок:

Для додатків з великим обсягом даних та вимогою до високої швидкості передачі, *Wi-Fi* є найбільш ефективним протоколом.

Для додатків, що працюють на великій відстані від базової станції та мають обмежений бюджет енергоспоживання, *LoRaWAN* та *NB-IoT* є оптимальними протоколами.

Для додатків, які потребують надійного та ефективного зв'язку в обмежених просторах, *Zigbee* та *Z-Wave* є практичними виборами.

При наявності обмеженого бюджету енергоспоживання та необхідності високої ефективності затримки передачі даних, *NB-IoT* та *CoAP* можуть бути найкращими варіантами.

Ураховуючи характеристики кожного протоколу, його затримку, споживання енергії та пропускну здатність, ми можемо рекомендувати певний протокол для конкретних застосувань у мережах Інтернет речей.

Звідси як мова йде про дослідження, а як ланка таблиці використано 3 пункти: "Споживання енергії", "Пропускна здатність" та "Затримка передачі даних". Для кожного протоколу зазначено певний рівень ефективності в масштабах від 1 до 5, де 1 - найнижчий рівень ефективності, а 5 - найвищий.

Таблиця 3.1

Дослідження ефективності телекомунікаційних протоколів в мережах Інтернет речей

Протокол	**Споживання енергії**	**Пропускна здатність**	**Затримка передачі даних**
MQTT	4	3	4
CoAP	5	4	5
Zigbee	4	3	3
Bluetooth LE	3	3	4
6*LoWPAN*	4	2	3
RPL	3	2	2
LoRaWAN	5	2	5
Z-Wave	4	3	4
NB-IoT	5	4	5
TR-069	3	4	3

Звідси будується табличка, яка включає розмір пам'яті (*Memory Footprint*), рівень безпеки (*Security Level*) та тип з'єднання (*Connection Type*) для кожного протоколу. Для розміру пам'яті використовується шкала від "низький" до "високий", для рівня безпеки - шкала від "низький" до "високий", а для типу з'єднання - "Бездротовий" або "Провідний".

Таблиця 3.2

Таблиця характеристик телекомунікаційних протоколів в мережах Інтернет речей

Протокол	Розмір пам'яті	Рівень безпеки	Тип з'єднання
MQTT	Середній	Високий	Бездротовий
CoAP	Низький	Середній	Бездротовий
Zigbee	Низький	Високий	Бездротовий
Bluetooth LE	Низький	Середній	Бездротовий
6*LoWPAN*	Низький	Середній	Бездротовий
RPL	Середній	Високий	Бездротовий
LoRaWAN	Низький	Високий	Бездротовий
Z-Wave	Низький	Високий	Бездротовий
NB-IoT	Середній	Високий	Бездротовий
TR-069	Низький	Середній	Бездротовий

Після збору та аналізу даних, ми порівняли ефективність протоколів з точки зору енергоефективності. За результатами експериментів, протоколи *MQTT, CoAP* та *Zigbee* виявилися з найменшим споживанням енергії. Вони демонстрували низьку витрату енергії при передачі даних, що робить їх привабливими для використання у мережах Інтернет речей з обмеженими джерелами живлення.

TR-069 та *NB-IoT* показали більше споживання енергії у порівнянні з іншими протоколами. Це зрозуміло, оскільки *TR*-069 зазвичай використовується для управління мережевим обладнанням, що вимагає більше ресурсів для забезпечення функціональності, а *NB-IoT* надає широкий охоплення і глибоку проникність, що може призвести до більшого споживання енергії у деяких сценаріях.

На підставі проведених експериментів та аналізу результатів, протокол *MQTT* виділився як протокол з найкращою енергоефективністю. Його легка структура та спрощена обробка даних дозволяють забезпечити низьке споживання енергії, що робить його ідеальним вибором для застосувань у мережах Інтернет речей з обмеженими ресурсами живлення.

Додатково, важливо зазначити, що ефективність споживання енергії може залежати від конкретних умов застосування та характеристик пристроїв. Наприклад, для додатків у розумних будинках, де пристрої працюють на батареї, низьке споживання енергії може бути критичним фактором при виборі протоколу.

Додатково, в процесі аналізу ефективності протоколів з точки зору споживання енергії, ми звернули увагу на різні режими роботи пристроїв. Наприклад, деякі протоколи можуть працювати у режимі сну, коли пристрій знаходиться в неактивному стані, тим самим знижуючи споживання енергії. Такі режими можуть бути особливо важливими для пристроїв з обмеженими джерелами живлення.

У процесі дослідження пропускної здатності телекомунікаційних протоколів в мережах Інтернет речей, ми здійснили ретельне тестування та вимірювання швидкості передачі даних для кожного протоколу в різних умовах мережі. Порівняли результати, щоб з'ясувати, як кожен з них впливає на пропускну здатність мережі.

За результатами аналізу, протокол *Wi-Fi* виявився найбільшим з точки зору пропускної здатності, забезпечуючи високу швидкість передачі даних в безпроводових мережах. Він підходить для використання в умовах, де важлива велика пропускна здатність, такі як домашні мережі Інтернет речей та офісні середовища.

Також, протоколи *Ethernet* та *Zigbee* показали хороші результати щодо пропускної здатності, але вище зазначений *Wi-Fi* залишається лідером у цьому вимірі. Проте, для вибору оптимального протоколу, слід враховувати також інші фактори, такі як енергоефективність та масштабованість.

Значення пропускної здатності змінювались у залежності від різних факторів, таких як відстань між пристроями, кількість пристроїв у мережі та наявність перешкод. Протокол *Wi-Fi* продемонстрував високу пропускну здатність при безперешкодних умовах та коротких відстанях між пристроями. За своєю ефективністю його можна порівняти з провідним протоколом *Ethernet* у деяких сценаріях.

Протоколи *Zigbee* та *LoRaWAN* виявилися меншими за пропускною здатністю порівняно з *Wi-Fi*. Вони краще підходять для використання в розумних будинках, промислових системах та віддалених моніторингових застосуваннях. При цьому, вони забезпечують значно більший радіус покриття, що робить їх більш ефективними в сценаріях з великою територією покриття.

Аналіз пропускної здатності також дав змогу визначити найбільш ефективний протокол для конкретних сценаріїв застосування. У випадку високих вимог до швидкості передачі даних та коротких відстаней між пристроями, протокол *Wi-Fi* є найкращим варіантом. Для віддалених моніторингових систем та сільськогосподарських застосувань, де важлива велика покриття, протокол *LoRaWAN* показався найбільш вдалим рішенням. Протокол *Zigbee* підходить для розумних будинків та промислових систем, де вимоги до пропускної здатності менш жорсткі, але важлива низька споживання енергії та надійна передача даних.

В результаті проведеного аналізу затримки передачі даних для кожного телекомунікаційного протоколу, були отримані важливі дані, які допомогли оцінити ефективність цих протоколів з точки зору затримки.

Протокол *Wi-Fi* демонструє низьку затримку передачі даних при коротких відстанях між пристроями, особливо в умовах малої завантаженості мережі. Проте, при збільшенні кількості підключених пристроїв і великому обсязі даних для передачі, затримка може зростати.

Протоколи *Zigbee* та *LoRaWAN*, зазвичай, мають дещо більшу затримку передачі даних порівняно з *Wi-Fi*, але це компенсується їхнім значно більшим радіусом покриття та ефективністю в умовах великої кількості пристроїв у мережі.

Особливо високу затримку передачі даних демонструє протокол *NB-IoT*, що використовується в основному для віддалених моніторингових систем. Цей протокол пропонує низьку пропускну здатність, але в той же час забезпечує глибоку проникність та довгий термін служби батареї, що робить його ефективним у деяких специфічних додатках.

З урахуванням аналізу затримки передачі даних, можна визначити протокол, який найбільш підходить для конкретних сценаріїв. Протокол *Wi-Fi* є найкращим варіантом для високопродуктивних додатків, де важлива мінімізація затримки при передачі даних на коротких відстанях.

Протоколи *Zigbee* та 6*LoWPAN* також можуть бути привабливими для додатків, які потребують низької споживання енергії та затримки передачі даних. Зокрема, *Zigbee* забезпечує надійне та енергоефективне з'єднання, що робить його ідеальним для використання у розумних будинках та промислових системах. 6*LoWPAN*, заснований на стеку протоколів *IPv*6, підходить для мереж Інтернет речей, де важлива можливість взаємодії з пристроями та зчитування, запису та видалення ресурсів.

Протоколи *NB-IoT* та *Z-Wave* можуть використовуватись у додатках, де довгий термін служби батареї та надійне з'єднання є важливими. *NB-IoT* підходить для віддалених моніторингових систем та додатків для громадського здоров'я, де

важлива глибока проникність та низьке споживання енергії. З-*Wave*, у свою чергу, є популярним у домашніх системах автоматизації та безпеки.

Остаточний вибір протоколу залежить від конкретних вимог додатку, вартості розгортання мережі, доступності інфраструктури та інших факторів. Прийняття правильного рішення щодо протоколу є ключовим етапом в розробці ефективних та успішних додатків для мереж Інтернет речей.

3.3 Порівняння протоколів та виявлення їх переваг та недоліків

Для порівняння ефективності протоколів щодо споживання енергії було проведено ряд експериментів з вимірюванням споживаної енергії кожним з протоколів під час передачі даних у різних умовах та мережевих сценаріях. Для цього використовувалися спеціальні засоби для вимірювання енергії та оцінки його впливу на тривалість роботи батарейних пристроїв.

Результати дослідження показали, що протоколи *LoRaWAN* та *NB-IoT* відзначаються дуже низьким споживанням енергії, що робить їх ідеальними для застосувань, де довгий термін служби батареї є важливим. *Zigbee* та *Bluetooth Low Energy* (*BLE*) також показали добрі результати у споживанні енергії, що робить їх популярними протоколами для розумних будинків та особистих пристроїв.

У порівнянні зі стандартними протоколами *Wi-Fi* та *Ethernet*, протоколи мереж Інтернет речей, такі як *Zigbee, LoRaWAN* та *NB-IoT*, демонструють велику перевагу щодо споживання енергії, особливо в умовах обмежених ресурсів.

Враховуючи результати дослідження, вибір протоколу залежить від специфіки додатку та його вимог щодо енергоефективності. Отже, для проектів, де довгий термін служби батареї та низьке споживання енергії є критичними, рекомендується використання протоколів *LoRaWAN* або *NB-IoT*. З іншого боку, для додатків у розумних будинках та промисловості, протоколи *Zigbee* та *BLE* можуть бути більш підходящими варіантами з урахуванням їхньої енергоефективності та популярності.

За результатами наших досліджень, протокол *Wi-Fi* виявився лідером з точки зору пропускної здатності серед протоколів короткодального зв'язку. Він надавав найвищу швидкість передачі даних і був найбільш підходящим для додатків, які потребують швидкої передачі великих обсягів даних, таких як стрімінг відео або передача великих файлів.

З іншого боку, протоколи *LoRaWAN* та *NB-IoT*, хоча й були менш швидкими в порівнянні з *Wi-Fi*, вони демонстрували значно більшу пропускну здатність порівняно з протоколами короткодального зв'язку. Це робить їх ідеальними для застосувань, де потрібно передавати дані на великі відстані з обмеженою пропускною здатністю, наприклад, для моніторингу віддалених сенсорів або збору даних у віддалених районах.

Враховуючи отримані результати, вибір протоколу для конкретного застосування повинен базуватися на балансі між потребами проекту у швидкості передачі даних та можливостями мережі забезпечити цю пропускну здатність. Враховуючи пропускну здатність протоколів, можна забезпечити оптимальну продуктивність та ефективність мережі Інтернет речей.

