

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. __/1

ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»

протокол від 22.02.2022 р. № 8

КОНСПЕКТ ЛЕКЦІЙ з навчальної дисципліни «АРХІТЕКТУРА І ТЕХНОЛОГІЇ IoT»

для здобувачів вищої освіти освітнього рівня «магістр»
спеціальності 172 «Телекомунікації та радіотехніка»
освітньо-професійна програма «Телекомунікації та радіотехніка»
факультет інформаційно-комп'ютерних технологій
кафедра біомедичної інженерії та телекомунікацій

Схвалено на засіданні кафедри
біомедичної інженерії та
телекомунікацій
_____ 2022 р., протокол № ____

Завідувач кафедри
_____ Тетяна НІКІТЧУК

Розробник: к.т.н., доц. кафедри біомедичної інженерії та телекомунікацій
АНДРЕСВ Олександр

Житомир
2021 – 2022 н.р.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. __/2

Зміст

Вступ.....	3
1. Загальні принципи побудови IoT.....	4
1.1. Основні поняття та визначення IoT.....	4
1.2. Архітектура IoT.....	12
1.3. Технологія взаємодії з інтернет-речами.....	15
2. Загальні відомості про датчики.....	17
2.1. Основні характеристики датчиків.....	19
2.2. Класифікація та типи датчиків.....	22
3. Засоби ідентифікації.....	29
3.1. Класифікація способів ідентифікації об'єктів IoT.....	29
3.2. Оптичні ідентифікатори.....	31
3.3. Радіочастотна ідентифікація.....	34
3.4. Система позиціонування на базі RFID-технології.....	42
3.5. Комунікації малого радіусу дії NFC.....	44
4. Принципи побудови сенсорних мереж.....	48
4.1. Основні поняття сенсорних мереж.....	48
4.2. Базова архітектура сенсорної мережі.....	50
4.3. Загальні принципи M2M – комунікацій.....	57
4.4. Цифрові апаратні інтерфейси.....	60
5. Принципи побудови бездротових сенсорних мереж.....	65
5.1. Ієрархія мережевих технологій, що використовуються в IoT.....	65
5.2. Особливості реалізації бездротової сенсорної мережі.....	67
5.3. Стандарт IEEE 802.15.4.....	73
5.4. Стандарт ZigBee.....	75
5.5. Стандарт 6LoWPAN.....	80
5.6. Радіомодуль ISM діапазону частот NRF24L01.....	82
5.7. Технологія ESP-NOW для мікроконтролерів ESP8266 і ESP32.....	85
6. Технології передачі даних в IoT.....	86
6.1. Стандарт Z-Wave.....	86
6.2. Стандарт Bluetooth.....	88
6.3. Стандарт Wi-Fi.....	90
6.4. Технологія LPWAN.....	94
7. Топологія хмарних обчислень в IoT.....	102
7.1. Модель хмарних сервісів.....	102
7.2. Модель туманних сервісів.....	107
8. Принципи взаємодії інтернет речей із хмарними платформами.....	111
8.1. Протоколи відповіді на запит.....	112
8.2. Протоколи передачі повідомлень.....	120
8.3. Хмарні додатки IoT.....	123
Перелік літератури.....	128

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. __/3

Вступ

У повсякденному житті ми все частіше стикаємось з тим, що навколишні предмети забезпечуються мініатюрними ідентифікаційними та сенсорними пристроями. За наявності необхідних каналів зв'язку з ними можна не тільки відстежувати ці об'єкти у просторі та часі, але й керувати ними. Сукупність різноманітних датчиків, виконавчих пристроїв, об'єднаних у мережу за допомогою будь-яких доступних каналів зв'язку, що використовують різні протоколи взаємодії між собою та єдиний протокол доступу до глобальної мережі Інтернет отримали назву «інтернету речей». Останнім часом значного розвитку набули методи радіочастотної ідентифікації, комунікації малого радіусу дії та між машинні комунікації. Пристрої і компоненти, які раніше не були підключені до світової мережі, тепер мають можливість ділитися зібраною інформацією з зовнішнім світом. Інтегруючись із глобальною мережею Інтернет, бездротові сенсорні мережі, дозволяють забезпечити простий зв'язок як між різними технічними пристроями, так і з зовнішніми сервісами. Вже сьогодні використання розумних датчиків дозволяє підвищувати ефективність управління інфраструктурою міста та оптимізувати пасажиро перевезення. Отже інтернет речей здатен потенційно підвищити прибутковість виробництва і покращити якість життя.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 4

1. Загальні принципи побудови IoT

1.1. Основні поняття та визначення IoT

Ідея Інтернету речей сама по собі дуже проста. Уявімо, що всі навколишні предмети та пристрої (домашні прилади та начиння, одяг, продукти, автомобілі, промислове обладнання та ін.) забезпечені мініатюрними ідентифікаційними та сенсорними (чутливими) пристроями. Тоді за наявності необхідних каналів зв'язку з ними можна не тільки відстежувати ці об'єкти та їх параметри у просторі та часі, але й керувати ними. Концепція *IoT (Internet of Things)* та термін для неї вперше сформульовані засновником дослідницької групи Auto-ID при Массачусетському технологічному інституті *Кевіном Ештоном* у 1999 році на презентації для керівництва компанії Procter & Gamble. У презентації розповідалося про те, як всеосяжне використання радіочастотних міток RFID зможе змінити систему управління логістичними ланцюгами в компанії.

Офіційне визначення Інтернету речей наведено в Рекомендації сектора стандартизації телекомунікацій Міжнародного союзу електрозв'язку (МСЕ-Т) У.2060, згідно з яким *IoT – глобальна інфраструктура інформаційного суспільства, що забезпечує передові послуги за рахунок організації зв'язку між речами (фізичними або віртуальними) на основі існуючих та розвитку сумісних інформаційних та комунікаційних технологій*. Під «речами» (things) тут розуміється фізичний об'єкт (фізична річ) або об'єкт віртуального (інформаційного) світу (віртуальна річ, наприклад, мультимедійний контент або прикладна програма), які можуть бути ідентифіковані та об'єднані через комунікаційні мережі. Вважається, що *першу* у світі інтернет-річ створив один із батьків протоколу TCP/IP *Джон Ромкі* у 1990 році, коли він підключив до мережі свій тостер. Але тільки в 21 столітті у зв'язку з бурхливим розвитком інфокомунікаційних технологій сформувалася концепція IoT і набула свого практичного втілення.

Окрім поняття «річ», МСЕ-Т також використовує поняття «пристрій» (device), під яким розуміється частина обладнання з обов'язковими можливостями з комунікації та необов'язковими можливостями із сенсорингу/зондування, приведення в дію речі, збору, обробки та зберігання даних. При цьому провідну роль відіграють саме пристрої, які можуть збирати різну інформацію та поширювати її по комунікаційних мережах різними

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. __/5

способами: через шлюзи та через мережу; без шлюзів, але через мережу; безпосередньо між собою. Рекомендація Y.2060 визначає різне поєднання перерахованих способів з'єднань. Це вказує на те, що МСЕ-Т передбачає використання для IoT безлічі мережевих технологій – глобальних мереж, локальних мереж, бездротових само організованих (ad-hoc) та пористих (mesh) мереж. Зазначені мережі зв'язку переносять дані, зібрані пристроями, до відповідних програм, а також передають команди від програмних додатків до пристроїв (рис.1.1).

У найзагальнішому вигляді з інфокомунікаційної точки зору Інтернет речей можна записати у вигляді наступної символічної формули:

IoT = Сенсори (датчики) + Дані + Мережі + Послуги.

У загальному випадку під Інтернетом речей розуміється сукупність різноманітних приладів, датчиків, пристроїв, об'єднаних у мережу за допомогою будь-яких доступних каналів зв'язку, що використовують різні протоколи взаємодії між собою та єдиний протокол доступу до глобальної мережі.

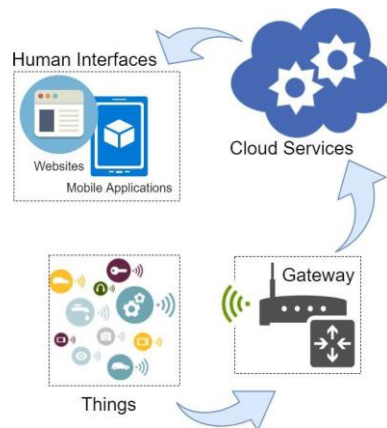


Рис. 1.1 – Чотири основні компоненти IoT

У ролі глобальної мережі для Інтернет-речей зараз використовується мережа Інтернет. Спільним протоколом є IP. Простіше кажучи, Інтернет речей – це глобальна мережа комп'ютерів, датчиків (сенсорів) та виконавчих пристроїв (актуаторів), що зв'язуються між собою з використанням протоколу IP (Internet

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___/6

Protocol). На основі Інтернету речей можуть бути реалізовані всілякі «розумні» (smart) додатки у різних сферах діяльності та життя людини (рис. 1.2).

«Розумна планета» – людина зможе буквально «тримати руку на пульсі» планети: своєчасно реагувати на упущення у плануванні господарств, забруднення та інші екологічні проблеми, а отже, ефективно розпоряджатися невідновлюваними ресурсами.

«Розумне місто» – міська інфраструктура та супутні муніципальні послуги, такі як освіта, охорона здоров'я, громадська безпека, ЖКГ, стануть більш пов'язаними та ефективними.

«Розумний будинок» – система розпізнаватиме конкретні ситуації, що відбуваються в будинку, та реагуватиме на них відповідним чином, що забезпечить мешканцям безпеку, комфорт та ресурсозбереження.

«Розумний транспорт» – переміщення пасажирів з однієї точки простору в іншу стане зручнішим, швидшим і безпечнішим.

«Розумна енергетика» – буде забезпечена надійна та якісна передача електричної енергії від джерела до приймача у потрібний час та у необхідній кількості.

«Розумна медицина» – лікарі та пацієнти зможуть отримати віддалений доступ до дорогого медичного обладнання або до електронної історії хвороби у будь-якому місці, буде реалізована система віддаленого моніторингу здоров'я, автоматизована видача лікарських засобів хворим та багато іншого.

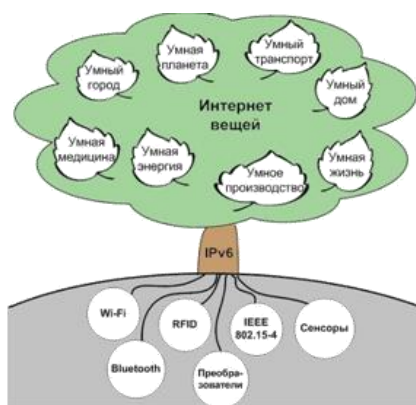


Рис. 1.2 – Розумні додатки на основі Інтернету речей

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 7

Очевидно, що із впровадженням Інтернету речей все наше повсякденне життя кардинально зміниться. Відійдуть у минуле пошуки потрібних речей, дефіцити товарів або їх надвиробництво, крадіжки автомобілів та мобільних телефонів, оскільки буде точно відомо, що, в якому місці та в якій кількості знаходиться, виробляється та споживається. Якщо всі об'єкти (речі) будуть забезпечені мініатюрними радіо мітками, їх можна буде дистанційно ідентифікувати, а за наявності певного «інтелекту» – і керувати ними.

Слід зазначити, що Інтернет речей не виключає участь людини. IoT не повністю автоматизує речі, оскільки він орієнтований на людину і надає можливість доступу до речей. Але багато речей зможуть поводитися інакше, ніж ми уявляємо собі сьогодні. У IoT кожна річ має свій унікальний ідентифікатор, який спільно утворює континуум речей, здатних взаємодіяти один з одним, створюючи тимчасові або постійні мережі. Так речі можуть брати участь у процесі їх переміщення, ділячись відомостями про поточну геопозицію, що дозволяє повністю автоматизувати процес логістики, а маючи вбудований інтелект, речі можуть змінювати свої властивості та адаптуватися до навколишнього середовища, у тому числі, для зменшення енергоспоживання.

З розвитком Інтернету речей все більше предметів підключатимуться до глобальної мережі, тим самим створюючи нові можливості у сфері безпеки, аналітики та управління, відкриваючи все нові та ширші перспективи та сприяючи підвищенню якості життя населення. Передбачається, що в майбутньому «речі» стануть активними учасниками бізнесу, інформаційних та соціальних процесів, де вони зможуть взаємодіяти та спілкуватися між собою, обмінюючись інформацією про навколишнє середовище, реагуючи та впливаючи на процеси, що відбуваються у навколишньому світі, без втручання людини.

Інтернет речей ґрунтується на трьох базових засадах. По-перше, розповсюджену комунікаційну інфраструктуру, по-друге, глобальну ідентифікацію кожного об'єкта і, по-третє, можливість кожного об'єкта надсилати та отримувати дані за допомогою персональної мережі або мережі Інтернет, до якої він підключений.

Найважливішими відмінностями Інтернету речей від існуючого інтернету людей є:

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___/8

фокусування на речах, а не на людині;
 значно більше підключених об'єктів;
 значно менші розміри об'єктів і низькі швидкості передачі;
 фокусування на зчитуванні інформації, а не на комунікаціях;
 необхідність створення нової інфраструктури та альтернативних стандартів.

У зв'язку з бурхливим розвитком мереж із пакетною комутацією і насамперед Інтернету на початку 2000-х років світове телекомунікаційне співтовариство спочатку виробило, а потім і розпочало реалізацію нової парадигми розвитку комунікацій – мереж наступного покоління NGN (Next Generation Networks). Технології NGN вже пройшли еволюційний шлях розвитку від гнучких комутаторів (Softswitch) до підсистем мультимедійного зв'язку IMS (IP Multimedia Subsystem) та бездротових мереж довготривалої еволюції LTE (Long Term Evolution). При цьому завжди передбачалося, що основними користувачами мереж NGN будуть люди і, отже, максимальна кількість абонентів у таких мереж завжди буде обмежена чисельністю населення планети Земля.

Проте останнім часом значного розвитку набули методи радіочастотної ідентифікації RFID (Radio Frequency IDentification), бездротові сенсорні мережі WSN (Wireless Sensor Network), комунікації малого радіусу дії NFC (Near Field Communication) та між машинні комунікації M2M (Machine-to-Machine), інтегруючись з Інтернет, дозволяють забезпечити простий зв'язок різних технічних пристроїв («речей»), число яких може бути величезним. За прогнозами компанії Cisco, ми неминуче перейдемо до «Всеохоплюючого Інтернету» (Internet of Everything, IoE), де всілякі неживі предмети почнуть враховувати контекст і користуватися ширшими обчислювальними ресурсами та сенсорними можливостями. Cisco визначає IoE як поєднання людей, процесів, даних речей, що підвищує цінність мережевих з'єднань до небувалого рівня (рис. 1.3).

IoE перетворює інформацію на конкретні дії, що створюють нові можливості, які розширюють досвід користувача та формують сприятливі умови для розвитку країн, компаній та користувачів.

Слід зазначити, що речі та пов'язані з ними пристрої можуть мати повноцінні керуючі процесори для обробки даних у вигляді «системи-на-

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арк. ___/9

кристалі», у тому числі з власною операційною системою, блоком сенсорингу/зондування навколишнього середовища та блоком комунікації.

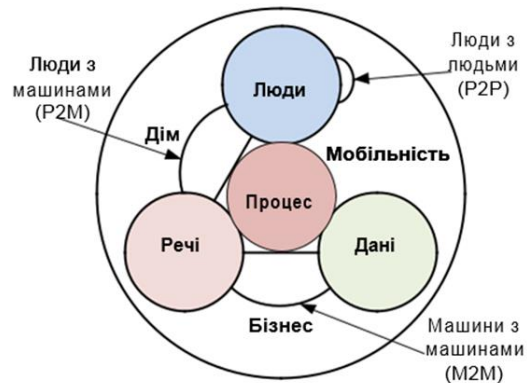


Рис. 1.3 - Всеохоплюючий Інтернет

Слід розрізняти поняття «Інтернет речей» та «інтернет-річ». Під «інтернет-річчю» розуміється будь-який пристрій, який:

має доступ до мережі Інтернет з метою передачі або запиту будь-яких даних;

має конкретну адресу в глобальній мережі або ідентифікатор, за яким можна здійснити зворотний зв'язок з річчю;

має інтерфейс взаємодії з користувачем.

Відмітимо основні *проблеми впровадження IoT*:

1. Відсутність єдиних стандартів для інтернету речей, що ускладнює можливість інтеграції запропонованих на ринку рішень та багато в чому стримує появу нових.