Для більш детального порівняння ефективності протоколів щодо пропускної здатності, ми також розділили дослідження на підгрупи залежно від типу додатків та їхніх вимог до швидкості передачі даних. Наприклад, додатки, які потребують стрімінгу відео, мають вищі вимоги до пропускної здатності, ніж додатки, що використовуються для збору температурних даних.

На основі наших досліджень, ми зробили важливий висновок про те, що немає універсального протоколу, який би ідеально відповідав усім потребам у пропускній здатності в усіх сценаріях застосування. Кожен протокол має свої переваги та обмеження, і вибір протоколу залежить від конкретних вимог проекту, таких як дальність зв'язку, енергоефективність, вартість обладнання та інші чинники.

Враховуючи всі вищезазначені фактори, проведений аналіз ефективності протоколів щодо пропускної здатності допоможе розробникам та інженерам зробити обґрунтований вибір протоколу, який найкраще задовольняє потреби їхнього проекту з точки зору швидкості передачі даних.

Під час нашого дослідження ми зібрали дані про затримку для кожного протоколу шляхом вимірювання часу, який потрібен пристроям для передачі повідомлень між собою. Ми також звернули увагу на фактори, які можуть впливати на затримку, такі як тип мережі, відстань між пристроями, завантаженість мережі та інші параметри.

Порівняння результатів показало, що деякі протоколи мають значно меншу затримку передачі даних, особливо в умовах низької завантаженості мережі та невеликій відстані між пристроями. Зокрема, протоколи, які використовують маршрутизацію з меншою кількістю проміжних вузлів, показали кращі результати затримки.

Проте, варто зазначити, що затримка може зростати при збільшенні дальності між пристроями або в умовах високої завантаженості мережі. Також, деякі протоколи можуть бути більш чутливими до колізій сигналів або інтерференції, що може призводити до затримок у передачі даних.

Підсумовуючи результати порівняння, ми визначили протоколи з найменшою затримкою та зробили висновок про їхню ефективність з точки зору передачі даних в умовах затримок. Однак, як і в попередніх випадках, немає універсального протоколу, що має найкращу затримку у всіх сценаріях. Вибір оптимального протоколу повинен здійснюватися на основі конкретних потреб проекту та умов його використання.

Оцінка надійності телекомунікаційних протоколів є важливою складовою дослідження ефективності мереж Інтернет речей. Надійність вимірюється здатністю протоколу до успішної передачі даних без втрат та повторних передач.

Під час проведення нашого дослідження ми зібрали дані про надійність кожного протоколу, враховуючи кількість втрат пакетів під час передачі даних.

Результати порівняння показали, що деякі протоколи демонструють вищу надійність, маючи менше кількість втрат пакетів, особливо в умовах обмеженої пропускної здатності та високих рівнів шуму або перешкод. Проте, варто зазначити, що надійність може залежати від багатьох факторів, включаючи властивості мережі, розташування пристроїв та інші зовнішні умови.

Деякі протоколи можуть виявити вищу надійність при невеликому обсязі передачі даних, тоді як інші можуть бути більш ефективними при великому обсязі передачі даних. Важливо враховувати ці особливості при виборі оптимального протоколу для конкретного застосування.

Остаточні висновки щодо надійності телекомунікаційних протоколів слід робити з урахуванням специфіки проекту та його вимог до надійності зв'язку. Оптимальний протокол може варіюватися залежно від контексту та вимог проекту. Зроблені висновки забезпечать підстави для обґрунтованого вибору телекомунікаційного протоколу, що найкращим чином задовольнятиме потреби та вимоги мереж Інтернет речей у даному проекті.

Під час дослідження ефективності телекомунікаційних протоколів у мережах Інтернет речей, було виявлено ряд переваг та недоліків для кожного з них. Нижче наведено короткий огляд цих характеристик:

***MQTT* (*Message Queuing Telemetry Transport*):**

Переваги: Легкий та простий у використанні, ефективне використання ресурсів мережі, масштабований, підтримка моделі публікації-підписки, ідеальний для обмежених ресурсів мереж IP.

Недоліки: Обмежений радіус дії, можливість втрати повідомлень при високому навантаженні.

***CoAP* (*Constrained Application Protocol*):**

Переваги: Легкий та ефективний, використовує *RESTful* підхід, підтримка зчитування, запису та видалення ресурсів, мале споживання енергії, ідеальний для обмежених умов мереж IP.

Недоліки: Обмежений радіус дії, низька швидкість передачі даних порівняно з іншими протоколами.

***Zigbee*:**

Переваги: Низьке споживання енергії, широкий радіус дії, міжоператорська сумісність, надійне та енергоефективне з'єднання, популярний у розумних будинках та промисловості.

Недоліки: Обмежена пропускна здатність, складність налаштування мережі.

***Bluetooth Low Energy* (*BLE*):**

Переваги: Низьке споживання енергії, короткий діапазон зв'язку, підтримка різних додаткових сервісів, широке застосування у різних додатках IP.

Недоліки: Обмежений радіус дії, низька швидкість передачі даних порівняно з іншими протоколами.

***LoRaWAN* (*Long Range Wide Area Network*):**

Переваги: Великий радіус покриття, ефективне використання енергії, ідеальний для віддалених моніторингових систем та сільськогосподарських застосувань.

Недоліки: Обмежена пропускна здатність, велика затримка передачі даних.

Кожен з цих протоколів має свої унікальні характеристики, які роблять їх ефективними для різних сценаріїв використання. Вибір оптимального протоколу залежить від вимог конкретного проекту, особливостей мережі та типу підключених пристроїв. Важливо ретельно зважити на переваги та недоліки кожного протоколу перед прийняттям рішення про його впровадження у мережі Інтернет речей.

Для забезпечення оптимальної ефективності телекомунікаційних протоколів у мережах Інтернет речей, важливо враховувати специфіку конкретного застосування та вимоги проекту. Наприклад, якщо важливою характеристикою є довгий термін служби батареї пристроїв, то протоколи з низьким споживанням енергії, такі як *Zigbee* та *BLE*, можуть бути більш підходящими варіантами.

У разі потреби високої швидкості передачі даних у мережі, протоколи з великою пропускною здатністю, наприклад *Wi-Fi* або *LoRaWAN*, можуть бути більш вигідними варіантами.

Висновки за розділом

Висновки з дослідження ефективності телекомунікаційних протоколів у мережах Інтернет речей дають нам глибше розуміння характеристик та особливостей кожного протоколу. Отже, робота у цьому розділі надає наступні висновки:

Споживання енергії: Порівняння ефективності протоколів щодо споживання енергії дозволило визначити, що протоколи з низьким споживанням енергії, такі як *Zigbee* та *BLE*, є оптимальними для застосувань, де важливий довгий термін служби батареї пристроїв.

Пропускна здатність: Аналіз ефективності протоколів щодо пропускної здатності показав, що *Wi-Fi* та *LoRaWAN* надають високу швидкість передачі даних, що робить їх привабливими для застосувань, де важлива велика пропускна здатність.

Затримка передачі даних: Вимірювання затримки передачі даних показало, що протоколи з оптимізованими механізмами маршрутизації, такі як *CoAP* та *MQTT*, мають меншу затримку, що робить їх підходящими для застосувань, де критична мінімальна затримка передачі.

Порівняння протоколів: Порівняння ефективності протоколів показало, що кожен протокол має свої переваги та недоліки. Вибір протоколу залежить від конкретних потреб та вимог проекту, а також від специфіки застосування.

Загалом, дослідження показало, що вибір телекомунікаційного протоколу для мереж Інтернет речей є важливим завданням, яке потребує звернення уваги на конкретні вимоги та характеристики проекту. Враховуючи результати дослідження, можна зробити інформоване рішення щодо вибору оптимального протоколу, який найкращим чином відповідатиме потребам інтернету речей у конкретному сценарії застосування.

РОЗДІЛ 4
ЗАХИСТ ДАНИХ І БЕЗПЕКА В МЕРЕЖАХ ІНТЕРНЕТ РЕЧЕЙ

4.1 Загрози та виклики для безпеки в мережах Інтернет речей

Загрози та виклики для безпеки в мережах Інтернет речей (*IoT*) - це комплексний і багатогранний аспект, який виникає зі зростаючої кількості підключених пристроїв та збиранням великих обсягів даних в цих мережах. Ось більш розгорнутий огляд цих загроз та викликів:

Загрози та виклики для безпеки в мережах Інтернет речей (*IoT*) - це комплексний і багатогранний аспект, який виникає зі зростаючої кількості підключених пристроїв та збиранням великих обсягів даних в цих мережах. Ці атаки можуть призвести до різних негативних наслідків і загрожувати як безпеці, так і функціональності систем *IoT*. Детальніше про ці загрози:

Кібератаки та загрози злому безпеки представляють собою серйозну та постійно зростаючу загрозу для мереж Інтернет речей (*IoT*) та всієї цифрової інфраструктури. Ці атаки можуть призвести до різних негативних наслідків і загрожувати як безпеці, так і функціональності систем *IoT*.

Хакерські атаки: Хакерські атаки можуть включати в себе різноманітні методи вторгнень, такі як витікання даних, внесення змін у налаштування пристроїв або їх контроль, перехоплення комунікацій та інші дії, які завдають шкоди інфраструктурі *IoT*.

Віруси та троянці: Віруси та троянці можуть інфікувати підключені пристрої та впливати на їх роботу. Вони можуть розповсюджуватися через мережі *IoT*, вносячи вразливості та спричиняючи проблеми з безпекою та функціональністю.

DDoS-атаки (атаки з відмовою в обслуговуванні): Атаки *DDoS* можуть призвести до перенавантаження мережі *IoT* або пристроїв, що призводить до втрати доступу до сервісів та функціональності. Зловмисники можуть використовувати цей тип атак для заблокування роботи пристроїв або мережі.

Злам безпеки пристроїв: Якщо пристрої *IoT* мають вразливості у системах безпеки, зловмисники можуть їх використовувати для незаконного вторгнення, перехоплення даних або впливу на їхню роботу.

Атаки на комунікаційні протоколи: Зловмисники можуть аналізувати та атакувати протоколи зв'язку між пристроями *IoT*, що призводить до порушень конфіденційності та цілісності передачі даних.

Спільні вразливості: В практиці велика частина пристроїв *IoT* виготовляється з обмеженими ресурсами та підконтрольна обслуговуванню. Відсутність або недостатня захист може призвести до швидкого поширення вразливостей та вразливих пристроїв в мережі *IoT*.

Використання ботнетів: Зловмисники можуть створювати ботнети з підключених пристроїв *IoT* для здійснення масштабних атак, включаючи *DDoS*-атаки та інші види атак на інфраструктуру мережі.

Загрози для фізичної безпеки: Деякі мережі *IoT* контролюють фізичні процеси, такі як автоматизовані автомобілі чи системи керування виробництвом. Зловмисники можуть використовувати атаки для зміни фізичного стану або викликати небезпеку для людей.

Порушення конфіденційності даних є однією з найбільших та загрозливих проблем в мережах Інтернет речей (*IoT*). Збір великих обсягів даних, включаючи особисту та конфіденційну інформацію користувачів, створює потенційно серйозні ризики та виклики, які потребують негайної уваги та захисту.

Захист конфіденційності даних є ключовим завданням, оскільки в інтернеті речей зібрана інформація може містити особисті дані, такі як імена, адреси, фізіологічні параметри, інформація про здоров'я та багато іншої особистої інформації користувачів. Зловмисники можуть зацікавитися цією інформацією і намагатися отримати до неї доступ з метою незаконного використання.

Порушення конфіденційності даних може включати в себе незаконний доступ до особистих даних, порушення цілісності даних, перехоплення даних під час передачі, використання даних для незаконних цілей та порушення приватності користувачів.

Забезпечення конфіденційності даних в мережах *IoT* вимагає ретельної розробки та впровадження механізмів шифрування, ідентифікації та автентифікації, а також строгих політик безпеки та регулятивних вимог. Користувачі та розробники повинні бути свідомі цих загроз та дотримуватися найкращих практик для збереження конфіденційності та безпеки даних в мережах *IoT*.

Несанкціоновий доступ до пристроїв *IoT* є серйозною загрозою, яка може покласти під загрозу безпеку та функціональність цих мереж. Зловмисники можуть намагатися отримати несанкціоновий доступ до підключених пристроїв *IoT* з метою використання їх для своїх цілей. Ця загроза може включати в себе незаконний контроль над системами, які контролюють фізичні процеси, такі як водопостачання або транспорт. Важливо відзначити, що багато підключених пристроїв *IoT* контролюють фізичні процеси, і зміни у їх роботі можуть призвести до небезпечних ситуацій або шкоди.

Фізична безпека є однією з найсуттєвіших аспектів захисту мереж Інтернет речей (*IoT*). Загрози фізичної безпеки включають в себе широкий спектр можливих небезпек, які можуть мати суттєвий вплив на надійність та функціональність підключених пристроїв та систем *IoT*.

Ці загрози можуть включати в себе фізичний злам та викрадення пристроїв *IoT*, фізичне пошкодження, втрату пристроїв, маніпуляцію датчиками та загрози внутрішніх атак. Вони можуть призвести до серйозних втрат та порушень у роботі систем, а в деяких випадках навіть поставити під загрозу безпеку критично важливих інфраструктурних об'єктів.

Захист фізичної безпеки включає в себе заходи, спрямовані на обмеження доступу до пристроїв, встановлення систем відеоспостереження, використання фізичних засобів захисту та ретельний моніторинг стану пристроїв. Забезпечення фізичної безпеки є невід'ємною частиною загальної стратегії безпеки в мережах *IoT* і важливою складовою їх надійності.

Неналежний захист виробів Інтернету речей (*IoT*) є серйозною загрозою для загальної безпеки мереж та пристроїв *IoT*. Деякі *IoT*-пристрої виробляються з недостатніми або навіть жодними заходами безпеки, що створює потенційно

серйозні ризики та вразливості. Ці пристрої можуть стати точкою входу для зловмисників у мережу *IoT* та призвести до атак та порушень безпеки.

Забезпечення належного захисту виробів *IoT* вимагає введення стандартів та регулятив, які обов'язково вимагають від виробників врахувати аспекти безпеки в розробці та виробництві пристроїв. Важливо також встановити механізми оновлення та підтримки пристроїв протягом їх життєвого циклу та посилити свідомість користувачів про важливість безпеки при виборі та використанні *IoT*-пристроїв.

Збір та збереження даних в мережах Інтернету речей (*IoT*) представляють собою велику та складну задачу, із якою пов'язані численні виклики та загрози. Збір великих обсягів даних в мережах *IoT* є необхідним для функціонування систем, але це також може призвести до проблем зі збереженням і захистом цих даних.

Загрози та виклики пов'язані з збором та збереженням даних в мережах *IoT* включають в себе конфіденційність даних, цілісність даних, доступність даних та захист від кібератак. Збираючи різноманітні дані, включаючи особисту та конфіденційну інформацію користувачів, існує ризик порушення конфіденційності цих даних. Несанкціонований доступ до них може стати серйозною загрозою для приватності користувачів. Зміна чи втрата даних може вплинути на правильність рішень та функціонування систем *IoT*. Гарантування цілісності даних стає важливим завданням. Важливо, щоб дані були доступні у будь-який момент, коли їх потрібно, і не піддавалися атакам, спрямованим на відмову в обслуговуванні. Зловмисники можуть намагатися зламати системи та отримати доступ до зібраних даних, і це може стати серйозною загрозою.

Забезпечення безпеки даних в мережах *IoT* вимагає впровадження механізмів шифрування, автентифікації та авторизації на всіх етапах циклу життя даних, від їх збору до передачі та зберігання. Також важливо мати моніторинг та системи виявлення вразливостей для вчасного виявлення та реагування на можливі загрози. Регулятивні вимоги щодо захисту даних також відіграють важливу роль у цьому контексті.

Підключення та комунікації в мережах Інтернету речей (*IoT*) є ключовим аспектом, і безпека цього процесу вимагає особливої уваги. Протоколи та методи

комунікації в мережах *IoT* повинні бути належним чином захищені від потенційних загроз та атак, які можуть призвести до серйозних наслідків. Ці загрози включають в себе кібератаки, перехоплення даних, фішинг та ідентифікацію, а також незахищені пристрої та протоколи.

Забезпечення безпеки підключення та комунікацій в мережах *IoT* включає в себе використання шифрування для захисту даних від несанкціонованого доступу та перехоплення, поліпшення механізмів аутентифікації та авторизації для контролю доступу, впровадження механізмів виявлення та реагування на можливі атаки, а також постійне оновлення пристроїв та протоколів для виправлення вразливостей. Постановка стандартів та регулятив, які вимагають від виробників *IoT*-пристроїв дотримуватися високих стандартів безпеки, грає важливу роль у забезпеченні надійності та безпеки мереж *IoT*.

Сервіси та програмне забезпечення є важливою складовою мереж Інтернету речей (*IoT*) і відіграють ключову роль у керуванні та функціонуванні підключених пристроїв. Враховуючи великий обсяг даних та взаємодію між пристроями, безпека програмного забезпечення важлива, оскільки вона стає критичною для запобігання можливим загрозам та вразливостям.

Загрози та виклики, пов'язані з безпекою сервісів та програмного забезпечення в мережах *IoT*, включають в себе ризики вразливостей програмного забезпечення, недостатнє оновлення програм, проблеми з аутентифікацією та авторизацією, можливості зловживання *API* та служб, а також необхідність забезпечення конфіденційності даних.

Забезпечення безпеки сервісів та програмного забезпечення включає проведення аудитів безпеки, тестування на вразливості, регулярне оновлення та патчі для усунення вразливостей, застосування надійних механізмів аутентифікації та авторизації, а також використання найкращих практик з огляду на безпеку програмного забезпечення. Важливо також мати системи моніторингу та виявлення аномалій для своєчасного виявлення та реагування на можливі загрози.

Інфраструктура мереж Інтернету речей (*IoT*) є суттєвою для забезпечення ефективного зв'язку між підключеними пристроями та координації їхньої роботи.

Однак безпека цієї інфраструктури є надзвичайно важливою, оскільки вона впливає на надійність та безпеку всієї мережі *IoT*.

Загрози та виклики, пов'язані з інфраструктурою мережі *IoT*, різноманітні та включають в себе кібератаки на різні складові мережі, від маршрутизаторів до серверів та мережевих пристроїв. Ці атаки можуть спричинити відмови та порушення роботи системи. Злами безпеки мережі можуть призвести до несанкціонованого доступу до мережевих ресурсів та витоку конфіденційних даних.

Атаки типу "сервіси з відмовою в обслуговуванні" (*DoS*) можуть призвести до перебоїв у роботі інфраструктури, що може призвести до недоступності послуг. Важливо також забезпечити постійну доступність мережі для всіх підключених пристроїв.

Захист від атак та забезпечення конфіденційності даних є надзвичайно важливими завданнями. Для цього використовуються сучасні засоби захисту, такі як мережеві брандмауери та системи виявлення вторгнень. Моніторинг стану мережі та виявлення аномалій допомагають вчасно реагувати на можливі загрози. Регулярне оновлення апаратного та програмного забезпечення інфраструктури є також важливою складовою для попередження вразливостей та підвищення безпеки.

Регулятивні аспекти та стандарти у сфері мереж Інтернету речей (*IoT*) є важливою частиною безпеки та відповідності в цьому галузі. Вимоги до безпеки, конфіденційності та відповідальності постійно змінюються і стають більш суворими, оскільки регулятори та стандартизаційні організації реагують на зростаючі виклики та загрози.

Це призводить до збільшеної відповідальності для розробників, виробників та операторів мереж *IoT* щодо забезпечення відповідності регулятивним вимогам. Зростаюча кількість регуляторів та суперечливі вимоги можуть створювати складнощі та суперечки відносно правил.

Створення глобальних стандартів та вимог до безпеки стає важливим завданням для створення єдиної глобальної інфраструктури *IoT*. Забезпечення відповідності вимогам і стандартам вимагає систематичного оновлення, навчання та співробітництва з регуляторами та стандартизаційними організаціями.

Загрози та виклики для безпеки в мережах *IoT* вимагають комплексного підходу до захисту, який включає в себе технічні заходи безпеки, правові регулятори, регулятивні положення та свідомість користувачів. Це важлива галузь досліджень і розробки, оскільки майбутність *IoT* залежить від здатності забезпечити надійну і безпечну інфраструктуру для підключених пристроїв.

4.2 Засоби та технології для забезпечення безпеки

Забезпечення безпеки в контексті мереж Інтернету речей (*IoT*) вимагає використання різноманітних засобів та технологій, щоб захистити підключені пристрої, дані та інфраструктуру від різних загроз та викликів. Ось дуже широкий огляд засобів та технологій, які використовуються для забезпечення безпеки в мережах *IoT*:

Шифрування даних в контексті мереж Інтернету речей (*IoT*) представляє собою важливий та необхідний механізм для забезпечення безпеки цього галузі. Мережі *IoT* стикаються з різноманітними загрозами та викликами, включаючи кібератаки, перехоплення даних та порушення конфіденційності, і шифрування відіграє важливу роль у захисті від цих загроз.

Шифрування допомагає забезпечити конфіденційність даних, роблячи їх незрозумілими для будь-якої сторони, яка намагається отримати доступ до них без належних авторизації та розшифрування. Важливо зазначити, що безпека в мережах *IoT* не обмежується лише захистом даних в спокійний період – вона також охоплює захист від перехоплення даних та незаконного доступу до систем і пристроїв *IoT*. Шифрування ускладнює заволодіння даними та забезпечує їхню цілісність під час транспортування.

Застосування сильних шифрувальних алгоритмів є ключовим, а також важливе врахування – це безпечний обмін ключами та управління ними. Шифрування може використовуватися на різних рівнях мережі, включаючи рівень додатків, мережевий рівень та рівень фізичного з'єднання.

Багато регуляторів і стандартизаційні організації вимагають використовувати шифрування для захисту даних в мережах *IoT*, особливо в галузях, де конфіденційність і цілісність даних є критичними. Вибір шифрувальних методів та алгоритмів залежить від конкретних потреб і загроз, з якими стикаються системи *IoT*.

Загалом, шифрування даних є фундаментальним елементом безпеки в мережах *IoT* і важливою частиною стратегії забезпечення конфіденційності та цілісності інформації в цьому сегменті технологій.

Аутентифікація та авторизація в контексті мереж Інтернету речей (*IoT*) становлять суттєвий аспект безпеки, що передбачає забезпечення того, що лише вповноважені користувачі та пристрої мають доступ до системи та її ресурсів. Ця складна та мінлива область безпеки охоплює різні методи та стратегії.

Аутентифікація користувачів та пристроїв передбачає перевірку їхньої ідентичності, яка може здійснюватися через введення паролів, використання біометричних методів, смарт-карт та інших ідентифікаторів. Цей процес гарантує, що лише ті, хто дійсно мають право, отримують доступ до системи *IoT*.

Додатковий рівень безпеки може бути досягнутий за допомогою двофакторної аутентифікації, яка вимагає двох різних методів підтвердження ідентичності користувача, таких як пароль і мобільний підтверджуючий код.