2. Інтернет-речі мають єдиний протокол взаємодії, за яким будь-який вузол мережі рівноправний у наданні своїх сервісів. На шляху переходу до здійснення ідеї Інтернету речей стояла проблема, пов'язана з протоколом IPv4, ресурс вільних мережевих адрес якого вже практично вичерпав себе. Однак підготовка до впровадження версії протоколу IPv6 дозволяє вирішити цю проблему і наближає ідею Інтернету речей до реальності. Складнощі переходу від IPv4 до нової версії мережного протоколу IPv6 пов'язані з потребою великих фінансових витрат з боку телекомунікаційних операторів та провайдерів послуг на модернізацію свого мережного обладнання.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 10

3. Проблема захисту даних у глобальних мережах та доступу до інформації, яка збирається «розумними речами» (відстеження місцезнаходження людей та їх власності).

4. Автономність всіх «розумними речами», тобто. датчики повинні навчитися отримувати енергію із навколишнього середовища, а не працювати від батарейок, як це відбувається зараз.

5. Необхідність зміни загальноприйнятих та перевірених бізнес-процесів та стратегій, що може призвести до значних фінансових витрат та ризиків.

Кожен вузол мережі інтернет-речей надає свій сервіс, надаючи якусь послугу постачання даних. У той же час, вузол такої мережі може приймати команди від будь-якого іншого вузла. Це означає, що всі інтернет-речі можуть взаємодіяти один з одним та вирішувати спільні обчислювальні завдання. Інтернет-речі можуть утворювати локальні мережі, об'єднані якоюсь однією зоною обслуговування або функцією.

У рекомендаціях MCE-T Y.2060 наведено еталонну модель IoT, яка дуже схожа на модель NGN, і включає чотири базові горизонтальні рівні (рис. 1.4):

рівень додатків IoT;

рівень підтримки додатків та послуг;

мережевий рівень;

рівень пристроїв.

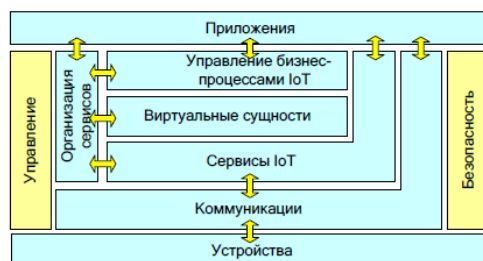


Рис. 1.4 – Еталонна модель IoT

Рівень додатків IoT у рекомендаціях детально не розглядається. Рівень підтримки послуг включає спільні можливості для різних об'єктів IoT з обробки та зберігання даних, а також можливості, необхідні для деяких програм IoT або груп таких програм. Мережевий рівень включає функції управління ресурсами мережі, доступу до мережі (авторизації, аутентифікації) та транспортні

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арк. ___ / 11

можливості, які полягають у забезпечення мережею передачі інформації додатків та послуг IoT. Нарешті, рівень пристроїв включає можливості пристрою та можливості шлюзу. Можливості пристрою передбачають прямий обмін із мережею зв'язку, обмін через шлюз, обмін через бездротову мережу, а також тимчасове зупинення та відновлення роботи пристрою для енергозбереження. Можливості шлюзу передбачають підтримку багатьох інтерфейсів для пристроїв (ZigBee, Bluetooth, WiFi та ін.) та для мереж доступу (2G/3G, LTE та ін.). Іншою можливістю шлюзу є підтримка конверсії протоколів, у разі, якщо протоколи інтерфейсів пристроїв і мереж відрізняються один від одного.

Існує також два вертикальні рівні – рівень управління та рівень безпеки, що охоплюють всі чотири горизонтальні рівні і забезпечують усунення наслідків відмов, зміну конфігурації, безпеку та дані для системи обліку наданих послуг та виставлення рахунків за них (білінгу). Основними об'єктами вертикального рівня управління є пристрої, локальні мережі та їх топологія, трафік та навантаження на мережу. Вертикальний рівень безпеки забезпечує авторизацію та аутентифікацію для кожного горизонтального рівня. Крім того, для рівня підтримки додатків та послуг розглядаються функції антивірусного захисту, тести цілісності даних, для мережного рівня – можливості захисту інформації протоколів сигналізації, а на рівні пристроїв – контроль доступу та конфіденційність даних.

Модель передачі даних в IoT відрізняється від існуючої моделі передачі даних через Інтернет (рис. 1.5).

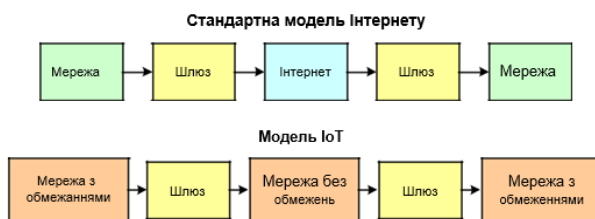


Рис. 1.5 – Порівняння моделей передачі даних в Інтернеті та IoT

У моделі архітектури IoT фігурують два важливі поняття. Мережа з обмеженнями характеризується відносно низькими швидкостями передачі менше 1 Мбіт (наприклад, стандарт IEEE 802.15.4) і досить високими

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арх. ___ / 12

затримками. Мережа без обмежень характеризується високими швидкостями передачі (десятки Мбіт/с і більше) і схожа на існуючу мережу Інтернет.

1.2. Архітектура IoT

Інтернет речей концептуально належить до мереж наступного покоління, тому його архітектура багато в чому схожа на відому чотиришарову архітектуру NGN. IoT складається з набору різних інфокомунікаційних технологій, що забезпечують функціонування Інтернету речей, та його архітектура показує, як ці технології пов'язані одна з одною. Архітектура IoT включає чотири функціональні рівні (рис. 1.6).

Рівень сенсорів та сенсорних мереж. Найнижчий рівень архітектури IoT складається з «розумних» (smart) об'єктів, інтегрованих з сенсорами (датчиками). Сенсори реалізують поєднання фізичного та віртуального (цифрового) світів, забезпечуючи збирання та обробку інформації в реальному масштабі часу. Мініатюризація, що призвела до скорочення фізичних розмірів апаратних сенсорів, дозволила інтегрувати їх безпосередньо в об'єкти фізичного світу. Існують різні типи сенсорів, наприклад, сенсори навколишнього середовища, сенсори для тіла, сенсори для побутової техніки, сенсори для транспортних засобів і т.і. Сенсори можуть мати невелику пам'ять, даючи можливість записувати деяку кількість результатів вимірювань. Сенсор може вимірювати фізичні параметри контрольованого об'єкта/явища та перетворювати їх на сигнал, який може бути прийнятий відповідним пристроєм. Більшість сенсорів вимагає з'єднання із шлюзом, який може бути реалізований з використанням локальної обчислювальної мережі LAN (Local Area Network), таких як Ethernet та Wi-Fi або персональної мережі PAN (Personal Area Network), таких як ZigBee, Bluetooth та ультра широкосмугового UWB, (Ultra-Wide Band) бездротового зв'язку на малих відстанях. Для сенсорів, які не потребують підключення до шлюзу, зв'язок із серверами/додатками може надаватися за допомогою глобальних бездротових мереж WAN, таких як GSM, GPRS та LTE. Сенсори, що характеризуються низьким енергоспоживанням та низькою швидкістю передачі даних, утворюють широко відомі бездротові сенсорні мережі WSN (Wireless Sensor Network). WSN набирають все більшої популярності, оскільки вони можуть містити набагато більше сенсорів з підтримкою роботи від батарей і охоплюють великі площі.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 13

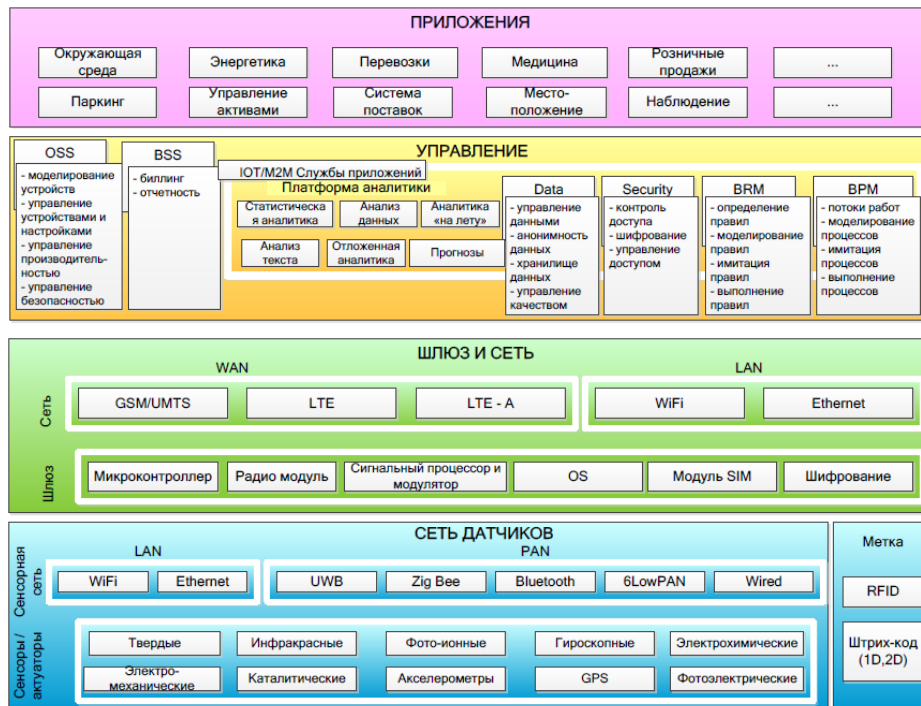


Рис. 1.6 – Архітектура IoT

Рівень шлюзів та мереж. Великий обсяг даних, створюваних на першому рівні IoT численними мініатюрними сенсорами, вимагає надійної та високопродуктивного транспортного середовища у вигляді провідної або бездротової мережної інфраструктури. Існуючі мережі зв'язку, що використовують різні протоколи, можуть бути використані для підтримки між машинних комунікацій M2M та їх додатків. Цей рівень складається з мережевої інфраструктури, що створюється шляхом інтеграції мереж різних технологій та протоколів доступу у єдину мережеву платформу в інтересах реалізації широкого спектру послуг та додатків в IoT. Ці мережі повинні забезпечувати необхідні значення якості передачі інформації - затримку, пропускну спроможність та безпеку.

Сервісний рівень містить набір інформаційних послуг, покликаних автоматизувати технологічні та бізнес операції в IoT, а саме: підтримка операційної та бізнес діяльності (OSS/BSS, Operation Support System/Business Support System), різна аналітична обробка інформації (статистичний,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 14

інтелектуальний аналіз даних та текстів, прогностична аналітика та ін.), зберігання даних, забезпечення інформаційної безпеки, управління бізнес-правилами (BRM, Business Rule Management), управління бізнес-процесами (BPM, Business Process Management) та ін.

Рівень додатків. На четвертому рівні архітектури IoT існують різні типи додатків для відповідних промислових секторів та сфер діяльності (енергетика, транспорт, торгівля, медицина, освіта та ін.).

Складовою частиною Інтернету речей є WEB of Things (WoT), який забезпечує взаємодію різних інтелектуальних об'єктів («речей») з використанням стандартів та механізмів Інтернету, таких як уніфікований ідентифікатор ресурсу URI (Uniform Resource Identifier), протокол передачі гіпертексту HTTP (HyperText Transfer Protocol), стиль побудови архітектури розподіленого додатку REST (Representational State Transfer) та ін. Фактично WoT передбачає реалізацію концепції IoT на прикладному рівні з використанням існуючих архітектурних рішень, орієнтованих на розробку web-додатків. Іншими словами, дані з розумних речей або управління ними мають бути доступним через WWW-сторінки.

Надзвичайно плідним може стати використання в IoT принципів і методів *когнітивності* (лат. *cognitio*, «пізнання, вивчення, усвідомлення») шляхом створення когнітивного Інтернету речей CIoT (Cognitive Internet of Things). При цьому об'єкт IoT має можливість самостійно визначати свій поточний стан і динамічно змінювати експлуатаційні параметри та режими роботи на користь оптимізації пропускнуєї спроможності мережі або інших показників.

Передбачається, що на практиці когнітивні інтернет-речі зможуть:

використовувати технології отримання знань про своє географічне середовище та місцезнаходження, наприклад, за допомогою стандартних технологій позиціонування GPS/ГЛОНАСС;

встановлювати самостійно або використовувати готові правила взаємодії між інтернет-речами;

динамічно та автономно коригувати свої робочі параметри відповідно до отриманих знань для досягнення заздалегідь визначених цілей, зокрема вибирати найбільш підходящу технологію передачі радіосигналу;

навчатися на основі досягнутих результатів з використанням кращих практик та найефективніших політик для досягнення цілей створення IoT.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 15

1.3. Технологія взаємодії з інтернет-речами

Використовують три способи взаємодії з інтернет-речами: прямий доступ, доступ через шлюз та доступ через сервер.

У разі *прямого доступу* інтернет-речі повинні мати власну IP-адресу або ім'я, за яким до них можна звернутися з будь-якої клієнтської програми і вони повинні виконувати функції веб-сервера. Інтерфейс з такими речами зазвичай виконаний у вигляді web-ресурсу з графічним інтерфейсом для керування за допомогою веб-браузера.

Якщо інтернет-речі не мають вбудованої підтримки протоколів IP та HTTP, а підтримують інші протоколи, наприклад, Bluetooth або ZigBee, то для взаємодії з ними можна використовувати спеціальний інтернет-шлюз, який перетворює зовнішні запити у формат запиту до специфічного API (англ. Application Programming Interface - інтерфейс прикладного програмування — це набір чітко визначених методів для взаємодії різних баз даних, апаратного забезпечення, програмних бібліотек і т.п.) пристрою, підключеного до цього шлюзу. Більшість стандартів бездротових сенсорних мереж не підтримують протокол IP, використовуючи власні протоколи взаємодії. Тому основна перевага використання інтернет-шлюзу в тому, що він може підтримувати кілька типів пристроїв, які використовують власні протоколи для зв'язку.

Третя форма взаємодії пристроїв в IoT через сервер передбачає наявність посередника між інтернет-речами та користувачем і може бути реалізована за допомогою посередницької платформи даних. Цей підхід передбачає наявність централізованого сервера або групи серверів, в основні функції яких входить:

прийом повідомлень від інтернет-речей та передача їх користувачам;

зберігання прийнятої інформації та її обробка;

забезпечення інтерфейсу користувача з можливістю двостороннього обміну між користувачем та інтернет-річчю.

Основною метою використання посередницьких платформ даних є спрощення пошуку, контролю, візуалізації та обміну даними з різними інтернет-речами. В основі цього підходу лежить централізоване сховище даних. Кожен пристрій, який має доступ до мережі Інтернет (прямий або через інтернет-шлюз), повинен бути зареєстрований у системі, перш ніж він зможе

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арх. ___ / 16

розпочати передачу даних. При цьому суттєво знижуються вимоги до продуктивності пристроїв, тому що від них не вимагається виконання функцій веб-сервера. Набір інструментів, що надаються платформами, значно спрощує розробку нових додатків для взаємодії та управління об'єктами WoT. Такий спосіб доступу є найбільш раціональним і часто використовується, оскільки дозволяє перенести навантаження обробки запитів користувачів з інтернет-речей на централізований сервер, тим самим розвантажуючи слабкий радіоканал зв'язку інтернет-речей, переносячи навантаження на канали зв'язку між сервером та користувачами.

Метод централізованого сервера також надає надійні засоби зберігання та обробки інформації, дозволяє інтернет-речам взаємодіяти один з одним та користуватися *хмарними обчисленнями*. Цей підхід може використовувати також метод шлюзу для з'єднання бездротових локальних мереж з сервером.

Шлюзи є засобом для об'єднання локальних мереж інтернет-речей з глобальною мережею та зв'язком з сервером управління або кінцевим користувачем. Оскільки локальні мережі інтернет-речей є в основному бездротовими сенсорними мережами, то шлюзи, що використовуються в інтернеті-речей, аналогічні використуванню у територіально-розподілених сенсорних мережах.

Існує кілька способів організації шлюзів. Перший спосіб полягає у використанні комп'ютерів, які мають точку доступу до глобальної мережі Інтернет, і кожна з мереж, що об'єднуються, підключена до такого комп'ютера. Основними недоліками такого підходу є вартість та громіздкість. Сенсорні мережі складаються з мініатюрних датчиків і повинні працювати автономно, проте територіально-розподілена сенсорна мережа при такому підході втрачає властивість автономності, оскільки вона залежить від наявності електрики і точки доступу в Інтернет на комп'ютері.

Другий спосіб полягає у використанні пристрою-шлюзу, що дозволяє з'єднати сенсорну мережу з найближчою провідною мережею, що має вихід в Інтернет. Такою провідною мережею, як правило, є мережа Ethernet. Пристрій має приймач, сумісний з сенсорною мережею, що об'єднується, порт для підключення до мережі Ethernet і мікроконтролер, що виконує функції перетворення пакетів однієї мережі в формат іншої. Такий спосіб відрізняється меншою вартістю, ніж перший і розмір такого пристрою невеликий, але він

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 17

потребує відносно високого енергоспоживання через те, що стандартні провідні мережі не розраховані на низький рівень сигналу та споживання енергії. Також такий пристрій не може гарантувати наявність точки доступу в найближчій дротовій мережі.