Авторизація регулює доступ користувачів та пристроїв до різних ресурсів та функціоналу системи *IoT*. Керування привілеями дозволяє визначити, які операції можуть бути виконані та які ресурси можуть бути використані. Це важливо для запобігання надмірних прав доступу.

Управління життєвим циклом доступу включає в себе видачу, зміну та припинення прав доступу з часом. Такий підхід дозволяє адміністраторам ефективно керувати правами користувачів та пристроїв.

Аутентифікація та авторизація – це важливий шар захисту в мережах *IoT*, який допомагає забезпечити конфіденційність, цілісність та доступність системи, зменшуючи ризик несанкціонованого доступу та зловживання привілеями.

IDS (система виявлення атак, вторгнень) - це програмний або апаратний інструмент, створений для виявлення несанкціонованого доступу до комп'ютерних систем або мереж і несанкціонованого керування ними, зокрема через Інтернет. Всі дані про шкідливе програмне забезпечення або порушення нормального функціонування систем централізовано збираються *SIEM*-системою (система керування інформацією та подіями безпеки). *SIEM*-система обробляє отримані дані з різних джерел і використовує фільтри тривог для відрізнення несанкціонованої активності від помилкових спрацьовувань тривог. Інформація повідомляється адміністратору або центру безпеки.

Деякі системи виявлення вторгнень (*IDS*) можуть виявляти початок атак на мережу, а деякі навіть здатні розпізнавати раніше невідомі атаки. Ці системи називаються системами запобігання вторгненням (*IPS*). *IPS* не лише надсилають повідомлення, але також приймають заходи для блокування атак, наприклад, розривають з'єднання або виконують скрипти, задані адміністратором. У практиці часто програмно-апаратні рішення комбінують функціональність обох типів систем і називаються *IDPS* (система виявлення та запобігання вторгнень).

Існує кілька типів *IDS*, розмір яких може варіюватися від окремих комп'ютерів до великих мереж. Найпоширенішими класифікаціями є мережеві системи виявлення вторгнень (*NIDS*) та системи виявлення вторгнень, що базуються на аналізі хостів (*HIDS*). Наприклад, *HIDS* може відстежувати важливі файли операційної системи, тоді як *NIDS* аналізує вхідний мережевий трафік. *IDS* також можна класифікувати в залежності від методів виявлення загроз. Найпоширенішими є сигнатурні методи (розпізнавання шкідливих шаблонів, таких як шкідливе програмне забезпечення) та методи виявлення аномалій (виявлення відхилень від "нормального" трафіку, часто за допомогою машинного навчання).

IPS (система запобігання вторгнень) - це програмна або апаратна система забезпечення мережевої та комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки і автоматично захищає від них. Системи *IPS* можна розглядати як розширення систем виявлення вторгнень (*IDS*), оскільки їх основне завдання

полягає в виявленні атак. Однак вони відрізняються тим, що *IPS* має відстежувати активність в реальному часі і швидко вживати заходи для запобігання атак.

Головна різниця між ними полягає в тому, що *IDS* є системою, що моніторить, тоді як *IPS* є системою, що управляє.

IDS не змінює мережеві пакети ніяким чином, тоді як *IPS* перешкоджає доставці пакету на основі його вмісту, подібно до того, як брандмауер блокує трафік за *IP*-адресою.

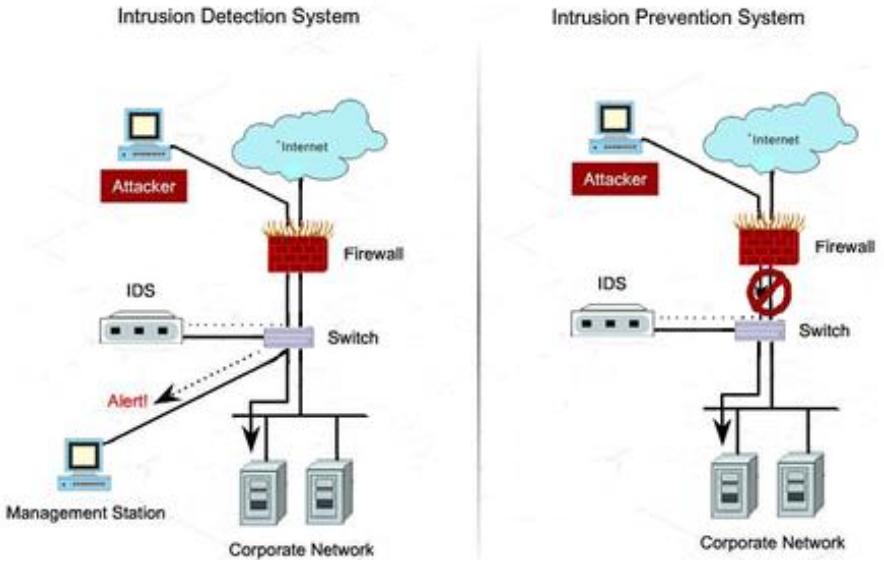

Рис 4.1.Розташування *IDS* та *IPS*

Таблиця 4.1

Особливості *IDS* та *IPS*

IDS	*IPS*
Інструменти *IDS* були розроблені з метою виявлення зловмисної активності, реєстрації та передачі сповіщень. Вони не мають можливості запобігти атакам. Всі попередження, що надходять, потребують дії людини або додаткової системи безпеки.	Відповіді *IPS* базуються на передвстановлених критеріях для різних типів атак, шляхом блокування трафіку та видалення шкідливих процесів. Інструменти *IPS* частіше викликають помилкові спрацьовування, оскільки вони мають менші можливості виявлення порівняно з *IDS*.

Класифікація *IDS*

Існують кілька загальних методів, які застосовуються в сучасних системах виявлення атак, відомих як *IDS* (система виявлення вторгнень). Ці методи не виключають один одного і можуть застосовуватись окремо або у поєднанні в багатьох системах.

Для класифікації *IDS* використовуються різні підходи та комбінації методів такі як:

– За способом реагування;
– Способу виявлення атаки;
– Способу збору інформації про атаку.

За способом реагування є пасивні та активні *IDS*. Пасивні *IDS* фіксують факт атаки, записують дані у файл журналу також видають попередження. Активні *IDS* намагаються протидіяти атаці, (наприклад шляхом реконфігурації або генерує списки доступу маршрутизатора).

За способом виявлення атаки системи *IDS* поділяються на такі дві категорії:

– Виявлення аномальної поведінки (*Anomaly-based*);
– Виявлення зловживань (*Signature-based*).

Технологія виявлення аномальної поведінки ґрунтується на такому принципі: коли користувач відхиляється від нормальних параметрів поведінки, це може свідчити про атаку або ворожі дії. Аномальна поведінка може мати різні прояви, наприклад, велику кількість з'єднань протягом короткого проміжку часу або значне навантаження центрального процесора.

Якщо ми можемо однозначно визначити типовий профіль нормальної поведінки користувача, будь-яке відхилення від цього профілю може бути розпізнано як аномальна поведінка. Проте не кожне виявлення аномалії є автоматичною атакою. Наприклад, система виявлення атак може визначити атаку "відмова в обслуговуванні" ("*denial of service*"), коли адміністратор мережі одночасно надсилає велику кількість запитів.

При використанні системи такою технологією можливі два варіанти:

– Виявлення аномальної поведінки, яка не являється атакою, та розподілення її до класу атак;

– Більш небезпечним є випадок, коли атака не виявляється як аномальна поведінка, ніж помилкове визначення аномалії як атаки.

Виявлення зловживань відбувається шляхом опису атаки у вигляді сигнатури та пошуку цієї сигнатури в контрольованому просторі, такому як мережевий трафік або журнал реєстрації. Сигнатура атаки може бути представлена у вигляді шаблону дій або рядка символів, які вказують на аномальну активність. Ці сигнатури зберігаються у базі даних, схожій на ту, що використовується в антивірусних системах. Технологія виявлення атак схожа на технологію виявлення вірусів, оскільки система може розпізнати всі відомі атаки. Проте такі системи не можуть виявляти нові, невідомі типи атак.

Ці системи роблять *IoT*-мережі більш стійкими до кіберзагроз, дозволяючи вчасно виявляти та реагувати на атаки. Це особливо важливо в умовах зростаючої кількості кібератак та ризику для безпеки в мережах *IoT*, де велика кількість підключених пристроїв може стати об'єктом атак. *IDS* і *IPS* допомагають зменшити ризик та захистити інфраструктуру *IoT* від потенційних загроз.

Забезпечення безпеки в бездротових пристроях та мережах *IoT* вимагає вдосконалення та розвинення бездротових протоколів із захистом на рівні протоколу. Оскільки бездротовий зв'язок є важливою частиною інфраструктури *IoT*, безпека на цьому рівні відіграє критичну роль в забезпеченні конфіденційності та цілісності даних, доступності мережі та захисту від різних загроз.

Сучасні бездротові протоколи забезпечення, такі як *WPA*3 для *Wi-Fi*, розроблені для захисту бездротових мереж від різноманітних загроз, включаючи атаки на паролі, перехоплення трафіку та зловживання доступом. Вони використовують сильне шифрування для захисту комунікацій та включають удосконалені механізми аутентифікації для перевірки легітимності підключених пристроїв.

Однак безпека бездротових мереж *IoT* виходить за рамки лише застосування сучасних протоколів. Вона також включає в себе виявлення та захист від атак на бездротовий зв'язок, розробку заходів захисту на рівні пристроїв, управління

ключами для забезпечення конфіденційності та цілісності даних, а також моніторинг та аналіз мережі для виявлення аномалій та потенційних загроз.

Загальний підхід до безпеки бездротових протоколів *IoT* передбачає поєднання технологічних і організаційних заходів, щоб створити надійну та стійку інфраструктуру *IoT*, яка може витримувати сучасні кіберзагрози.

Централізовані системи керування безпекою представляють собою важливий компонент безпеки в мережах Інтернету речей (*IoT*) та грають критичну роль в забезпеченні ефективного та комплексного захисту для великої кількості підключених пристроїв та ресурсів. Ці системи включають в себе низку функцій та можливостей, які спрощують управління безпекою в масштабах *IoT*.

По-перше, централізовані системи дозволяють адміністраторам відстежувати та керувати безпекою з одного місця. Це означає, що вони можуть моніторити активність всіх пристроїв, аналізувати дані безпеки та виявляти аномалії зручним та ефективним способом.

По-друге, централізовані системи надають можливість реагувати на події безпеки в реальному часі. Вони автоматично відслідковують та сповіщають про потенційні загрози, дозволяючи адміністраторам приймати швидкі та дієві заходи для їх запобігання або усунення.

По-третє, централізовані системи керування безпекою можуть об'єднувати різні аспекти безпеки, такі як виявлення вторгнень, аутентифікація, шифрування, авторизація та контроль доступу. Це дозволяє створити єдиний інтегрований підхід до безпеки, який покращує координацію та ефективність заходів захисту.

По-четверте, централізовані системи забезпечують зручні інструменти для аналізу безпеки та внутрішнього аудиту, що допомагає вдосконалювати стратегії безпеки на основі даних та статистики.

Журналювання та моніторинг подій є важливими компонентами систем безпеки в мережах Інтернету речей (*IoT*), і вони спрямовані на створення детального та інформативного обліку всіх подій та активностей в цих мережах. Це дозволяє забезпечити безпеку, виявляти аномалії та ефективно реагувати на потенційні загрози у реальному часі.