Третій спосіб полягає у використанні пристрою-шлюзу, який є повністю автономним і сам надає точку доступу до мережі Інтернет. Це можливо, якщо використовується бездротова технологія передачі даних. Пристрій складається з одного приймо - передавача, сумісного з сенсорною мережею і другого, що сумісний з тією чи іншою глобальною бездротовою мережею. Такими мережами можуть бути GSM або Wi-Fi. Існують також шлюзи, які надають доступ сенсорним мережам до найближчих мереж WiMAX для пошуку точки доступу до мережі Інтернет.

Таким чином, якщо необхідно організувати повністю автономну територіально-розподілену сенсорну мережу, слід використовувати третій спосіб. Якщо ж сенсорна мережа використовується як частина будь-якої великої провідної мережі, то немає потреби в її повній автономності і можливе використання перших двох способів.

2. Загальні відомості про датчики

Особливу роль в «Інтернеті речей» відіграють засоби вимірювання, що забезпечують перетворення відомостей про зовнішнє середовище в дані зрозумілі для ЕОМ, і тим самим здатні наповнити обчислювальне середовище цінною інформацією. Зараз використовується широкий клас засобів вимірювання, від елементарних датчиків (наприклад, температури, тиску, освітленості), приладів обліку споживання (таких, як інтелектуальні лічильники) до складних інтегрованих вимірювальних систем (рис.2.1). В рамках концепції IoT принциповим є об'єднання засобів вимірювання в мережі (такі, як бездротові сенсорні мережі, вимірювальні комплекси), за рахунок чого можлива побудова систем міжмашинної взаємодії.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 18



Рис.2.1- Датчики розумного будинку

Слід сказати, що на сьогоднішній день парадигма IoT ще тільки набирає обертів, однак досить давно існує область науки, що займається здійсненням вимірів на відстані, яка носить назву *телеметрія*. Телеметрія пов'язана з вимірюванням і передачею на відстань результатів вимірювань різних фізичних величин, більшість з яких є неелектричними. Вимірювання цих параметрів в основному здійснюється електричними методами. Як у телеметрії так і в IoT первинним джерелом інформації є датчик. Техніка конструювання і застосування датчиків (сенсорика), за останні роки розвилася у самостійну галузь вимірювальної техніки.

Датчиком називається інформаційний пристрій, що перетворює контрольований фізичний параметр в сигнал, зручний для подальшої обробки в каналі вимірювальної системи. Датчик (рис.2.2) включає в себе чутливий елемент і перетворювач неелектричних величин в електричні сигнали (ПНВЕС). Часто між чутливим елементом і перетворювачем включається підсилювач, необхідний для підвищення чутливості датчика.



Рис.2.2 - Будова найпростішого датчика

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 19

У відповідності з ГОСТ 16263-70, «Сенсор» це пристрій, що називається первинним вимірювальним перетворювачем (primary measuring transducer), його частина на яку безпосередньо діє вимірювана величина, – чутливим елементом (detector), а всі наступні складові вимірювального ланцюга – вимірювальним перетворюванням (measuring transducer).

Взагалі розрізняють три класи датчиків:

- аналогові датчики, тобто датчики, які виробляють аналоговий сигнал;
- цифрові датчики, що генерують на виході двійковий код вимірюємої величини;
- сигнальні (бінарні, двійкові) датчики, які виробляють сигнал тільки двох рівнів: (Low/ High).

Однак для «Інтернету Речей» можуть використовуватись лише цифрові та сигнальні датчики. При цьому будова датчика (рис. 2.3) дещо ускладнюється і він набуває певних «інтелектуальних» властивостей.



Рис.2.3 - Будова цифрового «інтелектуального» датчика

Електричний сигнал за допомогою АЦП перетворюється в цифровий код який може оброблятися та коректуватися мікроконтролером (часто АЦП входить до складу мікроконтролера) та за допомогою адаптера мережі пристосовуватись для передачі по Інтернету. Данні сигнального датчика можуть одразу ж передаватись через адаптер мережі. Важливим фактором для подальшої інтерпретації результатів вимірів є їх прив'язка до часу. Тобто доцільно разом з кодом вимірів фізичних процесів передавати і час їх виміру.

Інколи можливо чи доцільно організовувати вимірювальні системи (рис.2.4) коли один мікроконтролер обслуговує декілька датчиків. У цьому випадку передбачають адресне розділення кожного вимірювального елемента.

2.1. Основні характеристики датчиків

Перейдемо до розгляду деяких характеристик датчиків. Вище зазначалося, що датчик можна вважати перетворювачем вимірюваної величини $\lambda(t)$ у

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арк. ___ / 20

вихідний сигнал $s(t)$. У динамічному режимі $\lambda(t)$ і $s(t)$ безупинно змінюються, і зв'язок між ними визначається диференціальним рівнянням, отриманим на основі фізичного принципу і схеми датчика:

$$f_1[s^{(n)}, s^{(n-1)}, \dots, s] = f_2[\lambda^{(m)}, \lambda^{(m-1)}, \dots, \lambda].$$

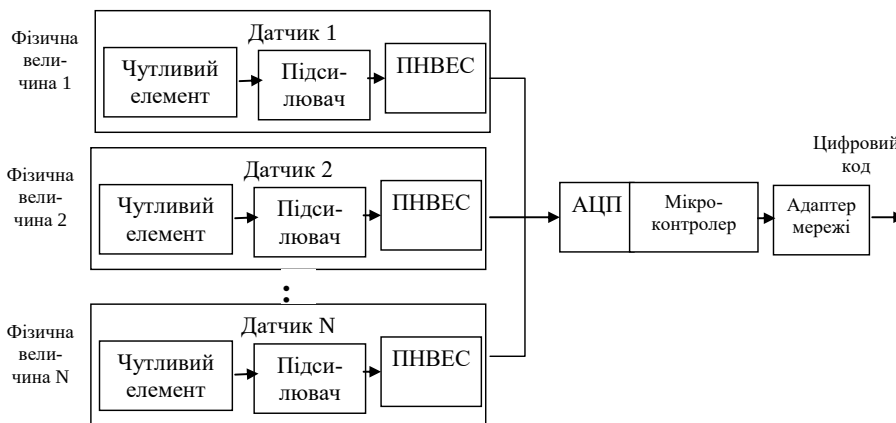


Рис. 2.4. – Багатоканальна вимірювальна схема

У сталому (статичному) режимі вимірювання всі похідні λ і S обертаються в нуль і диференціальне рівняння переходить в алгебраїчне рівняння, що визначає статичну характеристику датчика, $s = f(\lambda)$. Тому прийнято виділяти статичні і динамічні характеристики датчиків.

Статичні характеристики датчиків показують, наскільки коректно вихід датчика S відображає вимірювану величину λ через деякий час після її зміни, коли вихідний сигнал встановлюється у нове значення. Важливими статистичними параметрами є: *чутливість, роздільна здатність, лінійність, дрейф, робочий діапазон, повторюваність і відтворюваність результату.*

Статичну характеристику датчика прийнято називати *тарувальною* характеристикою. Вона може бути лінійною і нелінійною. Для зручності обробки інформації бажано мати лінійну характеристику $s = f(\lambda)$. Лінеаризація проводиться зазвичай шляхом введення спеціальної корекції в різні ланки датчика.

Чутливість датчика визначається як відношення величини зміни вихідного сигналу до одиничної зміни вхідної величини

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 21

$$s = \lim_{\Delta\lambda \rightarrow 0} \left(\frac{\Delta s}{\Delta\lambda} \right) = \frac{ds}{d\lambda}.$$

Роздільна здатність – це найменша зміна вимірюваної величини, котра може бути зафіксована і точно показана датчиком.

Точність визначає різницю між вимірюваною і дійсною величиною; вона може стосуватися датчика в цілому або конкретного його показника.

В процесі перетворення параметра λ в сигнал s виникають різні похибки, які складаються з методичних, динамічних та інструментальних похибок. У приладобудуванні точність датчиків оцінюють за допомогою приведеної відносної похибки, яка дорівнює відношенню абсолютної похибки до абсолютної величини діапазону вимірювання:

$$\varepsilon = \frac{\Delta\lambda}{L_\lambda} \quad \text{или} \quad \frac{\Delta s}{L_s}.$$

Лінійність не описується аналітично, а визначається виходячи з градаційної кривої датчика. Статична градаційна крива показує залежність вихідного сигналу від вхідного при стаціонарних умовах. Наближення цієї кривої до прямої лінії і визначає ступінь лінійності.

Статичне підсилення чи підсилення по постійному струму – це коефіцієнт підсилення датчика на дуже низьких частотах.

Дрейф визначається як відхилення показників датчика, коли вимірювана величина залишається постійною на протязі довготривалого моменту часу. Величина дрейфу може визначатися при нульовому, максимальному чи деякому проміжному значенні вхідного сигналу.

Деякі датчики через вплив сил тертя, люфтів і інших причин мають *зону нечутливості* (зону нульової чутливості). Для таких датчиків вводиться поняття порога чутливості, тобто мінімального збільшення параметра λ при якому сигнал s починає змінюватися.

Динамічну характеристику датчика можна експериментально отримати з реакції на стрибок вимірюваної вхідної величини. Параметри, що описують реакцію датчика, дають уяву про його швидкодію (наприклад, час нарощення,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ____ / 22

запізнювання, час досягнення першого максимуму), інерційних властивостей (час встановлення) і точності (зміщення).

Час проходження зони нечутливості – час між початком вимірювання фізичної величини і моментом реакції датчика, тобто моментом початку зміни вихідного сигналу.

Запізнювання – час, через який показання датчика перший раз досягають 50 % значення, що встановилося. В літературі зустрічаються і інші визначення запізнення.

Час нарощення – час, через який вихідний сигнал збільшується від 10 до 90% значення, що встановилося.

Час досягнення першого максимуму (peak time) – час досягнення першого максимуму вихідного сигналу.

2.2. Класифікація та типи датчиків

Залежно від методу перетворення неелектричних величин в електричні сигнали розрізняють параметричні й генераторні датчики. У параметричних датчиках зміна фізичної величини перетворюється в відповідну зміну будь-якого параметра електричного кола, що живиться від зовнішнього джерела. Такими параметрами зазвичай є опір, ємність або індуктивність. У генераторних датчиках відбувається безпосереднє перетворення фізичних величин в електричні сигнали без використання зовнішніх джерел живлення.

За характером вихідних електричних сигналів розрізняють датчики постійного і змінного струму. Перші іноді ототожнюють тільки з потенціометричними датчиками, хоча клас датчиків постійного струму значно ширше.

За способом подання інформації датчики діляться на аналогові і цифрові. В аналогових датчиках вихідний електричний сигнал є аналогом вимірюваної фізичної величини. Якщо параметр змінюється безперервно, то вихідний сигнал такого Датчика зазнає такі ж зміни. У цифрових датчиках при плавній зміні вхідної величини вихідний сигнал змінюється дискретно і представляється зазвичай у вигляді двійкового коду.

За видом отримуючої енергії: активні і пасивні перетворювачі. Пасивний отримує енергію від об'єкту дослідження (фотодіод). Активний – має зовнішнє живлення (фоторезистор).

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 23

За розмірністю у просторі: одиничні (точкові), одновимірні (розміщені вздовж однієї лінії, датчик фотоприймачів сканера), двовимірні (ПЗЗ – матриця цифрового фотоапарату), об’ємні (набір шарів датчиків, детектори космічних променів).

За фізичним принципом дії датчиків або за типом застосовуваних перетворювачів датчики діляться на: контактні (електромеханічні), резистивні, ємнісні, фотоелектричні, іонізаційні, п’єзоелектричні та ін. Електромеханічні перетворювачі мають механічний контакт, що керується зовнішнім впливом, наприклад, біметалічна пластинка. У резистивних датчиках змінюється опір при зміні температури, освітлення (терморезистори, фоторезистори), вологості, деформації. У ємнісних перетворювачах під дією вхідної величини змінюється ємність, що призводить до зміни напруги на виході датчика. Фотоелектричні перетворювачі (фотодіоди) засновані на явищі зовнішнього або внутрішнього фото ефекту. Робота іонізаційних перетворювачів базується на тому, що в газі, рідині або твердому тілі при дії іонізуючого випромінювання виникає струм іонізації між електродами. У електромагнітних перетворювачів генеруються електрорушійна сила при русі провідника у магнітному полі (мікрофон). Механічна деформація матеріалу приводить до виникнення напруги на виході п’єзоелектричних перетворювачів.

Датчики температури - це найбільш поширений тип датчиків. Вони застосовуються повсюдно: від інтелектуальних термостатів для холодних складів до охолоджувачів промислового обладнання. Термопара - це пристрій для вимірювання температури, якому не потрібно джерело живлення, тому що він саме генерує сигнал малої амплітуди (зазвичай мікрровольт). Термопара - це два провідника, виготовлені з двох різних матеріалів, з’єднані в точці вимірювання температури. На металевому електроді, в залежності від його температури, виникає електричний потенціал. У різних металів рівень цього потенціалу різний. Величина напруги залежить від властивостей вибраного металу. Термопари слід використовувати при виконанні не дуже відповідальних вимірювань, оскільки показання окремих термопар, при інших рівних умовах, можуть різнитися. Це викликано тим, що різні тонкі домішки, що входять до складу вимірювальних електродів, можуть призводити до невідповідності з довідковими таблицями. Термопари добре працюють в широкому діапазоні температур. Зазвичай подібні датчики використовуються в

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 24

промислових і високотемпературних середовищах при проведенні вимірювань в місцях, віддалених від оператора. *Резистивні датчики температури* (Resistance Temperature Detectors - RTD) працюють у вузькому діапазоні температур (нижче 600° С), але дозволяють виконувати вимірювання з більшою точністю, ніж термопари. Зазвичай вони виготовляються з дуже тонкого платинового дроту, щільно намотаного на керамічний або скляний сердечник. Електричний опір такої конструкції пропорційний її температурі. RTD виготовляються відповідно до прийнятих стандартів, в яких визначені допустимий діапазон і крок вимірів. Наприклад, для датчика 200 RT100 RTD крок вимірювань становить 0,00200 Ом / ° С, а діапазон вимірювань лежить в межах від 0 до 100 ° С. В межах цього діапазону залежність опору RTD від його температури зберігає лінійний характер. RTD рідко використовуються в діапазоні вище 600° С, що обмежує їх застосування в промисловості. *Термістор*- це теж датчик температури, електричний опір якого залежить від його температури. Цей тип датчиків забезпечує більш високу точність вимірювань в порівнянні з RTD. По суті, це терморезистори, але з дуже нелінійною залежністю опору від температури. Їх часто використовують у випадках, коли необхідна висока ступінь розрізнення вимірювань у вузькому діапазоні температур. Основна відмінність від RTD полягає в тому, що термістори виготовляються з кераміки або полімерів, тоді як основою RTD завжди є метал. Термістори знаходять застосування в медичному і науковому обладнанні, в харчовій промисловості, інкубаторах і в таких побутових приладах, як термостати. У табл. 2.1 наведені порівняльні характеристики різних типів датчиків температури.

Таблиця 2.1. - Зведена таблиця датчиків температури

Категория	Термопара	Резистивные датчики температуры	Термистор
Температурный диапазон (в °С)	От -180 до 2,320	От -200 до 500	От -90 до 130
Время реакции	Быстро (микросекунды)	Медленно (секунды)	Медленно (секунды)
Размеры	Большие (~10 мм)	Небольшие (~ 5 мм)	Небольшие (~ 5 мм)
Точность	Низкая	Средняя	Очень высокая

Фотоелектричні датчики використовуються в багатьох пристроях IoT для виявлення світла або визначення його інтенсивності. Такі пристрої необхідні, наприклад, в системах безпеки, інтелектуальних комутаторах або в системах

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 25

управління вуличним освітленням. Існує два типи таких датчиків, принцип дії яких зрозумілий з їх назви. *Фоторезистор* змінює опір в залежності від інтенсивності світла, а *фотодіод* перетворює світло в електричний струм. Фоторезистори виготовляються з напівпровідників з високим опором. Їх опір зменшується при збільшенні інтенсивності освітлення. У темряві опір фоторезистора може мати досить високий опір. Фотони, що поглинаються напівпровідником, переводять електрони в зону провідності, тим самим збільшуючи провідність матеріалу. Фоторезистори чутливі до довжини хвилі падаючого світла, тому їх типів і модифікацій існує величезна безліч. А ось фотодіоди - це повноцінні напівпровідникові прилади з р-п-переходом. Такі пристрої реагують на світло, створюючи електронно-діркову пару. Потік дірок, що рухаються до анода, і електронів, що рухаються до катода, створює електричний струм. Таким чином працюють традиційні сонячні батареї, що виробляють електрику під впливом сонячних променів.

Піроелектричний інфрачервоний (Pyroelectric Infrared – PIR) датчик руху дозволяє вловлювати рух. PIR датчики руху по суті складаються з чутливого піроелектричного елемента, який вловлює рівень інфрачервоного випромінювання. PIR датчики відмінно підходять для проектів, у яких необхідно визначати наявність або відсутність людини в межах певного робочого простору. Дуже часто використовуються у системах сигналізації. Крім перерахованих вище перевага подібних датчиків, вони мають велику зону чутливості. Піроелектричний датчик руху складається із двох основних частин. Кожна з частин включає спеціальний матеріал, чутливий до інфрачервоного випромінювання. Чутливі елементи датчика встановлюються в металевий герметичний корпус, який захищає від зовнішніх шумів, перепадів температур та вологості. Прямокутник у центрі виготовлений з матеріалу, який пропускає інфрачервоне випромінювання (зазвичай це матеріал на основі силікону). За цією пластиною встановлюються два чутливі елементи. PIR-датчики добре працюють в діапазоні хвиль від 8 до 14 мкм, цей діапазон характерний для випромінювань людського тіла. Діапазон чутливості до 6 метрів. Для забезпечення необхідного кута огляду 110 x 70 ° датчик забезпечений лінзою. При цьому лінза для датчика руху повинна бути маленька, тонка і виготовляється з пластику, хоча він і додає шумів у вимірювання. У більшості датчиків PIR використовуються лінзи Френеля (рис.2.5).

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 26



Рис. 2.5 - Типовий PIR-датчик з лінзою Френеля

Датчик фактично поділено на дві частини (рис.2.6). При цьому кожен із двох чутливих елементів має зону чутливості у вигляді великого прямокутника, в межах якого розташовується велика кількість маленьких зон чутливості. Для цього лінза поділяється на кілька секцій, кожна з яких являє собою окрему лінзу Френеля. Фактура окремих лінз відрізняється, у результаті і формується цілий набір чутливих ділянок, які взаємодіють між собою. Коли датчик перебуває у стані спокою, обидва сенсори визначають однакову кількість випромінювання. Наприклад, це може бути випромінювання приміщення чи навколишнього середовища на вулиці. Коли теплокровний об'єкт (людина чи тварина), проходить повз, він перетинає зону чутливості першого сенсора, у результаті чого на виході датчика генеруються два різні значення випромінювання. Коли людина залишає зону чутливості першого сенсора, значення вирівнюються. Саме зміни у показаннях двох датчиків реєструються та генерують на виході сигнал HIGH за наявності руху та сигнал LOW коли руху немає.

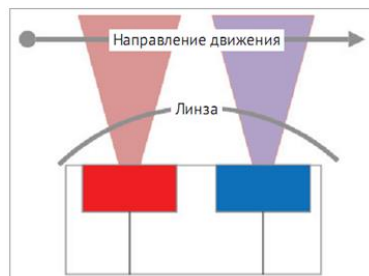


Рис. 2.6 - Датчик PIR

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 27

Детектор руху, температури, освітленості і вібрації FIBARO Motion Sensor (рис. 2.7,а) має діапазон чутливості PIR – датчика до 7 метрів, а похибка вимірювань температури складає $\pm 0.5^{\circ}\text{C}$ у діапазоні від 0 до $+40^{\circ}\text{C}$. Вартість ≈ 2000 грн. Для передачі даних використовуються малопотужні та мініатюрні радіочастотні модулі стандарту Z-Wave. Такі саме модулі використовуються також у датчику окису вуглецю Fibaro CO Sensor (рис. 2.7,б).

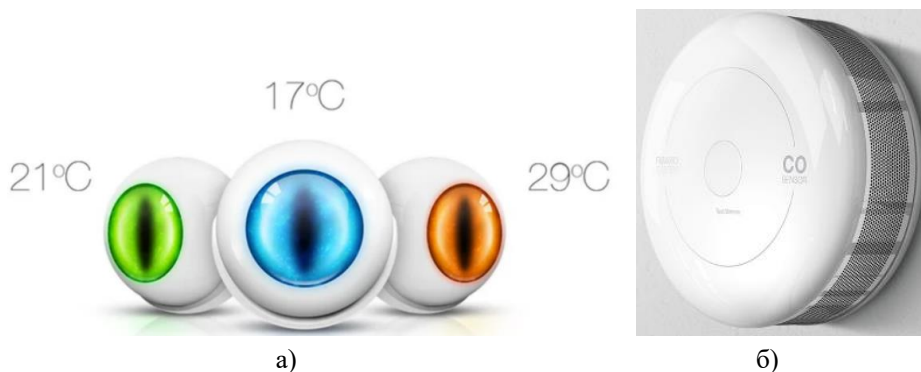


Рис. 2.7 - Датчик виробництва FIBARO

Бездротовий датчик температури та вологості Tervix Pro Line T&H (рис. 2.8) призначений для вимірювання та передачі отриманих даних іншим пристроям, що знаходяться в одній спільній мережі ZigBee. Вартість ≈ 1000 грн.



Рис. 2.8 - Датчик Tervix Pro Line ZigBee T&H

Датчики температури та вологості DHT11 та DHT22 (рис. 2.9) – досить відомі датчики для визначення відносної вологості та температури, складаються з емнісного датчика вологості та термістора. Також датчик містить в собі АЦП для перетворення аналогових значень вологості і температури. Основні характеристики датчиків наведені у табл. 2.2.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 28

Таблиця 2.2. - Характеристики датчиків температури

Параметри	DHT11	DHT22
Напруга живлення, В	3,...,5,5	
Споживаний струм, мА	0,1,...,2,5	0,05,...,2,5
Діапазон виміру вологості, %	20,...,95	0,...,100
Точність виміру вологості, %	5	2,..., 5
Діапазон виміру температури, °C	0,...,+50	- 40,...,+80
Точність виміру температури, °C	±2	±0.5
Частота вимірів	1Гц	0.5Гц
Розрядність	8 бит	16 бит
Вартість,грн	100	260

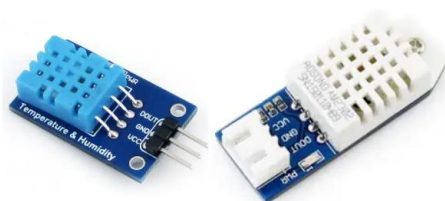


Рис. 2.9 - Датчики DHT11 та DHT22

Багатофункціональний пристрій Fibaro Door/Window Sensor (рис. 2.10,а) дозволить значно спростити процес контролю за будь-яким будинком або приміщенням. Сенсорний датчик здатний відстежити стан дверей та вікон. Датчик розбиття скла відстежує механічні та акустичні коливання, а датчик відкриття своєчасно сповістить про проникнення в приміщення. Такі датчики складаються з двох елементів, які спрацьовують при віддаленні один від одного. Він може працювати самостійно та поєднуватися з іншими пристроями. Налаштування відбувається через спеціальну програму, яка встановлюється на будь-який планшет або смартфон. Пристрій використовує бездротовий протокол Bluetooth. Розумний датчик відкриття дверей або вікна Orvibo SM10ZW (рис. 2.10,б), на відміну від попередника, для передачі даних використовує бездротовий стандарт ZigBee.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 29



а)



б)

Рис. 2.10 - Датчики відстежування стану дверей та вікон

Таким чином, датчики є основним джерелом даних і тому при реалізації бездротової сенсорної мережі від їх вибору залежить виконання задачі системою IoT в цілому.

3. Засоби ідентифікації

3.1. Класифікація способів ідентифікації об'єктів IoT

Залучення в «інтернеті речей» предметів фізичного світу, навіть не обов'язково оснащених засобами підключення до мереж передачі даних, вимагає застосування технологій ідентифікації цих предметів («речей»). Хоча поштовхом для появи концепції стала технологія RFID, але в якості таких технологій можуть використовуватися всі засоби, що застосовуються для автоматичної ідентифікації: оптично розпізнавані ідентифікатори (штрих-коди, Data Matrix, QR-коди). При всеосяжному поширенні «інтернету речей» принципово необхідно забезпечити унікальність ідентифікаторів об'єктів, що, в свою чергу, вимагає стандартизації.

Для об'єктів, безпосередньо підключених до мережі Інтернет, традиційний ідентифікатор - MAC-адреса мережевого адаптера, що дозволяє ідентифікувати пристрій на каналному рівні, при цьому діапазон доступних адрес практично невичерпний (2^{48} адрес в просторі MAC-48). Але використання ідентифікатора каналного рівня не дуже зручно для додатків. Ширші можливості по ідентифікації для таких пристроїв дає протокол IPv6, що забезпечує унікальними адресами мережевого рівня не менше 300 млн. пристроїв на одного жителя Землі.

Автоматична ідентифікація і збір даних (AIDC, від англ. Automatic Identification and Data Capture) загальний термін для методів автоматичної ідентифікації об'єктів, збору даних про них і обробку даних автоматичними і автоматизованими системами. Зазвичай до AIDC відносять такі технології:

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 30

контактні - магнітна карта, чіп-карта;

безконтактні - штрих код, QR-код, RFID, NFC, RTLS.

При проектуванні стандарту Ethernet було передбачено, що кожна мережева карта (так само як і вбудований мережевий інтерфейс) повинна мати унікальний шестибайтний номер (MAC-адресу), «прошитий» в ній при виготовленні. Цей номер використовується для ідентифікації відправника і одержувача фрейму. Передбачається, що при появі в мережі нового комп'ютера (або іншого пристрою, здатного працювати в мережі) адміністратору не доведеться налаштовувати MAC-адресу цього комп'ютера вручну.

MAC-адреса (від англ. Media Access Control - управління доступом до середовища) - унікальний ідентифікатор, який присвоюється кожній одиниці активного обладнання в комп'ютерних мережах Ethernet. Унікальність MAC-адрес досягається тим, що кожен виробник отримує в координаційному комітеті IEEE Registration Authority відповідний діапазон адрес і, в міру вичерпання виділених адрес, може запросити новий діапазон. Тому за трьома старшими байтами MAC-адреси можна визначити виробника. Існують таблиці, що дозволяють визначити виробника по MAC-адресі. У мережі Ethernet MAC-адреса дозволяє унікально ідентифікувати кожен вузол мережі і доставляти дані тільки цьому вузлу. Стандарти IEEE визначають 48-розрядний (6 октетів) MAC-адресу, який розділений на чотири частини (рис.3.1).

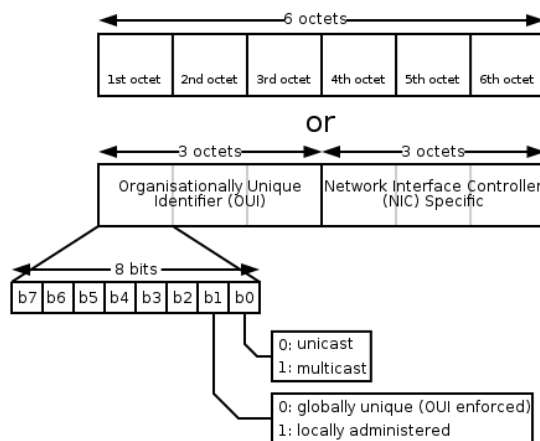


Рис. 3.1 - Структура MAC-адреси

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 31

Перші 3 октети містять 24-бітний унікальний ідентифікатор організації (OUI), або код MFG (Manufacturing, виробника), який виробник отримує в IEEE. При цьому, в найпершому октеті використовуються тільки 6 старших розрядів, а два молодших мають спеціальне призначення:

- нульовий біт - вказує: для одиночного (0) або групового (1) адресата призначений кадр;
- перший біт - вказує, чи є MAC-адреса глобально (0) або локально (1) адміністрованою.

Наступні три октети - вибираються виробником для кожного екземпляра пристрою.

Адміністратор мережі має можливість, замість використання «зашитого», призначити пристрою MAC-адресу на свій розсуд. Ознакою локально адміністрованої адреси є відповідний біт першого октету адреси.

Для того щоб дізнатися MAC-адресу мережевого пристрою, в Windows використовується команда «ipconfig /all».

3.2. Оптичні ідентифікатори

Штриховий код - графічна інформація, що наноситься на поверхню, маркування або упаковку виробів, що надає можливість зчитування її технічними засобами - послідовність чорних і білих смуг, або інших геометричних фігур. *Лінійними* (смуговими кодами) називаються штрих-коди, що читаються в одному напрямку (по горизонталі). Лінійні символики дозволяють кодувати невеликий об'єм інформації (рис 3.2).



Рис. 3.2 - Лінійний штрих-код

Двомірні коди були розроблені для кодування великого обсягу інформації. Розшифровка такого коду проводиться в двох вимірах (по горизонталі і по вертикалі). Двомірні коди поділяються на багаторівневі і матричні (matrix).

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 32

Багаторівневі штрих-коди являють собою поставлені один на одного кілька звичайних лінійних кодів. Матричні ж коди більш щільно упаковують інформаційні елементи по вертикалі. *DataMatrix* - двовимірний матричний штрих-код, який представляє собою чорно-білі елементи або елементи декількох різних ступенів яскравості, зазвичай у формі квадрата, розміщені в квадратній або прямокутній групі (рис.3.3).

Символи *DataMatrix* утворені з модулів, у вигляді періодичного масиву, розташованих в межах шаблону пошуку. Ними можна зашифрувати до 3116 кодів таблиці ASCII (включаючи надлишкову інформацію). Кожна область даних обмежена шаблоном пошуку і оточена з усіх чотирьох сторін межами вільної зони. Модулі можуть бути круглими або квадратними, конкретна форма стандартом не закріплена. За допомогою *DataMatrix* можна закодувати як текст, так і інші типи даних - веб-посилання, адреси електронної пошти, номери телефонів і SMS. Найчастіше в промисловості і торгівлі застосовуються бітові матриці, що кодують від декількох байт до 2 кілобайт даних.



Рис. 3.3 - Двовимірний матричний штрих-код

Data Matrix ECC 200 - це новітня версія *DataMatrix*, що використовує коди Ріда-Соломона для запобігання помилок і відновлення стертою інформації. ECC 200 робить можливим відновлення всієї послідовності закодованої інформації, коли символ містить 30% пошкоджень, припускаючи, що матриця все ще розташована в точності правильно. *DataMatrix* має частоту появи помилок менше, ніж 1 на 10 мільйонів відсканованих символів.

QR-код (англ. Quick Response Code - код швидкого реагування) - товарний знак типу матричних штрих-кодів, спочатку розроблених для автомобільної промисловості Японії. QR-код розроблений і представлений японською

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 33

компанією Denso-Wave в 1994 році. QR-код складається з чорних квадратів, розташованих у квадратній сітці на білому тлі, які можуть зчитуватися за допомогою пристроїв обробки зображень, таких як камера, і оброблятися з використанням кодів Ріда - Соломона з 8-бітовим кодовим словом. Є чотири рівня надмірності: 7, 15, 25 і 30%. Завдяки виправленню помилок вдається нанести на QR-код малюнок і все одно залишити його читаним (рис.3.4). Потім необхідні дані витягуються з шаблонів, які присутні в горизонтальних і вертикальних компонентах зображення. QR-код визначається датчиком або камерою як двовимірне зображення. Три квадрата в кутах зображення і менші квадратики по всьому коду дозволяють нормалізувати розмір зображення і його орієнтацію, а також кут, під яким датчик розташований до поверхні зображення. Точки переводяться в двійкові числа з перевіркою по контрольній сумі.



Рис. 3.4 - QR-код

Максимальна кількість символів, які поміщаються в один QR-код:
цифри десяткової системи числення (10 бітів на три цифри) - 7089 цифр;
цифри десяткової системи числення-10 цифр і букви- від А до Z (11 бітів на два символи) - до 4296 символів;
байти - 2953 (отже, близько 2953 літер кирилиці в кодуванні windows або близько 1450 літер кирилиці в utf-8);
ієрогліфи (13 бітів на ієрогліф) - 1817 ієрогліфів.

Основна перевага QR-коду - це легке розпізнавання скануючим обладнанням, що дає можливість використання в торгівлі, виробництві, логістиці. Найбільше визнання QR-код отримав серед користувачів мобільного зв'язку, які можуть моментально заносити в свій телефон текстову інформацію, додавати контакти в адресну книгу, переходити по web-посиланнях, відправляти SMS-повідомлення і т. д.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 34

3.3. Радіочастотна ідентифікація

Радіочастотна ідентифікація (Radio Frequency Identification- RFID) — це спосіб забезпечення зберігання та передачі інформації зі зручного носія-мітки в потрібне місце за допомогою спеціальних пристроїв. Такі мітки-ідентифікатори дозволяють полегшити розпізнавання різних об'єктів: товарів в магазині, рухомих засобів при транспортуванні, можуть ідентифікувати людей і тварин, не кажучи вже про широкі можливості ідентифікації документів і майна. Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом спеціальних міток, що несуть ідентифікаційну та іншу інформацію. Цей метод вже став основою побудови сучасних безконтактних інформаційних систем і має стійку назву RFID-технології.