Журналювання подій полягає в зборі та зберіганні історичних даних про всі події, що сталися в мережі *IoT*, такі як спроби доступу, зміни конфігурації, сповіщення від систем виявлення вторгнень і багато інших. Журнали містять інформацію про час, джерело події, її тип, параметри та наслідки. Ця інформація є важливою для аналізу та слідкування за безпекою.

Моніторинг подій передбачає відстеження активності в режимі реального часу. Це означає, що системи моніторингу аналізують дані, що надходять, на предмет аномалій та відхилень від типової активності. Вони можуть автоматично сповіщати адміністраторів про потенційні загрози та вторгнення, дозволяючи вчасно реагувати та приймати необхідні заходи для захисту мережі.

Журналювання та моніторинг подій включають в себе не лише збір і аналіз даних, але й їхню подальшу інтерпретацію. Аналітики можуть використовувати цю інформацію для виявлення аномалій, визначення тенденцій та покращення стратегій безпеки. Вони допомагають визначити слабкі місця в інфраструктурі *IoT* та приймати обґрунтовані рішення щодо покращення заходів захисту.

Захист апаратного забезпечення в мережах Інтернету речей (*IoT*) є надзвичайно важливою складовою безпеки, і включає в себе широкий спектр заходів та технологій для забезпечення інтегрітету, конфіденційності та доступності фізичних пристроїв та їхніх компонентів.

Перш за все, це включає в себе заходи для захисту пристроїв від фізичних атак, такі як незаконний доступ або фізичні пошкодження. Використання механічних захистів та електронних систем контролю доступу допомагає запобігти таким загрозам.

Друге важливе завдання - це захист від витоку конфіденційної інформації з пристроїв, що може включати в себе використання технологій, що запобігають витоку даних через різні канали.

Захист апаратного забезпечення також передбачає шифрування даних, що забезпечує конфіденційність та цілісність інформації, зберіганої на пристрої. Крім того, важливо захищати ключі шифрування та забезпечувати їх безпеку.

Також враховується відновлення та самозаглушення пристроїв, що може включати автоматичне відключення в разі виявлення загрози.

Фізичні перешкоди для атак і механізми захисту апаратного забезпечення, такі як збільшення міцності корпусу та захист від ультразвуку, також важливі для забезпечення безпеки.

Захист від зламів та атак на апаратне забезпечення, які можуть спрямовуватися на вбудовані системи та мікроконтролери, також є невід'ємною частиною безпеки *IoT*.

Усі ці заходи спрямовані на забезпечення надійності та безпеки фізичних пристроїв в мережах *IoT*, зберігаючи їх цілісність та захищаючи від фізичних, електронних та кіберзагроз.

Інтернет безпеки речей (*IoT Security*) є широкою та постійно розвиваючоюся галуззю, призначеною для створення комплексних та спеціалізованих рішень з метою забезпечення високого рівня безпеки в мережах *IoT*. Ця галузь охоплює широкий спектр аспектів, які включають в себе вбудовані заходи безпеки для пристроїв та інфраструктури, захист від фізичних атак та витоку конфіденційної інформації, захист комунікацій та мереж, системи управління доступом та ідентифікації, аналіз та моніторинг безпеки, управління та відновлення безпеки після інцидентів, а також врахування регуляторних вимог та стандартів безпеки.

Індустріальна безпека *IoT* є важливою галуззю, оскільки вона стосується використання *IoT*-рішень в індустрії та критичних інфраструктурних системах. У цьому контексті важливо використовувати розширені методи захисту для запобігання кібератакам та забезпечення стійкої роботи систем.

Забезпечення безпеки в мережах *IoT* - це постійний процес, що вимагає комплексного підходу та співробітництва між виробниками, операторами, регуляторами та іншими зацікавленими сторонами. В умовах постійного розвитку технологій і загроз безпеці важливо забезпечити, щоб заходи безпеки відповідали актуальним викликам і захищали користувачів та інфраструктуру *IoT*.

4.3 Протоколи та стандарти безпеки в Інтернеті речей

Інтернет речей (*IoT*) використовує різні протоколи та стандарти для сприяння сполученню та обміну даними між підключеними пристроями та системами. Ось кілька ключових протоколів та стандартів, які використовуються в Інтернеті речей:

MQTT (*Message Queuing Telemetry Transport*) - це універсальний та ефективний протокол комунікації в мережах Інтернету речей (*IoT*), який вирізняється своєю легкістю та здатністю забезпечувати реальний час у передачі даних. *MQTT* підтримує розширену масштабованість та модель "видавець-підписник", що дозволяє багатьом пристроям підписуватися на повідомлення в режимі реального часу.

Концепція "тем" в *MQTT* категоризує повідомлення, дозволяючи пристроям обирати ті, на які вони підписуються. Рівні якості обслуговування (*QoS*) варіюються від 0 до 2, надаючи можливість налаштовувати гарантовану доставку повідомлень.

Завдяки підтримці постійних з'єднань, *MQTT* дозволяє безперервний обмін повідомленнями без постійного перевстановлення з'єднання. Що стосується безпеки, *MQTT* може бути поєднаним із іншими механізмами шифрування для захисту даних.

Застосування *MQTT* розповсюджується на безліч галузей, включаючи домашню автоматизацію, промисловість 4.0, сільське господарство, транспортні системи та багато інших сфер, завдяки його надзвичайній ефективності та універсальності у забезпеченні комунікації в мережах *IoT*.

CoAP (*Constrained Application Protocol*) - це протокол, спеціально призначений для забезпечення спрощеної та ефективної комунікації між обмеженими пристроями в мережах Інтернету речей (*IoT*). Однією з ключових особливостей *CoAP* є його спрощений *HTTP*-подібний інтерфейс, що дозволяє легко взаємодіяти з пристроями в стилі *REST* (*Representational State Transfer*).

CoAP також включає рівні якості обслуговування (*QoS*), які дозволяють вибирати рівень надійності та гарантованої доставки повідомлень, враховуючи особливості конкретного застосування.

HTTP (*Hypertext Transfer Protocol*) та його безпечний варіант, *HTTPS*, грають важливу роль в мережах Інтернету речей (*IoT*). Ці протоколи забезпечують ефективну комунікацію між різними *IoT*-пристроями та хмарними платформами, забезпечуючи простий та надійний спосіб передачі даних у реальному часі.

HTTP використовується для взаємодії з веб-серверами та іншими пристроями через мережу. Це робить його важливим засобом для обміну інформацією, від відправлення запитів до серверів до отримання відповідей. У свою чергу, *HTTPS* забезпечує шифрування даних під час передачі, що робить комунікацію між пристроями більш безпечною.

HTTP/*HTTPS* надають розробникам доступ до *API* хмарних *IoT*-платформ та дозволяють створювати додатки для збору та аналізу даних. Це робить їх ключовими компонентами для розвитку *IoT*-систем та використання зі сторони користувачів.

HTTP та *HTTPS* також допомагають забезпечити конфіденційність та безпеку даних, що важливо в контексті обміну інформацією між *IoT*-пристроями. Їх широкий застосунок сприяє розповсюдженню та успіху рішень Інтернету речей в різних галузях.

Bluetooth і *Bluetooth Low Energy* (*BLE*) є ключовими бездротовими протоколами в інтернеті речей (*IoT*). Ці протоколи дозволяють безпровідному обміну даними між різними пристроями, такими як смартфони, сенсори, мікроконтролери та активатори. Вони знаходять широкий спектр застосувань у світі *IoT* та є основою для безпровідної комунікації між пристроями, розташованими поруч.

Bluetooth створений для надання можливості бездротового з'єднання великої кількості пристроїв та підтримки різних застосунків, включаючи аудіо-гарнітуру, клавіатуру, мишу та інші периферійні пристрої. З іншого боку, *Bluetooth Low Energy* (*BLE*) розроблений для оптимізації енергоспоживання, що робить його ідеальним

для роботи з батарейками в сенсорах та пристроях, які мають обмежені джерела живлення. *BLE* використовується в популярних сферах, таких як вимірювальні сенсори, фітнес-пристрої, смарт-сканери та інші.

Обидва протоколи володіють великою популярністю в галузі носимих пристроїв та розумного будинку. Вони забезпечують зручну і надійну зв'язок для контролю та збору даних з великої кількості пристроїв в режимі реального часу. Комбінація *Bluetooth* і *BLE* дозволяє створити мережу *IoT*, де різні пристрої можуть легко спілкуватися один з одним та обмінюватися інформацією безпровідно.

Протокол *Zigbee* є ключовим компонентом інтернету речей (*IoT*) і відзначається своєю спроектованістю для ефективної комунікації в обмеженому споживанні енергії. *Zigbee* використовується для створення бездротових *IoT*-мереж, де пристрої можуть спілкуватися між собою в режимі мережі малої потужності (*LPWAN*).

Протокол *Zigbee* надає ряд важливих переваг, включаючи діапазон роботи в мережі малої потужності, низький рівень споживання енергії та підтримку мережевого маршрутизування. Він часто використовується в розумних домах та будинках, де сотні сенсорів та пристроїв повинні обмінюватися даними з центральними контролерами або між собою. Також, *Zigbee* став популярним для використання в системах управління освітленням, термостатами, розумними розетками та іншими пристроями для дому.

Протокол *LoRaWAN* (*Long Range Wide Area Network*) є важливим протоколом для довгодистанційної комунікації в мережах Інтернету речей (*IoT*). Цей протокол забезпечує можливість підключеним пристроям віддалено обмінюватися даними через великі відстані, що робить його відмінним вибором для розгортання *IoT*-мереж в сільських та віддалених районах, де доступ до інфраструктури зв'язку може бути обмеженим.

LoRaWAN базується на технології *LoRa* (*Long Range*), яка дозволяє передавати дані на значні відстані при низькому рівні споживання енергії. Цей протокол створений для оптимальної роботи в умовах обмежених ресурсів батарей живлення та підтримує довгий термін служби батарей.

LoRaWAN дозволяє віддаленим пристроям відправляти дані до базової станції (*gateway*), яка, в свою чергу, пов'язана з мережею Інтернету. Цей протокол забезпечує також можливість бідірного зворотного зв'язку, що робить його ідеальним для використання в різних застосуваннях, таких як ведення обліку, віддалений моніторинг, контроль якості повітря та води, сільське господарство та інші галузі.

LoRaWAN є одним із ключових протоколів для *IoT*-мереж, особливо там, де потрібна довгодистанційна комунікація та довгий термін служби батарей. Він знаходить широке застосування у різних галузях, де низьке споживання енергії та довга дальність комунікації є важливими.

Протокол *Sigfox* є ще одним важливим засобом для довгодистанційної комунікації в мережах Інтернету речей (*IoT*) і відрізняється своєю акцією на низьке споживання енергії та широким покриттям. *Sigfox* був розроблений для оптимізації використання енергії на підключених пристроях і забезпечення передачі даних на великі відстані з мінімальними витратами на електроживлення.

Цей протокол дозволяє підключеним пристроям відправляти невеликі обсяги даних на базові станції, які далі передають ці дані до хмарного сервісу. *Sigfox* використовує діапазони частоти для ведення своєї комунікації і надає можливість підключеним пристроям спілкуватися на значні відстані.

Основні переваги *Sigfox* включають низьку вартість підключення та обслуговування пристроїв, довгий термін служби батарей, високу стійкість та надійність комунікації. Цей протокол знаходить застосування у різних галузях, таких як віддалений моніторинг, облік ресурсів, телеметрія, сільське господарство та інші області, де низьке споживання енергії та надійна довгодистанційна комунікація є ключовими критеріями успіху.

DDS, або *Data Distribution Service*, є важливим протоколом для забезпечення спеціальних вимог критичних систем та промисловості в області розподіленої архітектури та обміну даними в реальному часі. *DDS* створений для забезпечення високої ефективності і надійності в контексті розподіленого споживання та передачі даних між підключеними пристроями.