Вперше пасивний пристрій на відбитій енергії був продемонстрований в 1971 році владі Нью-Йорка і іншим потенційним покупцям як пристрій з 16 бітами пам'яті для стягування мита на дорогах. Патент США Маріо Кардулло від 1973 «Пасивний радіопередавач з пам'яттю» був, по суті, прабатьком сучасної RFID-технології.

Перша демонстрація сучасних RFID-чипів, що працювали на ефекті зворотного розсіювання на частоті 915 МГц з 12 бітами пам'яті, як пасивних, так і активних, була проведена в дослідницькій лабораторії Лос Аламоса в 1973 році, а перший патент США, пов'язаний власне з назвою RFID, був виданий Чарльзу Уолтону в 1983 році.

RFID-мітка приймає від антени електромагнітну хвилю. Хвиля активізує її, і стають можливими як запис даних на мітку, так і зчитування даних з мітки. Антена може безперервно працювати і постійно зчитувати мітки у великій кількості, весь час опитуючи їх, або може включатися на деякий час за сигналом від оператора.

Антену з прийомо-передавачем і декодером часто знаходяться в одному загальному корпусі, щоб сигнал від антени відразу б демодулювався, розшифровувався і передавався через стандартний інтерфейс на ПК для подальшої обробки отриманих даних. Антени різних форм і розмірів можуть вбудовуватися в різні засоби для роботи з RFID-мітками, з метою забезпечення доступу до інформації, що зберігається в мітках товарів, предметів, людей, транспорту і т. д.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 35

На мітку інформація може бути записана різними способами, в залежності від конструкції мітки. Існують RFID-мітки, що можуть використовуватись тільки для читання (RO - Read Only), коли дані заносяться на стадії виготовлення мітки, і більше не змінюються. Другий тип міток WORM (Write Once Read Many) - для одноразового запису і подальшого багаторазового зчитування. У ці мітки на виробництві не заносять ніяких даних, а інформація записується користувачем один раз і потім може багаторазово зчитуватися. Мітки для багаторазового запису і подальшого багаторазового зчитування інформації - RW (Read/Write).

Пасивна RFID-мітка здатна працювати без власного джерела енергії, вона отримує енергію для живлення тільки від сигналу сканера. Такі мітки відрізняються довгим терміном експлуатації, мають менші розміри ніж активні, легше по вазі та дешевше у виробництві.

Активна мітка відрізняється наявністю джерела живлення (наприклад, літєва батарейка). Головна перевага активних міток це взаємодія із сканером на більшій відстані. До того ж активна мітка може рухатися з високою швидкістю через зону дії сканера і все одно встигне спрацювати.

Система радіо-ідентифікації складається з трьох основних компонентів: зчитувача "рідера", ідентифікатора ("транспондера" - мітки) та комп'ютерної системи опрацювання даних (рис. 3.5). Зчитувач має приймально-передавальний пристрій - він посилає сигнал до мітки та приймає сигнал відповіді від мітки.

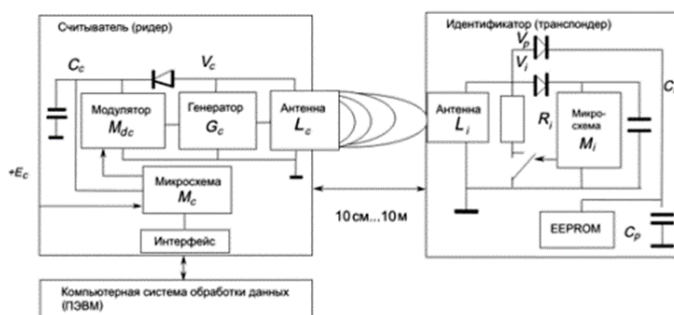


Рис. 3.5 – Система радіо-ідентифікації

Сама мітка зазвичай містить в собі антену, приймач, передавач, і пам'ять для зберігання даних. Все окрім антени поміщається в корпус маленької

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 36

мікросхеми — чипа, тому з вигляду може здатися що мітка складається лише з багатовиткової антени і чипа (рис. 3.6). Енергію мітка отримує з радіосигналу антени зчитувача або від власного джерела живлення. Після отримання зовнішнього сигналу мітка відповідає власним сигналом, у якому міститься певна ідентифікаційна інформація. Електричний струм, що наводиться в антені електромагнітним сигналом від зчитувача, забезпечує достатню потужність для функціонування чипа і передачі сигналу у відповідь.

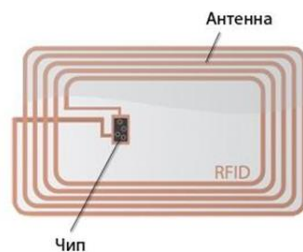


Рис. 3.6 - RFID-мітка

Переваги RFID-міток перед графічними ідентифікаторами полягають у тому, що штрих-код друкується один раз на стадії виробництва та упаковки, а інформація RFID-мітки може бути не тільки повністю змінена, але і доповнена. Мітки можуть зчитуватися відразу у великій кількості завдяки механізму виявлення колізії, чого важко досягти для графічних кодів.

Матричні коди здатні вміщати відносно великі обсяги даних, але їм потрібні великі площі для нанесення кодів, наприклад, щоб штрих-кодом записати 50 байт, знадобиться аркуш формату А4. У той же час як RFID-мітка з чіпом площею всього 1 квадратний сантиметр легко вмістить 1000 байт.

Графічні коди потрібно спочатку набирати, потім друкувати і наклеювати, та ще й зберегти цілісність зображення. З RFID-ідентифікаторами все простіше. На стадії виробництва RFID- мітка «імплантується» в упаковку (не обов'язково зовні), а потім безконтактним способом зчитати дані (не менше 1000000 взаємодій з антеною сканера).

Дані записані на мітку, цілком або частково, можна при необхідності захистити від зчитування або перезапису паролем — це надійний спосіб захисту від підробок. Зчитування відбувається при будь-якому положенні мітки в зоні дії сканера — це зручніше ніж графічний код, який потрібно рівно піднести до сканера.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 37

У RFID мітках використовуються такі діапазони частот:

1. Низькі частоти (НЧ) LF (Low Frequency) – до 135 кГц. Такі мітки краще за інших працюють поблизу рідин і металів, через що цей стандарт став особливо популярним у галузі розпізнавання тварин. НЧ мітки можуть зчитуватися з відстані кілька сантиметрів і мають найнижчу швидкість передачі даних. Пасивні мітки даного діапазону мають низькі ціни, проте у зв'язку з великою довжиною хвилі існують проблеми зі зчитуванням на великих відстанях, а також проблеми, пов'язані з появою колізій при зчитуванні.
2. Висока частота (ВЧ) HF (High Frequency) – 13,56 МГц. Мітки 13 МГц дешеві, не мають екологічних та ліцензійних проблем, добре стандартизовані, мають широку лінійку рішень, у них використовуються стандартизовані алгоритми шифрування. Широко застосовуються в таких областях, як картки контролю доступу, платіжні картки, боротьба з підробкою товарів, відстеження книг і т.д. ВЧ мітки можуть зчитуватися на відстані до 1м. Як і для діапазону LF, у систем, побудованих у HF-діапазоні, існують проблеми зі зчитуванням на великі відстані, зчитування в умовах високої вологості, за наявності металу, а також проблеми пов'язані з появою колізій при зчитуванні.
3. Надвисока частота UHF (Ultra High Frequency) – 433 МГц. Мітки даної частоти мають найбільшу дальність реєстрації, у багатьох стандартах даного діапазону присутні антиколізійні механізми. У UHF RFID-системах порівняно з LF та HF нижча вартість міток, при цьому вища вартість іншого обладнання. Активні мітки (радіомітки з елементами живлення) забезпечують максимальну дальність зчитування (до 1 км) та надійність зчитування (100%). Основним мінусом даних систем є вартість міток, що на порядок перевищує вартість пасивних UHF міток.
4. Надвисокі частоти (НВЧ) UHF (Ultra High Frequency) – діапазон 860-930 МГц. Найпопулярніший діапазон у сучасних RFID системах. UHF мітки можуть зчитуватися на відстані до 10 метрів і забезпечують швидкість передачі даних понад 128 кбіт/сек. Цей стандарт став основним у таких галузях, як логістика та управління ланцюжками поставок завдяки зусиллям світових лідерів у цій галузі (Walmart, Metro Group, Департамент оборони США та ін.).
5. Мікрохвильові частоти SHF (Super High Frequency) – 2,45-5,8 ГГц. Використовуються в таких галузях, як промислова автоматизація, електронний збір платежів та контроль доступу. Мають діапазон зчитування, який можна

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 38

порівняти з UHF (НВЧ), і більш високі швидкості передачі даних. Мітки, що використовуються, є в основному активними або напівактивними, що обмежує області їх застосування.

Особливості технології. RFID-міткам не потрібен контакт або пряма видимість, дані з пасивної мітки можуть бути отримані на порівняно невеликій відстані до кілька метрів (метро, офіси, банки, магазини). Активні мітки мають радіус зчитування до 300 м і здатні зберігати більший обсяг інформації. RFID-мітки можуть бути використані як для читання, так і для запису великого обсягу інформації, яка зчитується швидко і точно, що дозволяє виконувати велику кількість сканувань. RFID-мітки можна використовувати навіть в агресивних середовищах, через бруд, фарбу, пар, воду, пластмасу, деревину, а також імплантувати у живу тканину. Пасивні RFID-мітки мають фактично необмежений термін експлуатації, мають низьку собівартість.

Функції RFID-зчитувача (Рис. 3.7):

1. Енергопостачання пасивних міток за рахунок передачі енергії міткам з використанням електромагнітного поля.
2. Читання даних, що зберігаються на мітці.
3. Запис даних на мітку – використовуючи мітки з можливістю читання-запису, дані можна змінювати, додавати нові та видаляти старі, будь-коли протягом усього життєвого циклу продукту.
4. Зв'язок із комп'ютерною системою - зчитувач відповідає за транспортування інформації між мітками та комп'ютерною системою, це відбувається за допомогою порту Bluetooth, мережі Ethernet або інших дротових чи бездротових технологій.

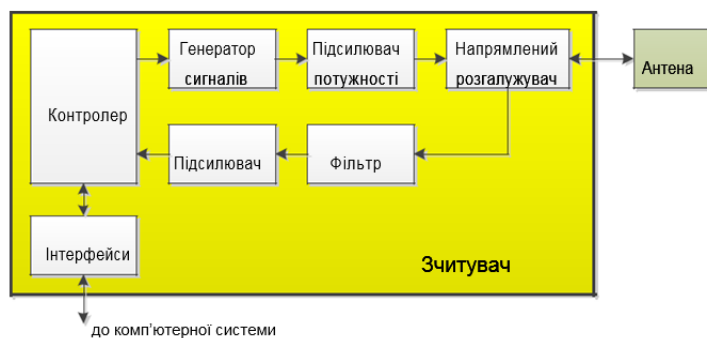


Рис. 3. 7 – Структурна схема RFID-зчитувача

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 39

Зчитувачі можуть бути стаціонарними та мобільними. Стаціонарні зчитувачі кріпляться нерухомо на стінах, дверях, рухомих складських пристроях. Вони можуть бути виконані у вигляді замка, вмонтовані в стіл або закріплені поряд з конвеєром на шляху проходження виробів. В порівнянні з мобільними, зчитувачі такого типу зазвичай мають більшу зону читання та потужність і здатні одночасно обробляти значний потік інформації. Стаціонарні зчитувачі на виробництві інтегруються в інформаційну систему, що дозволяє поетапно фіксувати переміщення маркованих об'єктів в реальному часі, або ідентифікувати положення мічених предметів в просторі. Мобільні зчитувачі мають порівняно меншу дальність дії і часто не мають постійного зв'язку з програмою контролю і обліку. Мобільні зчитувачі мають внутрішню пам'ять, в яку записуються дані з прочитаних міток (потім цю інформацію можна синхронізувати з системою обліку) і, як і стаціонарні зчитувачі, здатні записувати дані в мітку (наприклад, інформацію про проведений контроль).

Недоліки RFID-технології:

- мітку можна виявити на товарі і в багатьох випадках пошкодити або відірвати;
- мітки, можуть використовуватись для шпигунства без згоди власника товару;
- у випадку оплати товару картою банку є можливість асоціювання імені власника з товаром;
- технічно можливо збирати приватну інформацію, наприклад, з паспортів;
- RFID-мітки відносно легко ввести в оману. Для цього необхідно щоб мітка пройшла в радіусі дії несанкціонованого зчитувача, часто мобільного, який збереже інформацію з мітки у себе. Після цього достатньо прийти до точки доступу і транслювати зчитану інформацію системі за допомогою спеціального транслятора.

Типові застосування RFID-систем:

- електронний контроль за доступом і переміщеннями персоналу на території підприємств;
- керування виробництвом, товарними і митними складами, магазинами, переміщенням товарів і матеріальних цінностей, ідентифікація тварин в сільських господарствах;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 40

- автоматичний збір даних і при необхідності здійснення електронних платежів для усіх видів транспорту, включаючи організацію платних доріг, автоматичний збір плати за проїзд і транзит, платні автостоянки;
- контроль, планування і керування рухом, інтенсивністю трафіка і вибором оптимальних маршрутів;
- громадський транспорт — керування рухом, оплата проїзду й оптимізація пасажиропотоків;
- захист і сигналізація на транспортних засобах, забезпечення безпеки у комплексі з іншими технічними засобами.

Радіочастотна ідентифікація відноситься до ключових технологій майбутнього і є базовою технологією в Інтернеті речей. Ось лише кілька характерних прикладів застосування RFID у різних галузях людської діяльності.

Промисловість та сільське господарство. Технологія RFID забезпечує покращене управління складськими запасами та дозволяє значно підвищити ефективність логістичних процесів у промисловості. Наприклад, промислові компанії використовують RFID-систему для контролю за важливими комплектуючими, що переміщуються від одного цеху до іншого, що забезпечує автоматичний контроль, зменшення кількості помилок та витрат на пошук необхідних деталей на виробничій лінії.

Реалізовано проекти автоматизації заправки автотransпортних засобів та автоматичної ідентифікації автотransпорту з використанням технології RFID. Система забезпечує прозорий та достовірний облік палива при проведенні всіх технологічних операцій, відпуск палива лише авторизованим автомашинам за допомогою RFID-міток, ефективне планування та контроль споживання палива по кожній одиниці автомобільної техніки.

Щоб захистити свою продукцію від підробок, фармацевтичні підприємства розміщують транспондери на упаковках медикаментів. Завдяки цьому вдається відстежувати шляхи препаратів від виробника до аптеки.

У багатьох країнах фермери маркують велику рогату худобу за допомогою кріплення транспондерів на вухо тварини. Таким чином, при раптовому спалаху хвороби або епідемії стадо стає можливим швидко ізолювати.

Державні та громадські установи. Деякі бібліотеки впровадили RFID у свої системи книгообміну. При цьому в книгах, плівках і компакт-дисках

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 41

розміщуються транспондери. В результаті відвідувачі можуть самостійно оперативно отримувати вибрані ними носії інформації, причому транспондерами ці носії надійно захищені від крадіжки. Використання RFID-міток дозволяє автоматизувати процес видачі та повернення носіїв, ефективніше проводити інвентаризацію та захистити фонд від крадіжок. Крім того, квитки читачів також можна оснастити RFID-мітками, що дозволить боротися з їх підробками і підробками.

Лікарні також використовують радіочастотну ідентифікацію для того, щоб полегшити ідентифікацію пацієнтів та оптимізувати їхнє розміщення в палатах. Пацієнти забезпечуються ручними браслетами з інтегрованими в них транспондерами, у яких закодовано ім'я пацієнта та номер історії його хвороби, що зберігається в електронній базі даних. За допомогою мобільного комп'ютера з пристроєм, що зчитує, лікар отримує оперативний доступ до історій хвороби своїх пацієнтів.

Наука. Дослідники простежували за допомогою технології RFID життя бджіл. Крихітні чіпи приклеювалися на спинки комах. Отримана при цьому інформація про діяльність бджіл також допомагає ефективніше боротися з хворобами.

Вчені з допомогою технології RFID спостерігали зростання генетично змінених дерев. Ця система помітно перевершувала всі попередні методи маркування, оскільки транспондер, поміщений всередину дерева, захищений від впливу навколишнього середовища.

Побут та дозвілля. Споживачі вже сьогодні практично щодня стикаються із системами RFID. Наприклад, у багатьох країнах транспондери інтегруються до закордонних паспортів, а в деяких клубах — до членських карток.

Технологія RFID вже довго і успішно використовується як електронний ключ для керування доступом до приміщень. Перевага RFID-карти в порівнянні з магнітною картою в тому, що немає жодного контакту між картою та зчитувачем, вона менше зношується, менше додаткового обслуговування.