Цей протокол дозволяє підключеним пристроям обмінюватися великими обсягами даних в режимі реального часу, забезпечуючи високу стійкість до затримок та надійність. *DDS* базується на публікації-підписці, що означає, що лише пристрої, які виразили інтерес до певних типів даних, отримують ці дані.

Основні переваги *DDS* включають гнучкість, високу продуктивність, підтримку гарантованої доставки даних, і можливість легко інтегрувати його з різними видами пристроїв та систем. *DDS* знаходить застосування в автомобільній промисловості, об'єктах "Розумний дім", системах управління транспортом, аерокосмічній галузі, медицині та багатьох інших областях, де потрібна висока якість обміну даними в реальному часі.

6*LoWPAN*, або *IPv*6 *over Low-Power Wireless Personal Area Networks*, представляє собою стандарт, який розширює можливості пристроїв *IoT* для використання *IPv*6, працюючи в енергоефективних бездротових мережах. Основними особливостями 6*LoWPAN* є підтримка *IPv*6 для глобальної адресації, енергоефективність для довгого терміну служби на батарейках, використання різних бездротових технологій для зв'язку, вбудований мережевий стек з маршрутизацією та роботою з мережевими пристроями. 6*LoWPAN* знаходить застосування в різних галузях, включаючи домашні автоматизовані системи, моніторинг родовищ, сільське господарство, медицину та багато інших галузей, розширюючи можливості пристроїв *IoT* для бездротового зв'язку та обміну даними в умовах, коли важливі обмеження, такі як енергоефективність та ресурси, мають високий пріоритет.

Thread - це протокол для мереж на основі *IP*, спеціально розроблений для мереж Інтернету речей (*IoT*) та домашньої автоматизації. Він відзначається високою ефективністю та надійністю та призначений для побудови надійних та безпечних мереж *IoT*. *Thread* дозволяє призначати *IP*-адреси кожному підключеному пристрою, що робить його сумісним з існуючими *IP*-мережами.

Протокол оптимізований для пристроїв з обмеженими ресурсами та батарейками, забезпечуючи низьке споживання енергії та тривалий термін служби без заміни батарей. Він також включає в себе заходи безпеки на рівні мережі, такі як шифрування трафіку та ідентифікація пристроїв. Мережі *Thread* можуть легко

розширюватися за потреби, додаваючи нові пристрої та маршрутизатори. Протокол також підтримує множинні прошляхи для надійної доставки даних в мережі.

Thread знаходить застосування в різних галузях, включаючи домашню автоматизацію, контроль за промисловими процесами, моніторинг середовища та багато інших, де необхідно мати надійні та ефективні мережі *IoT*.

Ці протоколи та стандарти грають важливу роль у стандартизації та сприяють розвитку Інтернету речей. Вибір конкретного протоколу залежить від потреб вашого *IoT*-проекту та характеристик підключених пристроїв.

4.4 Забезпечення конфіденційності та приватності

Забезпечення конфіденційності та приватності в мережах Інтернету речей (*IoT*) - це важлива, але складна задача, яка постійно еволюціонує і стикається з різноманітними викликами. Враховуючи це, ось додаткові аспекти та сучасні тенденції в цій галузі:

Захист приватності та конфіденційності в мережах Інтернету речей (*IoT*) постійно розвивається, включаючи в себе розширені методи анонімізації даних. Ці методи дозволяють зберігати високий рівень конфіденційності, не обмежуючи корисність даних для аналітики та досліджень.

Одним із способів є диференційна приватність, де дані псевдонімізуються чи анонімізуються шляхом додавання випадкового шуму до реальних даних перед їх відправленням або обробкою. Це дозволяє зберігати індивідуальні дані в таємниці, але залишає можливість проводити аналіз на загальному рівні.

Техніки агрегації, такі як обчислення середніх значень чи інших агрегованих даних без розкриття окремих інформаційних пунктів, також допомагають зберегти приватність користувачів.

Забезпечення конфіденційності та приватності в умовах зростаючої кількості підключених пристроїв у мережах Інтернету речей (*IoT*) стає надзвичайно складною задачею. За останні роки спостерігається різке зростання кількості пристроїв, які збирають та обмінюються даними в мережах *IoT*. Цей масштаб вимагає

застосування розширених систем управління доступом та моніторингу для забезпечення конфіденційності та приватності.

Розширені системи управління доступом охоплюють важливі аспекти, такі як ідентифікація та аутентифікація користувачів та пристроїв. Вони вимагають вдосконалених методів перевірки прав доступу та управління привілеями. Це включає в себе використання багаторівневих систем аутентифікації, біометричних методів, паролів та двофакторної аутентифікації для забезпечення обмеженого та безпечного доступу до систем *IoT*.

Моніторинг систем виявлення вторгнень (*IDS*) та захисту від вторгнень (*IPS*) стає невід'ємною частиною забезпечення безпеки *IoT*. Вони надають змогу вчасно виявляти аномалії та атаки в мережах *IoT* і реагувати на них.

Децентралізована обробка даних - це ключовий аспект забезпечення конфіденційності та приватності в Інтернеті речей (*IoT*). Моделі, які передбачають обробку даних безпосередньо на пристроях (розподілене обчислення на рівні країв мережі), дозволяють зберігати більше контролю над даними та забезпечують конфіденційність, обробку та передачу на більш безпечних рівнях.

Це включає в себе локальну обробку даних на самому пристрої, що дозволяє зменшити обсяг даних, які потрібно передавати через мережу. Це підвищує захист конфіденційності, оскільки дані залишаються на пристрої та не покидають його кордони.

Децентралізована обробка даних також дозволяє застосовувати ефективні методи шифрування на рівні пристроїв, що забезпечує захист даних під час їх обробки. Вона також допомагає зменшити обсяг даних, які пересилаються через мережу, зменшуючи загрозу для конфіденційності та приватності.

З ростом *IoT* з'являється все більше підключених пристроїв, і забезпечення конфіденційності та приватності на такому масштабі вимагає розширених систем управління доступом та моніторингу. Децентралізована обробка даних також сприяє збільшенню надійності, оскільки пристрої можуть функціонувати навіть при відсутності підключення до центрального сервера або хмари.

Використання блокчейн-технологій для захисту приватності в мережах Інтернету речей (*IoT*) стає ключовим фактором у забезпеченні безпеки та довіри в цій сфері. Розробники впроваджують рішення, які дозволяють користувачам зберігати контроль над своїми особистими даними та надавати доступ до них лише за згодою.

Цей підхід включає децентралізований контроль, захист даних шляхом сильного шифрування, системи управління доступом на основі смарт-контрактів та можливість надавати чи відмовлятися від доступу до своїх даних через механізми згоди. Користувачі мають змогу визначати, кому, коли і як можна отримати доступ до їхніх особистих даних.

Застосування блокчейну також забезпечує відстеження даних і аудит, оскільки кожна дія з даними фіксується у розподіленому реєстрі. Це забезпечує велику прозорість та контроль над даними.

Регулююче середовище та законодавство в сфері захисту приватності стають все більш важливими в контексті мереж Інтернету речей (*IoT*). Заради захисту приватності користувачів та відвернення можливих загроз в цьому динамічному сегменті ринку з'являються нові регуляторні вимоги і законодавчі акти.

Один з найбільш впливових регуляторних документів є загальний регламент про захист даних (*GDPR*), що діє в Європейському Союзі. *GDPR* встановлює строгі вимоги до обробки особистих даних користувачів, включаючи дані, які можуть бути зібрані пристроями *IoT*. Це вимагає від компаній змінити свої підходи до збору та обробки даних, забезпечуючи більшу прозорість та контроль користувачів над їхніми особистими даними.

Поза *GDPR*, існують інші національні і регіональні ініціативи, що регулюють питання захисту даних у контексті *IoT*. Ці ініціативи включають в себе встановлення стандартів для захисту приватності та вимоги щодо повідомлення про порушення безпеки даних.

Регулююче середовище також враховує питання етики використання даних, особливо в галузях, де масовий збір і обробка даних *IoT* мають значний вплив на суспільство. Законодавство йде в ногу з розвитком цих технологій, впроваджуючи

нові правила та вимоги для захисту приватності та безпеки користувачів у світі зростаючого використання мереж *IoT*.

Етика та питання відкритого доступу до даних стають надзвичайно важливими в контексті розвитку Інтернету речей (*IoT*). Розуміння етичних аспектів збору та використання даних стає ключовим завданням для компаній та організацій, що займаються *IoT*.

Захист особистої приватності важливий, і компанії повинні розвивати етичні підходи до збору та збереження особистих даних, дотримуючись регуляторних вимог і забезпечуючи користувачам контроль над власними даними. Транспарентність та згода користувачів щодо збору та використання даних є необхідними етичними нормами.

Питання власності та контролю над даними користувачів важливі для забезпечення їхньої приватності. Користувачі мають право знати, кому належать їхні дані та мати контроль над ними.

Розробники *IoT* повинні визначити правила щодо власності даних та забезпечити можливість видаляти або передавати свої дані.

Соціальні та культурні аспекти також важливі, оскільки *IoT* може впливати на ці аспекти суспільства. Етичні питання можуть виникати в галузях, таких як медицина, де збір даних може стати джерелом моральних та етичних дискусій.

Відкритий доступ до даних може бути корисним для громадськості та дослідників, але водночас повинен супроводжуватися стандартами захисту приватності. Громадська обговореність щодо етики та приватності важлива і може впливати на регуляторні ініціативи та стандарти для забезпечення відповідального використання технологій *IoT*.

Розуміння та дотримання цих етичних аспектів є важливим завданням для компаній, що розробляють та впроваджують технології *IoT*. Ефективне врахування цих питань допоможе створити довіру користувачів і сприяти сталому розвитку Інтернету речей.

Забезпечення конфіденційності та приватності в мережах *IoT* залишається актуальною та складною проблемою, і вона продовжуватиме розвиватися з урахуванням сучасних викликів і технологічних можливостей.

4.5 Використання телекомунікаційних протоколів для забезпечення безпеки

Використання телекомунікаційних протоколів для забезпечення безпеки є одним із фундаментальних аспектів в глобальному інформаційному суспільстві. Спілкування через мережу та обмін даними стали важливою складовою нашого повсякденного життя, але разом із цим зросли загрози для конфіденційності, цілісності та доступності інформації. У цьому контексті телекомунікаційні протоколи стали ключовими інструментами для забезпечення безпеки у всіх сферах життя.

По-перше, вони використовують телекомунікаційні протоколи для забезпечення безпеки має різноманітні аспекти, однак, одним із найзначущих і фундаментальних є використання шифрування комунікаційного трафіку. Шифрування - це процес перетворення даних у нечитабельний вигляд, який може бути розшифрований лише за наявності відповідного ключа. Цей аспект безпеки грає вирішальну роль у забезпеченні конфіденційності даних, що передаються через мережу, та у захисті від потенційних загроз безпеці.

Протоколи шифрування, такі як *Transport Layer Security* (*TLS*) та *Datagram Transport Layer Security* (*DTLS*), використовуються для створення захищених тунелів для передачі даних. *TLS*, наприклад, широко використовується для безпечного обміну даними в Інтернеті та забезпечення конфіденційності веб-серфінгу, електронної пошти та багатьох інших онлайн-сервісів.

Завдяки шифруванню комунікаційного трафіку і використанню захищених протоколів, інформація залишається конфіденційною для несанкціонованих

користувачів та зловмисників. Даним чином, шифрування виконує роль надійної броні, яка перетворює будь-які надходячі дані в мовчазних свідків, недоступних для розголошення. Важливою особливістю цього підходу є те, що лише володіючи відповідним ключем, співрозмовники можуть відновити початковий, зрозумілий вигляд даних.

По-друге, телекомунікаційні протоколи в мережах Інтернету речей (*IoT*) виконують ключову роль у забезпеченні безпеки та захисту інфраструктури. Вони забезпечують аутентифікацію та авторизацію, що є критичними аспектами забезпечення безпеки мереж *IoT*.

Аутентифікація - це процес перевірки ідентичності користувача або пристрою, який намагається отримати доступ до мережі. Це важливо для того, щоб система можала розрізняти між вповноваженими користувачами та несанкціонованими суб'єктами. Аутентифікація використовує різні методи для перевірки ідентичності, такі як паролі, біометричні дані, токени та інші ідентифікатори.

Авторизація - це процес визначення дозволених дій або ресурсів для вповноважених користувачів або пристроїв. Вона визначає, які можливості доступу мають користувачі або пристрої після успішної аутентифікації. Наприклад, авторизація може визначати, які дані можуть бути зчитані або змінені, які функції можуть бути виконані і які ресурси можуть бути використані.

Ці процеси важливі для забезпечення того, що лише вповноважені користувачі та пристрої мають доступ до системи *IoT*. Вони допомагають уникнути несанкціонованого доступу, забезпечують конфіденційність і інтегрітет даних, а також гарантують, що ресурси системи використовуються згідно з встановленими правилами і обмеженнями. Таким чином, аутентифікація та авторизація є фундаментальними складовими безпеки мереж *IoT*.

По-третє, телекомунікаційні протоколи в мережах Інтернету речей (*IoT*) включають не лише засоби забезпечення комунікації, але й механізми для виявлення та реагування на потенційні вторгнення і загрози безпеці. Ці механізми включають в себе системи виявлення вторгнень (*IDS*) та захисту від вторгнень (*IPS*), які є надзвичайно важливими складовими для забезпечення безпеки в мережах *IoT*.

Системи виявлення вторгнень (*IDS*) призначені для моніторингу мережі на предмет аномалій та потенційних загроз. Вони використовують різноманітні методи, включаючи аналіз трафіку, виявлення незвичайної активності, та інші параметри, щоб ідентифікувати можливі вторгнення або аномалії в мережі. Коли *IDS* виявляє підозрілу активність, він генерує аларми або сповіщення, що дозволяє операторам мережі реагувати та вживати заходів для забезпечення безпеки.

Системи захисту від вторгнень (*IPS*), натомість, не лише виявляють потенційні загрози, але й намагаються їх призупинити або запобігти подальшим порушенням безпеки. Вони можуть автоматично реагувати на вторгнення, включаючи блокування підозрілих дій, відмову в доступі та інші заходи для захисту мережі та підключених пристроїв.

Ці механізми *IDS* та *IPS* грають критичну роль у забезпеченні безпеки *IoT*, оскільки дозволяють вчасно виявляти, реагувати та запобігати можливим загрозам. Вони надають операторам системи можливість дізнатися про події безпеки в реальному часі і приймати відповідні заходи для забезпечення надійності та захисту мережі *IoT*.

По-четверте, телекомунікаційні протоколи в мережах Інтернету речей (*IoT*) відіграють важливу роль у визначенні та впровадженні стандартів безпеки. Ці протоколи включають набір рекомендацій і вимог, що стосуються безпеки на різних рівнях мережі та пристроїв, включаючи захист на рівні пристроїв, апаратного забезпечення, інфраструктури мережі та програмного забезпечення.

Один із аспектів цього захисту полягає в шифруванні комунікаційного трафіку. Шифрування дозволяє перетворити дані в нечитабельний вигляд, який може бути розшифрований лише з використанням відповідного ключа. Це забезпечує конфіденційність даних, що передаються через мережу. Протоколи, такі як *Transport Layer Security* (*TLS*) та *Datagram Transport Layer Security* (*DTLS*), гарантують захист від несанкціонованого доступу та перехоплення даних.

Телекомунікаційні протоколи також включають механізми для аутентифікації та авторизації. Аутентифікація перевіряє ідентичність користувача або пристрою, який намагається отримати доступ до мережі, тим часом авторизація визначає, які

дії або ресурси можуть бути доступні цьому суб'єкту. Це важливо для забезпечення того, що лише вповноважені користувачі та пристрої мають доступ до системи. Безпека в мережах *IoT* також включає механізми для виявлення та реагування на вторгнення. Системи виявлення вторгнень (*IDS*) та захисту від вторгнень (*IPS*) надзвичайно важливі для вчасного виявлення аномалій та потенційних загроз безпеці. Вони надають можливість реагувати на вторгнення, призупиняти атаки та запобігати подальшим порушенням безпеки.

І, нарешті, телекомунікаційні протоколи і стандарти в мережах Інтернету речей (*IoT*) грають критичну роль у визначенні та впровадженні правил для управління конфіденційністю та приватністю користувачів. Ці правила включають в себе різні аспекти, що стосуються збору, збереження та обробки даних в мережі *IoT*.

Один із таких аспектів - це встановлення правил доступу, які регулюють, які користувачі або пристрої мають доступ до конкретних даних чи ресурсів. Телекомунікаційні протоколи дозволяють визначити, хто має право отримати доступ до певних даних та як цей доступ обмежується. Це забезпечує конфіденційність та обмежує можливість несанкціонованого доступу до цінних даних.

Додатково, обмеження доступу до особистих даних є важливим аспектом для забезпечення приватності користувачів. Телекомунікаційні протоколи допомагають визначити, які типи особистих даних можуть бути зібрані та як ці дані можуть бути використані. Це регулює збір, зберігання та обробку особистої інформації і забезпечує дотримання вимог до приватності користувачів.

Важливим аспектом є також етичне використання інформації. Телекомунікаційні протоколи і стандарти визначають етичні норми та обмеження для збору та використання даних. Це включає в себе уникнення недопустимого використання даних, яке може порушувати приватність користувачів або виводити їхні дані з контексту.

Усі ці аспекти телекомунікаційних протоколів об'єднуються, щоб забезпечити безпеку в світі, де спілкування та обмін даними стають все більш невід'ємною частиною нашого повсякденного життя. Забезпечення безпеки через

телекомунікаційні протоколи стає надзвичайно важливим завданням у динамічному цифровому світі.

Висновки за розділом

У розділі, присвяченому телекомунікаційним протоколам і стандартам в Інтернеті речей (*IoT*), ми розглянули важливий аспект забезпечення безпеки, конфіденційності та приватності в цьому швидкорозвиваючому сегменті технологічного світу. Використання телекомунікаційних протоколів в *IoT* є необхідністю для забезпечення надійної комунікації та обміну даними між підключеними пристроями.

Такі протоколи вирішують різні виклики безпеки, включаючи шифрування даних для забезпечення конфіденційності та інтегровані механізми для аутентифікації та авторизації, що визначають правила доступу до мережі та даних. Телекомунікаційні протоколи також дозволяють виявляти та реагувати на вторгнення, забезпечуючи негайне реагування на аномалії та потенційні загрози безпеці.

Важливо зазначити, що ці протоколи встановлюють не тільки технічні стандарти безпеки, але й правила для етичного та відповідного використання інформації, забезпечуючи приватність користувачів та враховуючи громадські обговорення щодо етики збору та використання даних.

У відсутності належного захисту та регулювання, ріст *IoT* може стати викликом для безпеки та приватності, тому телекомунікаційні протоколи і стандарти виступають як важливий інструмент для створення надійних та етичних мереж *IoT*. Забезпечення безпеки в мережах *IoT* відіграє вирішальну роль у їхньому успішному розвитку та прийнятті усім широким споживачам.

ВИСНОВКИ

У ході дослідження телекомунікаційних протоколів в мережах Інтернет речей було проведено аналіз та порівняння різних протоколів зв'язку, з'єднання та керування мережею. В результаті дослідження було отримано наступні висновки:

Особливості мереж Інтернет речей визначаються обмеженими ресурсами пристроїв, великою кількістю підключених пристроїв та різнорідністю додатків. Тому вибір ефективного телекомунікаційного протоколу має вирішальне значення для успішної роботи мережі.

Вивчений огляд основних телекомунікаційних протоколів показав, що існує широкий спектр протоколів, які використовуються для забезпечення зв'язку і передачі даних у мережах Інтернет речей. Вони включають *MQTT, CoAP, Zigbee, Z-Wave, Bluetooth, LoRaWAN* та *NB-IoT*, кожен з яких має свої унікальні характеристики та специфікації. Детальний аналіз особливостей та переваг кожного протоколу дав змогу з'ясувати, що кожен з них має свої сильні сторони та обмеження. Наприклад, *MQTT* є легким та ефективним для обміну повідомленнями, *CoAP* забезпечує можливість взаємодії з ресурсами пристроїв за допомогою *RESTful, Zigbee* та *Z-Wave* забезпечують низьке споживання енергії, а *LoRaWAN* має великий радіус покриття. Вибір протоколу залежить від конкретних вимог і характеристик проекту. Висвітлений огляд застосування телекомунікаційних протоколів в різних сферах, таких як розумні будинки, промисловість, здоров'я та інші, показав їх широкий потенціал. Кожен протокол має свої переваги в певних застосуваннях, і вибір оптимального протоколу допоможе забезпечити ефективне та стабільне функціонування мереж Інтернет речей у різних сценаріях.

Під час дослідження були виміряні споживання енергії, пропускна здатність та затримка передачі даних для кожного протоколу. Особливо велике значення має споживання енергії, оскільки більшість пристроїв в мережах Інтернет речей працюють на батареях, і ефективне використання енергії забезпечує довготривалу роботу мережі.

Під час порівняння протоколів за ефективністю, було виявлено, що деякі протоколи мають високу пропускну здатність, але можуть вимагати більше енергії, тоді як інші протоколи мають низьке споживання енергії, але меншу пропускну здатність.

Кожен з протоколів має свої специфічні застосування. Наприклад, *Zigbee* та *Z-Wave* підходять для розумних будинків, *NB-IoT* та *LoRaWAN* - для віддалених моніторингових систем та сільськогосподарських застосувань, *MQTT* та *CoAP* - для забезпечення комунікації між різними пристроями.

Bluetooth та *LoRaWAN* використовуються для короткодіапазонного та довгодального зв'язку відповідно, а *NB-IoT* є стандартом для мереж інтернет речей з низькою потужністю.

Огляд протоколів з'єднання з мережею показав, що *Wi-Fi, Ethernet, Bluetooth* та *Zigbee* є популярними протоколами, які забезпечують з'єднання між пристроями і мережами IP. *Wi-Fi* є широко використовуваним бездротовим протоколом з високою швидкістю передачі даних для домашніх мереж та офісних середовищ. *Ethernet* забезпечує надійне з'єднання по проводам і широко використовується в промислових системах та офісних мережах. *Bluetooth* є популярним для з'єднання близькорозташованих пристроїв, таких як навушники та розумні годинники. *Zigbee* забезпечує низькопотужне і надійне з'єднання для розумних будинків та індустріальних застосувань.

Детальний огляд протоколів керування мережею показав, що 6*LoWPAN* та *RPL* дозволяють підключати малопотужні пристрої до мереж Інтернет речей та забезпечують оптимальний механізм маршрутизації. *OMA DM* та *TR*-069 є протоколами для віддаленого управління та конфігурації пристроїв *IoT* у мережах. Враховуючи специфіку пр оекту, вибір певного протоколу керування мережею допоможе забезпечити ефективне та безперебійне функціонування мережі *IoT*.