RFID технологія також завойовує популярність як зручний спосіб оплати різноманітних послуг. Один з популярних способів - оплата дорожнього мита без зупинки автомобіля. RFID також починає використовуватись як зручний спосіб оплати проїзду в автобусах, метро та поїздах. Багато міст у світі перейшли від карт з магнітною смугою до RFID-карт, оскільки це дозволяє

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 42

людям швидше проходити через турнікети, зменшує скупчення та прискорює обслуговування в касах.

RFID також використовується для охорони власності. Більшість сучасних автомобілів йде в комплекті з RFID-зчитувачем в рульовій колонці. Ретранслятор вставлений у пластмасу навколо основи ключа. Рідер повинен отримати посвідчення особи від ключа або автомобіль не заводитиметься.

Активні RFID-мітки можуть бути поєднані з датчиками тривоги: наприклад, якщо зброя на об'єктах переноситься без дозволу – лунає сигнал тривоги. RFID-мітки можуть бути в комп'ютерах з цінною інформацією: так файл не буде видалено без посвідчення особи та перевірки прав доступу.

Наведені приклади далеко ще не вичерпують перелік основних додатків, у яких застосування безконтактної ідентифікації не тільки зручно, а й економічно виправдано.

3.4. Система позиціонування на базі RFID-технології

Система позиціонування в режимі реального часу (Real-time Locating Systems - RTLS) - автоматизована система, що забезпечує ідентифікацію, визначення координат, відображення на плані місцезнаходження контрольованих об'єктів в межах території, охоплених необхідною інфраструктурою. RTLS накопичує, обробляє і зберігає інформацію про місцезнаходження і переміщення людей, предметів, мобільних механізмів і транспортних засобів з метою моніторингу технологічних і бізнес-процесів, сигналізації про відхилення від регламентів, а також з метою ретроспективного аналізу тих чи інших процесів і ситуацій.

До основних характеристик RTLS можна віднести:

точність позиціонування - точність визначення координат об'єкту, що контролюється. Для різних технологій RTLS характерна точність позиціонування становить від декількох десятків метрів (для WiFi) до декількох сантиметрів (для ультразвукових);

достовірність позиціонування - в реальних умовах точність позиціонування в значній мірі залежить від впливу перешкод і багатопроменевого загасання (відбитих сигналів), тому говорячи про точність позиціонування RTLS зазвичай вказують і вірогідну характеристику

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 43

достовірності. Наприклад, «точність позиціонування 1 метр з достовірністю 90%», тобто точність буде забезпечуватися в 90% вимірювань;

періодичність опитування - для забезпечення позиціонування в режимі реального часу проміжок часу між вимірами повинен бути таким, щоб об'єкт, рухаючись з характерною для нього швидкістю, встигав проходити відстань не більш подвоєною точності позиціонування. Наприклад, щоб забезпечити позиціонування в реальному часі з точністю один метр людини, що має характерну швидкість пересування 1,5 метра в секунду (5,4 км/год), виміри треба проводити з періодичністю не менше одного разу кожні 1,3 секунди. Це дозволяє будувати досить точні для практичних цілей траєкторії руху об'єкта навіть при різких змінах швидкості та напрямку руху;

надійність і живучість (здатність самовідновлюватися при виході з ладу будь-якого вузла);

малі габарити і вага, а також низьке енергоспоживання міток (з метою економії заряду акумуляторів).

До складу більшості типів RTLS зазвичай входять активна мітка та відповідна інфраструктура RTLS. Активна мітка - радіоелектронний пристрій, який прикріплюється до контрольованих об'єктів і взаємодіє зі зчитувачами RTLS. Інфраструктура RTLS - базові станції, мережа передачі даних і серверне програмне забезпечення. Базова станція – пристрій (зчитувач), який взаємодіє з мітками в процесі визначення координат останніх. Базові станції мають фіксовані координати, щодо яких визначаються координати міток. Базові станції розташовуються так, щоб в будь-якій точці контрольованої території мітка могла «бачити» мінімум три базові станції. Серверне програмне забезпечення керує процесом вимірювань, здійснює розрахунок координат об'єктів, обробку та накопичення даних. А також сигналізує про знаходження об'єктів в заданих або заборонених зонах, контролює рух об'єктів по заданих маршрутах або відхилення від них, порушення швидкісного режиму, відображає на екранах операторів місцезнаходження обраних об'єктів і траєкторії їх руху за заданий відрізок часу.

Мітки в RTLS позиціонуються щодо базових станцій з відомими координатами, при цьому вимірюються відстані або кути напрямку на БС (рис.3.8,3.9). Системою RTLS можуть контролюватися різні об'єкти - люди,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. / 44

обладнання, транспортні засоби, рухомі механізми, інструменти, вантажі, цінні і небезпечні предмети та ін.

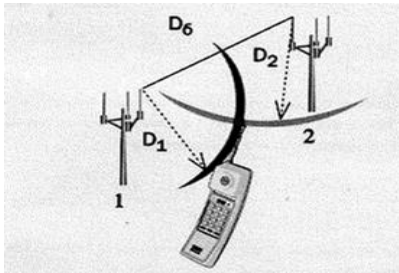


Рис.3.8 - Далекомірний метод

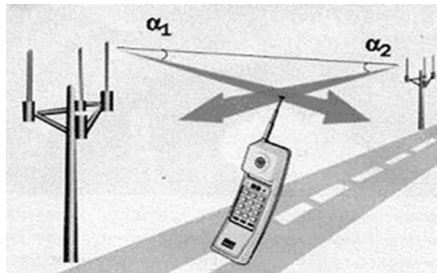


Рис.3.9 - Кутомірний метод

3.5. Комунікації малого радіусу дії NFC

Технологія зв'язку на малих відстанях NFC (Near Field Communication) – спільна розробка компаній NXP Semiconductor та Sony – є комбінацією кількох існуючих безконтактних технологій радіочастотної (РЧ) ідентифікації і зв'язку. Ця технологія – просте розширення стандарту безконтактних карток, що поєднує інтерфейс смарткарти та зчитувача в єдиний пристрій. Пристрій NFC може підтримувати зв'язок і з існуючими смарткартами, зчитувачами стандарту ISO 14443 та з іншими пристроями NFC і таким чином сумісний з існуючою інфраструктурою безконтактних карток, що вже використовується у громадському транспорті та платіжних системах. NFC націлена насамперед на використання в мобільних телефонах. Технологія NFC дозволяє обмінюватися різною інформацією, наприклад, номерами телефонів, картинками, музичними файлами або ключами цифрової авторизації між двома розташованими один до одного пристроями з підтримкою NFC. Це можуть бути будь-які портативні пристрої, а також смарт-карти або пристрої RFID. Ця технологія може використовуватися як ключ доступу до даних або сервісів, таких як безготівкова оплата або електронний замок.

Для використання сервісу NFC потрібен вбудований у мобільний телефон спеціальний модуль. Послуги з використанням технології NFC (як, втім, і багато інших у мобільному зв'язку та мережі Інтернет) передбачають наявність в апараті користувача деяких спеціальних функцій, що стосуються лише цієї групи послуг. Іншими словами, програми не можуть бути реалізовані звичайними засобами мереж зв'язку, а вимагають присутності в терміналі

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 45

користувача спеціальної програми, яка, з одного боку здійснює взаємодію за інтерфейсом NFC, а з іншого – використовує функцію підтримки додатків у мережному обладнанні. Частота роботи системи NFC – 13,56 МГц, швидкість передачі – 106 кбіт/с (можливі 212 кбіт/с та 424 кбіт/с) на відстані приблизно 10 см. На відміну від існуючих технологій безконтактного зв'язку на даному діапазоні частот, які дозволяють передавати інформацію тільки від активного пасивному пристрою, NFC забезпечує обмін між двома активними (рівноправними) пристроями. Таким чином, NFC можна використовувати для доступу до пристроїв радіочастотної ідентифікації RFID. В основі технології NFC лежить індуктивний зв'язок (рис. 3.10).



Рис.3.10 - Технологія NFC

За рахунок індуктивного зв'язку між пристроями, що опитують і прослуховують, пасивний пристрій впливає на активний. Зміна імпедансу пристрою, що прослуховує, викликає зміну амплітуди або фази напруги на антені опитувального пристрою, яке він виявляє. Цей механізм називається модуляцією навантаження. Вона виконується в режимі прослуховування із застосуванням допоміжної піднесучої 848 кГц. Залежно від стандарту, застосовується амплітудна (ASK-Amplitude Shift Keying) або фазова маніпуляція (BPSK). Характеристики режимів кодування та модуляції наведено в табл. 3.1. Використовується також пасивний режим, що здійснюється без допоміжної піднесучої з маніпуляцією ASK на частоті 13,56МГц. У пасивному режимі працюють мітки NFC, що призначені для обміну з активними NFC-пристроями. Як і мітки RFID, мітки NFC використовуються для зберігання невеликої кількості даних.

У модулі NFC є мікропроцесор, який забезпечує надійне зберігання сервісних додатків, криптографічний захист та підтримує три основні канали зв'язку:

– NFC для безконтактних транзакцій;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арх. ___ / 46

- інформаційний потік із TSM («Trusted Service Manager») через мережу мобільного оператора;
- обмін даними з користувачем через інтерфейс користувача – мобільний додаток телефону.

Таблиця 3.1- Режими роботи NFC

Стандарт	Тип пристрою	Кодування	Модуляція	Швидкість передачі, кбіт/с	Несуча, МГц
NFC-A	Опитування	Модифікований код Міллера	ASK 100%	106	13,56
	Прослуховування	Манчестер	Модуляція навантаження (ASK)	106	13,56 ± 848 кГц
NFC-B	Опитування	NRZ-L	ASK 100%	106	13,56
	Прослуховування	NRZ-L	Модуляція навантаження (BPSK)	106	13,56 ± 848 кГц
NFC-F	Опитування	Манчестер	ASK 100%	212/424	13,56
	Прослуховування	Манчестер	Модуляція навантаження (ASK)	212/424	13,56

Усього визначено 4 типи міток NFC (табл. 3.2). Технологія NFC призначена насамперед портативних пристроїв. Вона є логічним продовженням та розвитком технології RFID.

Таблиця 3.2 - Типи міток NFC

Тип мітки	1	2	3	4
Стандарт	14443 A	14443 B	JIS 6319-4	14443 A/B
Виробник	Innovision Topaz	NXP Mifare	Sony FeliCa	NXP DESFire, SmartMX-JCOP
Швидкість передачі, кбіт/с	106	106	212, 424	106, 212, 424
Об'єм пам'яті	96 байт	48 байт	до 1 Мбайта	до 32 кбайт
Захист від колізій	ні	так	так	так

Безперечна перевага NFC – простота використання. Для обміну інформацією необхідно піднести пристрої близько один до одного. Істотна

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 47

перевага NFC над технологією Bluetooth – більш короткий час встановлення з'єднання. Особливо велика область додатків, які можна отримати завдяки суміщенню технології NFC з можливостями мобільного зв'язку. Це і різні схеми електронної комерції (включаючи продаж та контроль квитків на транспорті, на видовищних заходах тощо), та різноманітні платні та безкоштовні довідково-інформаційні послуги, реклама, дистанційні системи контролю, електронні гроші, посвідчення особи, мобільна торгівля, електронні ключі тощо. Мобільні телефони можуть використовуватися для отримання по мережі мобільного зв'язку якогось контенту, який потім передається через інтерфейс NFC на стаціонарні термінали, забезпечені відповідним інтерфейсом, наприклад, текст - на принтер, відеокліпи - на телевізор і т.д.

Деякі стандартні сфери використання технології:

оплата за допомогою мобільного телефону - купівля квитків або оплата таксі, робота з платіжними системами;

телефон як електронний ключ - контроль доступу до приміщень, автомобіля, до глобальних мереж або блокування Bluetooth;

передача та доступ до даних - завантаження розкладів з електронного табло, завантаження карт, зчитування навігаційних координат;

зберігання електронних квитків на мобільному телефоні.

Споживча суть технології NFC стосовно мобільної комерції, що привертає сьогодні найбільшу увагу фахівців, полягає у можливості розміщення постачальником товарів/послуг/інформації множини порівняно простих та дешевих пристроїв з інтерфейсом NFC (міток) у місцях, зручних для бізнесу постачальника. Мітки можуть використовуватись самостійно або як додаток до платіжного терміналу або іншого пристрою. При піднесенні телефону, забезпеченого інтерфейсом NFC, до мітки активується обмін інформацією між міткою та телефоном, внаслідок чого програмний додаток, записаний у телефонному апараті, без участі абонента взаємодіє з інформаційною системою постачальника (рис.3.11). Все різноманіття можливих послуг NFC через оператора мобільного зв'язку укладається в рамки наступних основних сценаріїв:

- запит та отримання безкоштовної інформації будь-яким користувачем;
- запит та отримання безкоштовної інформації авторизованим користувачем;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 48

- запит платної послуги з відстроченим її отриманням (наприклад, придбання електронного квитка);
- запит та негайне отримання платної послуги (прохід через турнікет).

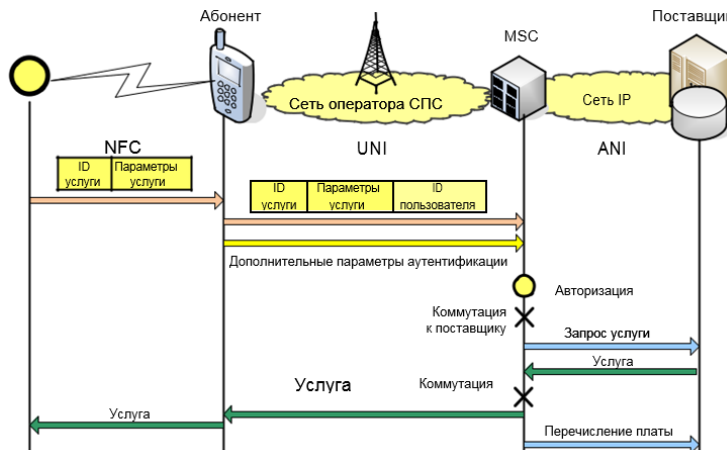


Рис.3.11 - Сценарій запиту та отримання платної послуги за допомогою NFC

Інтерфейс NFC на рівні програм повинен як мінімум забезпечувати передачу ідентифікатора послуги та, якщо потрібно, параметри послуги. Інформація, отримана від мітки, передається до центру комутації мобільного зв'язку (MSC), де має бути перевірена допустимість запитаної послуги для цього абонента. На основі ідентифікатора (ID) послуги визначається адреса, за якою надсилається запит постачальнику послуги. У відповідь постачальник надсилає відповідний контент, який після виконання MSC контрольних процедур надсилається абоненту.

4. Принципи побудови сенсорних мереж

4.1 Основні поняття сенсорних мереж

Сенсор – пристрій, який приймає контрольований вплив (світло, тиск, температуру тощо. п.), вимірює його кількісні та якісні характеристики і перетворює дані виміру у сигнал. Сигнал може бути електричним, хімічним або іншим типом.

Датчик – пристрій, який використовується для перетворення одного виду енергії в інший. Отже, сенсор також є датчиком, який перетворює фізичну інформацію на електричну, яка може бути передана обчислювальній системі або контролеру для обробки.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арх. ___ / 49

Актuator – виконавчий пристрій, який реагує на сигнал, що надійшов, для зміни стану керованого об'єкта. В актуаторі відбувається перетворення типів енергії, наприклад, електрична енергія, або енергія стисненого (розрідженого) повітря (рідини, твердого тіла) перетворюється на механічну.

Сенсорний вузол – це пристрій, який складається, принаймні, з одного сенсора (може також включати один або кілька актуаторів), і має обчислювальні та провідні або бездротові мережеві можливості.

Сенсорна мережа – система розподілених сенсорних вузлів, що взаємодіють між собою, а також з іншими мережами для запитів, обробки, передачі та надання інформації, отриманої від об'єктів реального фізичного світу з метою вироблення реакції на цю інформацію. Таким чином, сенсорна мережа включає як мінімум сенсори, актуатори і комунікаційні вузли. Основною сферою застосування сенсорної мережі є контроль та моніторинг вимірюваних параметрів фізичних середовищ та об'єктів та в деяких випадках – управління цими об'єктами (активація в них певних процесів) (рис. 4.1).

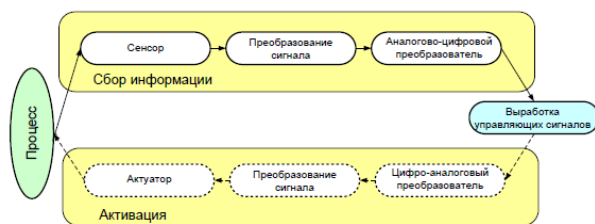


Рис. 4.1 – Збір даних та управління в сенсорних мережах

Область покриття сенсорної мережі може становити від кількох метрів до кількох кілометрів за рахунок можливості ретрансляції повідомлень від одного елемента мережі до іншого. Сенсорна мережа має здатність до ретрансляції повідомлень ланцюжком від одного вузла до іншого, що дозволяє у разі виходу з ладу одного з вузлів організувати передачу інформації через сусідні вузли без втрати якості. Сама мережа визначає оптимальний маршрут руху інформаційних потоків (рис. 4.2).