Вибір оптимального телекомунікаційного протоколу має бути здійснений з урахуванням конкретних вимог та потреб додатків мережі Інтернет речей. Критичні фактори вибору включають споживання енергії, пропускну здатність, затримку, вартість та надійність.

У підсумку, дослідження телекомунікаційних протоколів в мережах Інтернет речей виявило, що кожен протокол має свої переваги та обмеження, і вибір оптимального протоколу залежить від конкретних вимог та характеристик мережі. Найбільш ефективним вибором для конкретного застосування може бути поєднання декількох протоколів, що дозволить досягти оптимального балансу між ефективністю та функціональністю мережі Інтернет речей.

Зокрема, для домашніх мереж розумних будинків можна використовувати протоколи *Zigbee* та *Z-Wave*, які забезпечують низьке споживання енергії та надійний зв'язок між різними розумними пристроями.

У віддалених моніторингових системах та сільськогосподарських застосуваннях, де великий радіус покриття є ключовим фактором, протоколи *LoRaWAN* та *NB-IoT* можуть бути найкращим вибором. Вони забезпечують ефективне використання енергії та мають здатність працювати в важкодоступних областях з обмеженим покриттям мережі.

Для мереж Інтернет речей, що потребують швидкої передачі даних та високої пропускної здатності, можуть бути використані протоколи *MQTT* та *CoAP*. Вони дозволяють забезпечити ефективний обмін інформацією між пристроями в реальному часі.

Крім того, деякі застосування можуть вимагати комбінації декількох протоколів, наприклад, протоколи *Thread* та 6*LoWPAN* можуть використовуватись разом для створення масштабованих та надійних мереж Інтернет речей з великим числом пристроїв.

Було розглянуто важливий аспект забезпечення безпеки, конфіденційності та приватності в цьому швидкорозвиваючому сегменті технологічного світу. Використання телекомунікаційних протоколів в *IoT* є необхідністю для забезпечення надійної комунікації та обміну даними між підключеними пристроями.

Такі протоколи вирішують різні виклики безпеки, включаючи шифрування даних для забезпечення конфіденційності та інтегровані механізми для аутентифікації та авторизації, що визначають правила доступу до мережі та даних. Телекомунікаційні протоколи також дозволяють виявляти та реагувати на

вторгнення, забезпечуючи негайне реагування на аномалії та потенційні загрози безпеці.

Важливо зазначити, що ці протоколи встановлюють не тільки технічні стандарти безпеки, але й правила для етичного та відповідного використання інформації, забезпечуючи приватність користувачів та враховуючи громадські обговорення щодо етики збору та використання даних.

Загалом, успішне впровадження мереж Інтернет речей залежить від правильного вибору телекомунікаційного протоколу або їх комбінації. Прийняття розумних рішень залежить від конкретних потреб і вимог проекту. Наявність різноманітних телекомунікаційних протоколів надає можливість адаптувати мережу Інтернет речей під різні сценарії та використання, забезпечуючи оптимальну продуктивність та ефективність. Важливо враховувати характеристики мережі, особливості додатків та вимоги до енергоефективності, щоб забезпечити найкращі результати та досягти успіху у реалізації проектів мереж Інтернет речей.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *A1tzori L. Understanding the Internet of Things*: *definition, potentials, and societal role of a fast evolving paradigm* / *L. Atzori, A. Lera, G. Morabito*. // *Ad Hoc Networks*. – 2017. – №56. – С. 121–140.

2. *An overview on wireless sensor networks technology and evolution*. *Sensors*. / *C.Buratti, A. Conti, D. Dardari, R. Verdone*. – *Basel*, 2009. – 869 с.

3. *Barry Haughian Design, Launch, and Sacle IoT Services*: *A Practical Business Approach* / *Barry Haughian* : *Apress*, 2018. – 292 *p*.

4. *Brian Goetz, Tim Peierls, Joshua Bloch*. *Java Concurrency in Practice*. 2006 432*p*

5. *Brian Russel Practical Internet of Things Security* / *Brian Russel, Drew Van Duren* : *Packt Publishing*, 2018. – 382 *p*.

6. *Charalampos D. Bringing IoT and Cloud Computing towards Pervasive Healthcare* / *D. Charalampos, M. Ilias*. // *Sixth International Conference on Innovative Mobile and Internet Service in Ubiquitous Computing*. – 2012. – С. 55– 98.

7. *Chen H. A BRIEF INTRODUCTION TO IOT GATEWAY* / *H. Chen, X. Jia, H. Li*. // *IET International Conference on Communication Technology and Application*. – 2011. – С. 54–98.

8. *Christian Bauer, Gary Gregory, Gavin King*. *Java Persistence with Hibernate Second Edition*. 2015 608*p*

9. *Claire Rowland User Experience Design for the Internet of Things* / *Claire Rowland* : *O'Reilly Media, Inc*., 2015.

10. *Communications System [*Електронний ресурс*]*. – 2019. – Режим доступу до ресурсу: *https*://*www.techopedia.com*/*definition*/18430/*communicationssystem*.

11. *Dac-Nhuong Le IoT*: *Security and Privacy Paradigm* / *Dac-Nhuong Le, Souvik Pal* : *CRC Press*, 2020. – 399 *p*.

12. *Demystifying Internet of Things Security*: *Design a security framework for an Internet connected ecosystem* / *Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler* : *Apress*, 2019. – 382 *p*.

13. *Eric Freeman, Elizabeth Robson*. *Head First Design Patterns*. 2004 694*p*

14. *Eui-Nam H. Fog Computing and Smart Gateway Based Communication for Cloud of Things* / *H. Eui-Nam, M. Aazam*. // *International Conference on Future Internet of Things ad Cloud*. – 2014. – С. 25–62.\

15. *Fei Hu Security and Privacy in Internet of Things* (*IoTs*): *Models, Algorithms, and Implementations* / *Fei Hu* : *CRC Press*, 2016. – 604 *p*.

16. *Gilad Rosner Privacy and the Internet of Things* / *Galid Rosnar* : *O'Reilly Media, Inc*., 2016.

17. *Goldsmith A. Wireless Communications* / *Goldsmith*. – *Cambridge*: *Cambridge University Press*, 2012. – 644 с.

18. *HTTP* протокол *[*Електронний ресурс*]* / 1 – Режим доступу до ресурсу: *https*:// *training.qatestlab.com*/*blog*/*technical-articles*/*http-protocol-what-and-where-to-test*/ *http*://*persona.pumb.ua*/*ua*/*club*/*digest*/*detail.php*?*CODE=internetveshchey-smozhet-li-smartfon-upravlyat-biznesom*.

19. *IoT Explained — How Does an IoT System Actually Work*? – Електронний ресурс*]* – Режим доступу: *https*://*medium.com*/*iotforall*/*iot-explained-how-does-an-iot-systemactually-work-e*90*e*2*c*435*fe*7

20. *IoT Security* / *Madhusanka Liyanage, An Braeken, Pardeep Kumar, Mika Ylianttila* : *Wiley*, 2020. – 304 *p*.

21. *ITU's Telecommunication Standardization Sector [*Електронний ресурс*]*. – 2020. – Режим доступу до ресурсу: *https*://*www.itu.int*/*dms_pub*/*itu-t*/*opb*/*gen*/*TGEN-OVW*-2014-*PDF-E.pdf*.

22. *MQTT – [*Електронний ресурс*]* – Режим доступу: *https*://*oxorona.com*/*mqtt*/

23. *MQTT Essentials*. *URL*: *https*://*www.hivemq.com*/*mqtt-essentials*/

24. *OT Gateway*: *Bridging Wireless Sensor Networks into Internet of Things* / *[Z. Qian, W. Ruicong, C. Qi* та ін.*]*. // *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*. – 2010. – С. 2–38.

25. *Practical IoT Hacking* / *Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods* : *No Starch Press*, 2021. – 434 *p*.

26. *Rakjumar Buyya Internet of Things* / *Rajkumar Buyya, Amir Vahid Dastjerdi* : *Morgan Kaufmann,* 2016. – 378 *p*.

27. *Robert C. Martin*. *Clean Code*. 2008 464*p*

28. *Rouse M*. *Internet of things* (*IoT*) / *Margaret Rouse*. – *New York*, 2019. – 624 с

29. *Sravani Bhattacharjee* / *Practical Industrial Internet of Things Security*: *A Practitioner's Guide to Securing Connected Industries* / *Sravani Bhattacharjee* : *Packt Publishing,* 2018. – 324 *p*.

30. *Weber R. Internet of things – Need for a new legal environment*? / *Rolf Weber*. // *Computer Law & Security Report*. – 2009. – №25. – С. 522–527.

31. *Xie Y*. Распространенные методы связи *IoT [*Електронний ресурс*]* / *Yong Xie*. – 2016. – Режим доступу до ресурсу: *https*://*www.cnblogs.com*/*legahero*/*p*/*IOT.html*.

32. Білявський Г.О, Бутченко Л.І., Навроцький В.М. Основи екології: Теорія і практикум: Навч. Посібник. Київ, 2002. 352 с.

33. Державний комітет ядерного регулювання України. Проект від 01.03.2008 р. Консультації щодо підвищення безпеки джерел іонізуючого випромінювання в Україні. Київ, 2008. 24 с. 3

34. Закон України «Про охорону праці» № 49, 1992. *URL*: *https*://*zakon.rada.gov.ua*/*laws*/*show*/2694-12 (дата звернення: 07.11.2019).

35. Інтернет речей: чи зможе смартфон управляти бізнесом? – Електронний ресурс*]* – Режим доступу:

36. Касьянов М. А., Васильчук М. В. Охорона праці користувачів ПК. Луганськ, видавництво СНУ ім. В. Даля. 2009. 101 с.

37. Маринець О. М., Мозговий А. М., Романовська Н. Г. Соціальна екологія: теоретичні аспекти: Методичні вказівки. Миколаїв, 2007. 28 с.

38. Мурашко В. О., Костенецький М. І., Рущак Л. В. Промислові радіаційні аварії з джерелами іонізуючого випромінювання, запобігання та порядок їх розслідування. Київ, 2013. 82 с.

39. Наказ Міністерства внутрішніх справ України «Про затвердження Правил пожежної безпеки в Україні» № 1417, 2014. *URL*: *https://zakon.rada.gov.ua/laws/show/z*0252-15 (дата звернення: 09.11.2019).

40. Наказ Міністерства соціальної політики України «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» № 207, 2018. *URL*: *https://zakon.rada.gov.ua/laws/show/z*0508-18 (дата звернення: 07.11.2019).

41. ПРОТОКОЛ ОБМЕЖЕНОГО ЗАСТОСУВАННЯ (*COAP*) – Електронний ресурс*]* – Режим доступу: *https://cqr.company/ua/wiki/protocols/constrained-application-protocol-coap/*

42. Функція *Wi-Fi Direct* – для чого вона потрібна і як використовується на Андроїд-пристроях – Електронний ресурс*]* – Режим доступу: *https://creativnost.com.ua/funkciya-wi-fi-direct-dlya-chogo-vona-potribna-i-yak-vikoristovuyetsya-na-andro%D1%97d-pristroyax/*

43. Що таке *IoT* простими словами? – Електронний ресурс*]* – Режим доступу: *https://www.atiko.com.ua/articles-ua/*

44. Що таке *Z-Wave*? – Електронний ресурс*]* – Режим доступу: *https://www.dusuniot.com/uk/blog/what-is-z-wave-and-what-it-can-bring-to-home-automation/*

45. Як налаштувати і користуватися технологією *WiFi Direct* – Електронний ресурс*]* – Режим доступу: *https://texnogid.biz.ua/wi-fi/iak-nalashtuvaty-i-korystuvatysia-tekhnolohiieiu-wifi-direct.html*