Мережа зв'язку, що самоорганізується (лат. ad hoc – «для конкретного випадку») – мережа, у якій число вузлів є випадковою величиною у часі може змінюватися від 0 до деякого максимального значення. Взаємозв'язки між

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 50

вузлами в такій мережі також випадкові в часі і утворюються для передачі інформації між подібними вузлами і в зовнішню мережу зв'язку.

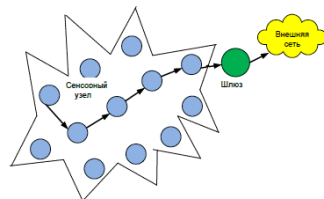


Рис. 4.2 – Маршрутизація інформації в сенсорній мережі

Бездротова сенсорна мережа (БСМ) (англ. WSN – Wireless Sensor Network) – розподілена сенсорна мережа, що містить безліч сенсорів і виконавчих пристроїв, об'єднаних між собою за допомогою радіоканалів.

4.2. Базова архітектура сенсорної мережі

Дослідницька група з сенсорних мереж SGSN (Study Group on Sensor Networks) визначила базову архітектуру сенсорної мережі та її основні інтерфейси.

Типова архітектура сенсорної мережі включає три типи вузлів (рис. 4.3):

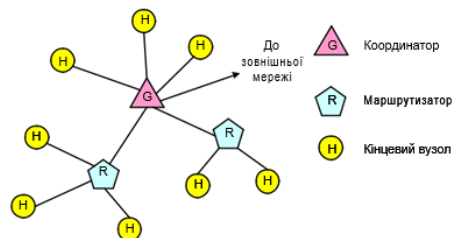


Рис. 4.3 - Типи вузлів сенсорної мережі

Координатор – здійснює глобальну координацію, організацію та встановлення параметрів мережі, є найскладнішим пристроєм, що потребує найбільшого обсягу пам'яті та найбільшої потужності джерела живлення. В одній мережі повинен бути присутнім лише один координатор. З координатора здійснюється вихід у зовнішню мережу (він реалізує функцію шлюзу – gateway).

Координатор виконує такі функції:

Додано примітку [АО1]:

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 51

визначає незадіяні канали з переліку каналів, доступних для організації мережі та організує мережу;

передає мережеві сигнальні пакети з інформацією про існуючу мережу;

керує мережевими підлеглими пристроями, встановлює параметри мережі;

визначає максимальну глибину вкладених підмереж, число мережевих маршрутизаторів та число підлеглих пристроїв;

забезпечує маршрутизацію інформації між підлеглими пристроями;

більшу частину часу перебуває у режимі прийому;

забезпечує організацію таблиць маршрутизації;

дозволяє маршрутизаторам та кінцевим пристроям входити в мережу.

Маршрутизатор – приймає, буферизує та передає дані від інших вузлів мережі, а також визначає напрямки передачі.

Маршрутизатор виконує такі функції:

визначає активні канали, підключається до мережі та дозволяє кінцевим пристроям входити в мережу, використовуючи списки активних каналів;

ретранслює сигнальні мережні пакети з параметрами мережі від координатора;

адмініструє мережеві адреси підключених до маршрутизатора підлеглих пристроїв;

підтримує функції маршрутизації багатокоміркових мереж: створює таблиці мережевої маршрутизації з параметром якості зв'язку з кожним із сусідніх мережевих вузлів, ретранслює пакети запиту та підтвердження визначення маршрутів між пристроями;

підтримує функції маршрутизації за деревоподібним принципом – транслює повідомлення вгору і вниз ієрархічною деревоподібною структурою гілки в залежності від адреси одержувача повідомлення.

Кінцевий вузол (сенсорний вузол) – виконує лише прикладні дії (збір інформації та управління віддаленим об'єктом) та не здійснює ретрансляцію даних.

Сенсорний вузол має такі особливості:

завжди шукає та намагається увійти в існуючу мережу – використовує списки активних каналів та сигнальні пакети синхронізації координатора існуючої мережі для визначення параметрів мережі та маршрутизатора для входу до мережі;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 52

запитує дані координатора та здатний до 99,99% від усього часу роботи перебувати у «сплячому» режимі.

Сенсорні вузли являють собою мініатюрні обчислювальні пристрої (рис.4), які забезпечені датчиками, актуаторами та засобами комунікації. Сенсорний вузол є платою, на якій розміщується процесор, пам'ять - флеш та оперативна, цифро-аналогові та аналого-цифрові перетворювачі, засоби зв'язку, джерело живлення та різні датчики і актуатори.

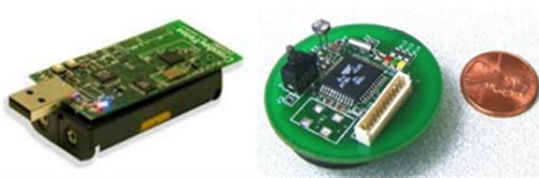


Рис. 4.4 – Зовнішній вигляд сенсорних вузлів

Датчики можуть бути найрізноманітнішими. Найчастіше використовуються датчики температури, тиску, вологості, освітленості, вібрації, розташування, рідше – магнітоелектричні, хімічні (наприклад, що вимірюють вміст CO, CO₂, рівень радіаційного фону), звукові та деякі інші. Набір застосовуваних датчиків залежить від функцій, що виконуються сенсорним вузлом.

Отримані від датчика електричні сигнали часто неготові обробки, тому вони проходять стадію перетворення. Наприклад, сигнал часто вимагає посилення збільшення амплітуди, можливе застосування фільтрів для усунення небажаного шуму в певних діапазонах частот і т.п. Перетворений сигнал трансформується за допомогою аналого-цифрового перетворювача (АЦП) у цифровий сигнал.

У результаті сигнал виходить у цифровій формі і він готовий до подальшої обробки у процесорі та зберігання в пам'яті мікроконтролера. За наявності виконавчих механізмів можлива також передача впливів керуючих від вузлів мережі через актуатор. Живлення сенсорного вузла зазвичай здійснюється від невеликої батареї.

Крім розміру, сенсорний вузол має споживати якомога менше енергії, працювати з великою кількістю вузлів на малих відстанях, бути автономним та працювати без обслуговування, а також мати низьку вартість виробництва та високу надійність.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 53

Сенсорний вузол складається з апаратного забезпечення, базового програмного забезпечення та прикладного програмного забезпечення.

Апаратна частина сенсорного вузла може бути розділена на чотири підсистеми (рис.4.5):

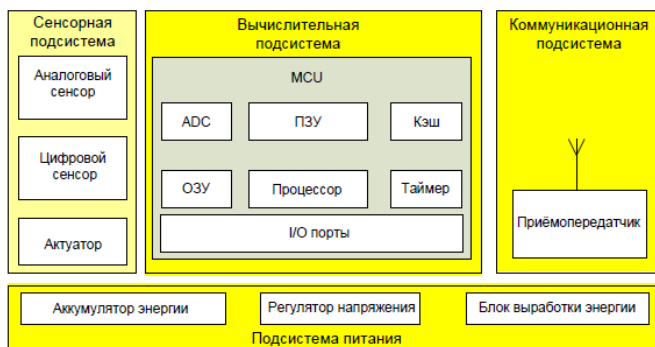


Рис. 4.5 – Вузол бездротової сенсорної мережі

комунікаційна підсистема – забезпечує бездротові або дротові з'єднання з іншими вузлами в сенсорній мережі;

обчислювальна підсистема – забезпечує обробку даних та функціональність вузла і складається з мікроконтролера MCU, до складу якого входять процесор, оперативна SRAM, енергонезалежна EEPROM та флеш-пам'ять, аналого-цифровий перетворювач ADC, таймер, порти введення/виведення;

сенсорна підсистема, до складу якої можуть входити аналогові та цифрові сенсори і актуатори, забезпечує з'єднання з обчислювальною підсистемою;

підсистема електроживлення – забезпечує енергетичне постачання всіх елементів бездротового сенсорного вузла та включає пристрої генерації та акумулювання енергії, а також регулювання напруги.

У складі архітектури сенсорної мережі визначено чотири базові інтерфейси:

інтерфейс між базовим та прикладним програмним забезпеченням сенсорного вузла;

інтерфейс між базовим програмним забезпеченням та апаратним забезпеченням сенсорного вузла;

бездротові або дротові інтерфейси між вузлами в сенсорній мережі;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 54

інтерфейс між сенсорною мережею та зовнішнім середовищем (провайдери послуг, користувачі).

До складу БСМ завжди входять трансівери, що працюють у заданому діапазоні радіочастот.

Як приклад у табл. 4.1 наведено параметри плат, на яких можуть бути створені сенсорні вузли.

Таблиця. 4.1 - Параметри плат для вузлів БСМ

Мікроконтролер	ESP32	ESP8266
Процесор	Tensilica Xtensa 32-біти	Tensilica 32-біти
Тактова частота, МГц	160(240)	80(160)
Оперативна пам'ять, кбайт	512	50
АЦП	12-біт	10-біт
Цифрові апаратні інтерфейси	UART/SPI/I2C/ I2S, IЧ-порт	UART/SPI/ I2S, IЧ-порт
Трансивер		
Діапазон частот, МГц	2400 - 2483,5	2400 - 2483,5
Тип інтерфейсу	802.11 b / g / n, BLE	802.11 b/g/n
Робоча напруга	3,3В	3,0 – 3,6 В

ESP32 та ESP8266 – це недорогі модулі Wi-Fi, які ідеально підходять для самостійних проєктів у галузі IoT. ESP32 є наступником ESP8266. Обидва чіпи мають 32-бітний процесор. ESP32 – двоядерний процесор із частотою від 160 до 240 МГц, а ESP8266 – одноядерний, що працює на частоті 80 МГц. ESP32 має більше GPIO і крім Wi-Fi підтримує також Bluetooth 4.2 та Bluetooth низької енергії (BLE). ESP32 поставляється з датчиками торкання, вбудованим датчиком Холла та датчиком температури. Обидві плати дешеві, але ESP32 трохи дорожче.

Виділяють два *типи архітектури сенсорних мереж*: однорангові та ієрархічні (кластерні). *Однорангові мережі* (рис.4.6) можуть формувати довільні топологічні структури (точка-точка, зірка), обмежені лише дистанцією між кожною парою вузлів. У одноранговій мережі типу кластерне дерево більшість пристроїв є FFD (Fully Function Device). Пристрої RFD (Reduced Function Device) підключаються до кластера як кінцеві вузли. *Коміркова топологія* (Mesh Topology) – це топологія, в якій кожен маршрутизатор мережі з'єднується з декількома іншими маршрутизаторами *цієї самої мережі*.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 55

Можливість самоорганізації та самовідновлення мереж комірчастої топології дозволяє у разі виходу частини сенсорних вузлів з ладу спонтанно формувати нову структуру мережі. Правда, у будь-якому випадку необхідний центральний функціональний вузол-координатор, який приймає та обробляє всі дані, або шлюз передачі даних на обробку зовнішньому вузлу. Характеризується високою стійкістю до відмови, але і більш складним налаштуванням. Пересилання даних в одноранговій мережі відбувається за найефективнішими за деякими критеріями маршрутами, що дозволяє досягти економії таких важливих ресурсів, як енергія (передача йде за маршрутом з найвищим запасом енергії) і час (передача відбувається за найкоротшим маршрутом). Однак при такій організації мережі формування зв'язків між вузлами відбувається спонтанно, що веде до зіткнень пакетів і виникнення затримок, пов'язаних з виходом з режиму сну вузлів, що знаходяться на вибраному шляху передачі.

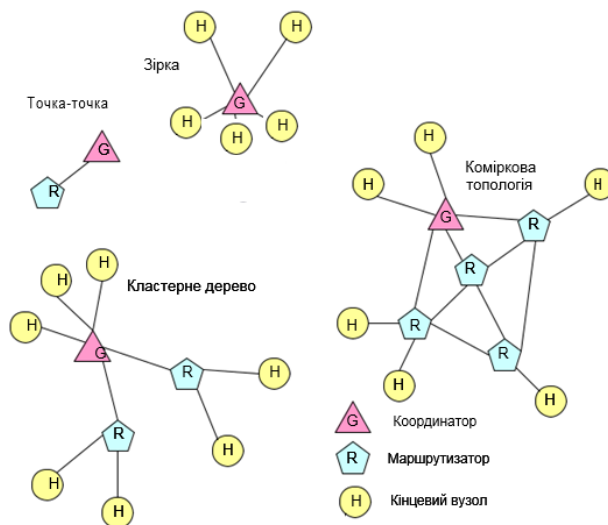


Рис. 4.6 - Архітектура однорангової сенсорної мережі

Альтернативним підходом є ієрархічна маршрутизація. Вона полягає в розподілі мережі на області, що називають кластерами. Кластер утворюють маршрутизатор і кінцеві вузли, у яких він запитує сенсорні дані (рис.4.7). Всередині кожного кластера маршрутизатор відповідає за збір інформації з усього кластера, її обробку та подальшу передачу. Інші вузли кластера здійснюють лише збір даних та передачу їх маршрутизатору.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 56

Таким чином, вузли в ієрархічній мережі не є рівноправними. По-перше, агрегування даних відбувається на маршрутизаторах і, по-друге, пересилання агрегованих даних далі може здійснюватися лише маршрутизаторами. Отже мінімізуються затримки передачі, оскільки маршрутизатори доступні завжди. Зіткнення пакетів виключено завдяки централізованому методу створення посилань. Однак, така маршрутизація не надає оптимальних шляхів передачі даних.

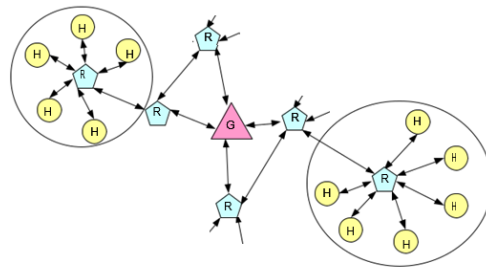


Рис. 4.7 - Кластерна архітектура сенсорної мережі

Для визначення маршруту передачі від кінцевого вузла до вузла-координатора, і навіть між кінцевими вузлами, використовуються спеціальні *протоколи маршрутизації*. Протоколи маршрутизації вирішують такі завдання:

- самоорганізація вузлів мережі та максимізація зони покриття мережі;
- маршрутизація пакетів даних та адресація вузлів;
- мінімізація енергоспоживання вузлів мережі та збільшення загального часу життя всієї мережі;
- збір та агрегація даних;
- регулювання швидкості передачі та обробки даних у мережі;
- забезпечення заданої якості обслуговування (QoS) та захист від несанкціонованого доступу.

Робота протоколу маршрутизації може ґрунтуватися на різних засадах:

протоколи маршрутизації з багатьма маршрутами – використовуються кілька маршрутів від джерела до точки призначення, що підвищує надійність з'єднання, але збільшує накладні та енерговитрати;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 57

протоколи маршрутизації «за запитом» – вузол надсилає запит на дані в мережу а інший вузол, який має дані, що запитуються, відповідає на запит;

протоколи маршрутизації, засновані на «переговорах» між вузлами;

протоколи, що враховують якість обслуговування, що дозволяє забезпечити певний рівень послуг у мережі.

Протоколи маршрутизації відповідають за підтримку маршрутів у мережі та повинні гарантувати надійний зв'язок навіть у самих несприятливих умовах.

При виборі шляху передачі в мережі в якості метрик в них можуть бути використані наступні параметри: довжина шляху (кількість ділянок переприймання інформації), надійність, затримка, пропускна здатність, завантаження, вартість передачі трафіку та ін.

4.3. Загальні принципи M2M - комунікацій

Машинно-машинна взаємодія (Machine-to-Machine, M2M) – загальна назва технологій, які дозволяють машинам обмінюватися інформацією один з одним, або ж передавати її в односторонньому порядку в автоматичному режимі між пристроями без участі людини. M2M - комунікації є найважливішою складовою Інтернету речей. Концепція M2M поєднує телекомунікаційні та інформаційні технології для автоматизації різних технологічних та бізнес процесів.

При всьому своєму практичному різноманітті ідея машино-машинної взаємодії може бути зведена до простої схеми з трьох елементів. Уявіть собі цифровий пристрій (машину) А, зайнятий збиранням будь-якої інформації. Зібрані відомості передаються через канал зв'язку (провідний або бездротовий) на пристрій (машину) В, що робить аналіз отриманих даних і зберігання результатів, а при необхідності і генерацію керуючих команд для пристрою А (рис. 4.8). Здатність керувати віддаленими пристроями за допомогою бездротового сигналу дозволила мінімізувати залежність від місцезнаходження і часу. Останнє покоління M2M-модулів забезпечує підтримку таких базових технологій, як GSM/GPRS, GPS, Bluetooth, ZigBee, Ethernet, WiFi та ін.

Сьогодні M2M-обладнання дуже широко використовується у протиугінних та охоронних системах. Наприклад, при спробі проникнення до квартири, сигнал про подію передається через мережу GSM на диспетчерський пульт черговому оператору у вигляді SMS-повідомлення або голосового сигналу.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 58



Рис. 4.8 - Машинно-машинна взаємодія

Крім моніторингу стаціонарних об'єктів, застосування M2M можливе в мобільних системах. Вантажоперевізники можуть відстежувати за допомогою GPS переміщення своїх автомобілів у реальному масштабі часу, отримувати інформацію про їх технічний стан, коригувати маршрути, тим самим прискорюючи доставку вантажу. Банкомати або платіжні термінали можуть автоматично передавати необхідну інформацію по мережах GSM, а датчики моніторингу вологості ґрунту дозволять зробити витрату води максимально економічною та ефективною в аграрному комплексі. Модулями зв'язку забезпечують безліч різних датчиків контролю температури, рівня освітленості, вогню та диму, а система «розумний дім» давно перетворилася із мрії на реальність.

Мережева технологія M2M, що використовується для побудови розподілених систем збирання даних та управління на промислових підприємствах, отримала назву «промислової мережі».

Промисловою мережею називають комплекс обладнання та програмного забезпечення, які забезпечують обмін інформацією (комунікацію) між декількома пристроями (різні датчики, виконавчі механізми, промислові контролери) у межах промислової автоматизованої системи.

Промислові мережі використовуються для:

діагностики та віддаленого конфігурування датчиків та виконавчих механізмів;

калібрування датчиків;

живлення датчиків та виконавчих механізмів;

зв'язку між датчиками, виконавчими механізмами та контролерами автоматизованої системи управління технологічними процесами.

Промислові мережі можуть взаємодіяти зі звичайними комп'ютерними мережами, зокрема, використовувати глобальну мережу інтернет.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 59

Порівняно з традиційними локальними обчислювальними мережами, промислові мережі мають підвищену стійкістю до дії електромагнітних перешкод і забезпечують роботу з лініями зв'язку протяжністю від сотень метрів до кількох кілометрів. Крім того вони мають підвищену міцність кабелю, ізоляції, роз'ємів та забезпечують підвищену надійність передачі з можливістю самовідновлення після збою.

З'єднання між компонентами промислової мережі виконується за допомогою інтерфейсів. Найбільш важливими параметрами інтерфейсу є пропускна здатність і максимальна довжина кабелю, що підключається. Промислові інтерфейси зазвичай забезпечують гальванічну розв'язку між пристроями, що з'єднуються.

Взаємодія пристроїв у промислових мережах виконується відповідно до моделей клієнт-сервер або видавець-передплатник (publisher-subscriber). У моделі клієнт-сервер взаємодіють два об'єкти, сервером є об'єкт, який надає сервіс, тобто який виконує деякі дії на запит клієнта. Мережа може містити кілька серверів та кілька клієнтів. Кожен клієнт може надсилати запити кільком серверам, і кожен сервер може відповідати на запити кількох клієнтів. Ця модель зручна для передачі даних, які з'являються періодично або заздалегідь у відомий час, як, наприклад, значення температури в періодичному технологічному процесі. Однак ця модель незручна для передачі випадкових подій, наприклад, події, що полягає у випадковому спрацьовуванні датчика рівня, оскільки для отримання цієї події клієнт повинен періодично, з високою частотою, запитувати стан датчика і аналізувати його, перевантажуючи мережу марним трафіком.

У моделі взаємодії видавець- передплатник є один видавець і безліч передплатників. Передплатник під час реєстрації повідомляє видавцеві список тегів, значення яких він хоче отримувати за розкладом або в міру появи нових даних. Кожен клієнт може підписатися на свій набір тегів. Відповідно до встановленого розкладу видавець розсилає передплатникам повідомлення із інформацією, що запитувалась.

У будь-якій моделі взаємодії можна виділити пристрій, який керує іншим (підлеглим) пристроєм. Пристрій, який виявив ініціативу в обміні, називають ведучим або головним (master). Пристрій, який відповідає на запити майстра, називають веденим чи підлеглим (slave). Ведений пристрій ніколи не починає

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 60

комунікацію першим. Він чекає на запит від ведучого і лише відповідає на запити. Наприклад, у моделі клієнт-сервер клієнт є ведучим, а сервер – підлеглим. У моделі видавець-передплатник на етапі передплати ведучим є клієнт, а на етапі розсилки публікацій – сервер.

Деякі мережі використовують багатоабонентський режим, коли одне й те повідомлення надсилається декільком пристроям одночасно. Мережі можуть мати топологію зірки, кільця, шини чи змішану. У промисловій автоматичі використовується найбільш часто загальна шина, у різних місцях якої може бути підключена довільна кількість пристроїв.

4.4. Цифрові апаратні інтерфейси

I2C - це послідовний двопровідний інтерфейс, який використовується для "міжмікросхемного" (inter-IC) управління. У стандартному режимі забезпечується передача послідовних 8-бітних даних зі швидкістю до 100 кбіт/с і до 400 кбіт/с у "швидкому" режимі. Шина I²C нового покоління може обмінюватися даними із швидкістю від 400 кбіт/с до 5 Мбіт/с.

Для здійснення процесу обміну інформацією I2C шині, використовується всього два сигнали SDA (Serial DATA)- лінія даних і SCL (Serial Clock) - лінія синхронізації. Кожний I2C-сумісний пристрій розпізнається за унікальною адресою і може працювати як передавач або приймач, залежно від призначення пристрою.

Крім того, пристрої можуть бути класифіковані як ведучі та ведені при передачі даних. Ведучий – це пристрій, який ініціює передачу даних та виробляє сигнали синхронізації. При цьому будь-який пристрій, що адресується, вважається веденим по відношенню до ведучого. Виходячи зі специфікації роботи шини, у кожен окремий момент у шині може бути тільки один ведучий, а саме той пристрій, який забезпечує формування сигналу шини SCL. Ведучий може виступати як у ролі ведучого-передавача, так і ведучого-приймача. Проте - шина дозволяє мати кілька ведучих, накладаючи певні особливості їхньої поведінки у формуванні сигналів управління та контролю стану шини.

У вихідному положенні обидва сигнали SDA та SCL знаходяться у високому стані (рис. 4.9). Процедура обміну починається з того, що ведучий формує стан СТАРТ - перехід сигналу лінії SDA з високого стану в низький,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 61

при високому рівні на лінії SCL. Цей перехід сприймається усіма пристроями, підключеними до шини як ознака початку процедури обміну.

Сигнал синхронізації при пересиланні даних по шині завжди генерує ведучий.

Процедура обміну завершується тим, що ведучий формує стан СТОП - перехід лінії SDA з низького стану у ВИСОКИЙ при ВИСОКОМ стані лінії SCL. Стан СТАРТ та СТОП завжди виробляються ведучим. Вважається, що шина зайнята після фіксації стану СТАРТ. Шина вважається такою, що звільнилася через деякий час після фіксації стану СТОП.

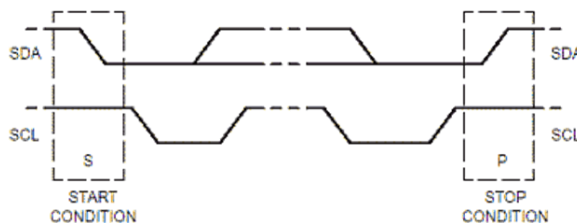


Рис. 4.9 – Процедура обміну I2C

Після формування стану СТАРТ, ведучий переводить лінію SCL у низький стан і виставляє на лінію SDA старший біт першого байта повідомлення. Кількість байт у повідомленні не обмежена. Специфікація шини I2C дозволяє зміни на лінії SDA тільки за низького рівня сигналу на лінії SCL.

Для підтвердження прийому байта від ведучого - передавача веденим - приймачем у специфікації протоколу обміну по шині I2C вводиться спеціальний біт підтвердження, що виставляється на шину SDA після прийому 8 біт даних.

Кожен пристрій, підключений до шини, може бути програмно адресований унікальною адресою. Процедура адресації на шині I2C полягає у тому, що перший байт після сигналу СТАРТ визначає, який ведений адресується ведучим щодо циклу обміну.

Перші сім бітів першого байта утворюють адресу веденого. Восьмий, молодший біт, визначає напрямок пересилання даних. "Нуль" означає, що ведучий буде записувати інформацію у вибраного веденого. "Одиниця" означає, що ведучий зчитуватиме інформацію з веденого. Після того, як адреса надіслана, кожен пристрій в системі порівнює перші сім біт після сигналу СТАРТ зі своєю адресою. При збігу пристрій вважає себе обраним як ведений-

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 62

приймач або як ведений-передавач, залежно від біта напряму. Всі ІМС, що підтримують роботу в стандарті шини I2C, мають набір фіксованих адрес, перелік яких вказаний виробником в описах контролерів.

I²S (Inter-IC Sound) – це стандарт інтерфейсу послідовної шини, що використовується для передачі аудіо даних між інтегральними схемами в електронних пристроях. Цей стандарт був уперше представлений Philips Semiconductor у 1986 році.

Протокол **UART** (Universal asynchronous receiver/transmitter) — найстаріший і найпоширеніший на сьогоднішній день фізичний протокол передачі даних. Найбільш відомий з сімейства UART протокол RS-232 (COM-порт, той самий що стоїть у комп'ютері). Основні робочі лінії протоколу RS-232– RXD (Received Data) та TXD (Transmitted Data) або просто RX та TX. Вихід передавача TX з'єднаний із входом приймача RX і навпаки. Електричний принцип роботи RS-232 відрізняється від стандартної 5-вольтової TTL логіки. У цьому протоколі логічний нуль лежить від +3 до +12 В, а одиниця від -3 до -12В, відповідно. Проміжок від -3 до +3В вважається зоною невизначеності (рис. 4.10). Така велика амплітуда робочої напруги, цілих 24 вольта, потрібна в першу чергу для перешкодостійкості ліній зв'язку. За стандартом довжина кабелю може бути 15 м.

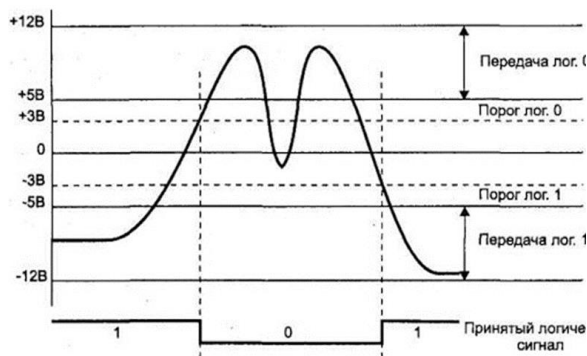


Рис. 4.10 – Протокол UART

Стандартна посилка займає 10 біт. Початок передачі позначають стартовим бітом, який завжди дорівнює нулю. Потім іде передача восьми біт даних. Завершує посилку біт парності та стоповий біт. Біт парності здійснює

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 63

перевірку переданих даних. Стоповий біт свідчить, що пересилання даних завершено. Стартовий і стоповий біти дорівнюють нулю (рис. 4.11).

Другий за розповсюдженням інтерфейс після RS-232 – це RS-485. Він є промисловим стандартом, і передача в ньому здійснюється по кручений парі, що дає йому непогану стійкість до перешкод і підвищену швидкість передачі до 4 Мбіт в секунду. Довжина дроту тут може досягати 1 км. Існують мікросхеми сполучення USB з UART, наприклад, мікросхема FT232rl, яка з 5 вольт генерує негативну напругу, щоб сполучати 5-вольтовий UART з RS-232.



Рис.4.11 – Сигнал UART на екрані осцилографа.

SPI (3-wire) – популярний інтерфейс для послідовного обміну даними між мікросхемами. Інтерфейс SPI, поряд з I2C, відноситься до найбільш широко використовуваних інтерфейсів для з'єднання мікросхем. Спочатку він був придуманий компанією Motorola, а зараз використовується в продукції багатьох виробників. Його найменування є аббревіатурою від «Serial Peripheral Bus», що відображає його призначення - шина для підключення зовнішніх пристроїв. Шина SPI організована за принципом ведучий-підлеглий. Як ведучий шини зазвичай виступає мікроконтролер. У ролі підлеглих виступають різноманітні мікросхеми, зокрема, запам'ятовуючі пристрої (EEPROM, Flash-пам'ять, SRAM), цифрові датчики та ін. Пристрої на шині нерівнозначні, тобто має бути як мінімум один головний (англ. master) і один або кілька підлеглих (англ. slave) пристроїв. Шина SPI містить у загальному випадку 4 дроти:

- SLK (Serial Clock) — на цій лінії головний пристрій подає тактуючий сигнал, синхронізуючий прийом або передачу даних.
- MISO (Master Input, Slave Output) – дані йдуть від підлеглого до головного.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 64

• MOSI (Master Output, Slave Input) - дані йдуть від головного пристрою до підлеглого.

• CS (Chip Select, іноді SS - Slave Select) — дозволяє підлеглому пристрої почати працювати.

Існує три типи підключення до шини SPI, у кожному з яких беруть участь чотири сигнали. Найпростіше підключення, у якому беруть участь лише дві мікросхеми, показано рис.4.12. Подану схему можна спростити виключенням лінії MISO, якщо підпорядкований пристрій не передбачає відповідну передачу даних. Односторонню передачу даних можна зустріти у таких мікросхем як ЦАП, цифрові датчики. Щоб підпорядкована IC приймала та передавала дані, крім наявності сигналу синхронізації, необхідно також, щоб лінія SS була переведена в низький стан. Інакше підпорядкована IC буде неактивна.

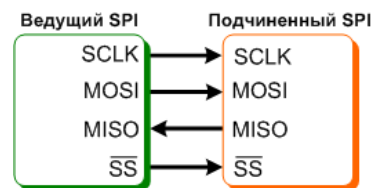


Рис. 4.12 - Найпростіше підключення по шині SPI

При необхідності підключення до шини SPI кількох мікросхем використовується або незалежне (паралельне) підключення (рис. 4.13), або каскадне (рис.4.14). При незалежному підключенні всі сигнали, крім вибору мікросхем, з'єднані паралельно, а ведучий шини, переводом того чи іншого сигналу SS в низький стан, задає, з якою підпорядкованою IC він обмінюватиметься даними. Головним недоліком такого підключення є необхідність додаткових ліній для адресації підлеглих мікросхем.

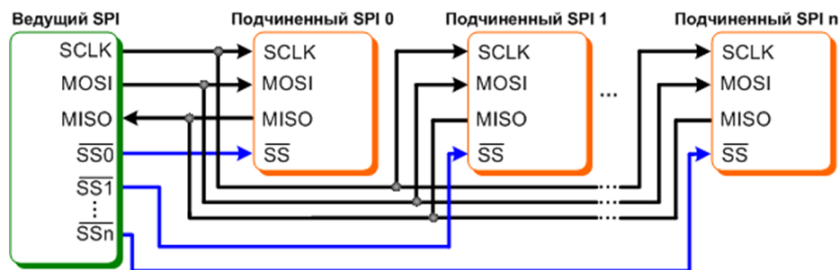


Рис. 4.13 - Незалежне підключення до шини SPI

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 65

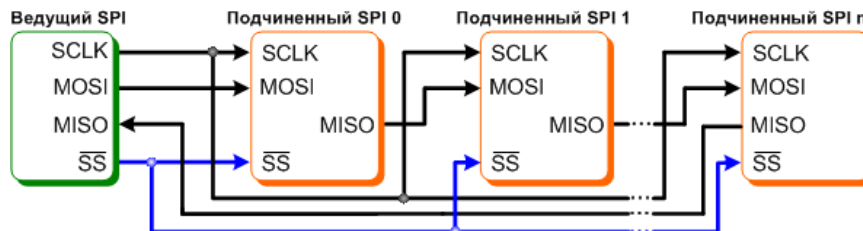


Рис. 4.14 - Каскадне підключення до шини SPI

Каскадне (послідовне) включення позбавлене цього недоліку - із кількох мікросхем утворюється один великий зсувний регістр. Для цього вихід передачі однієї IC з'єднується з входом прийому даних іншої. Однак використання каскадного підключення можливе лише в тому випадку, якщо його підтримка вказана в документації на мікросхеми, що використовуються. Щоб з'ясувати це, важливо знати, що таке підключення англійською називається "daisy-chaining".

Інтерфейс однопровідної шини SDA використовується для передачі цифрових даних, наприклад, датчиків DHT11/22. Управління шиною SDA відбувається «притисканням до землі» (подачею логічного «0») та «відпусканням» шини, тоді в шині з'являється логічна «1» через резистор, що підтягує. Після подачі на вихід SDA "стартового" сигналу він видає 40 біт інформації, де перші 16 біт - вологість, наступні 16 біт - температура, останні 8 біт - контрольна сума.

Приклад 40 біт відповіді датчика:

00000001 10101010 00000001 00001111 10111011

426=42,6% 271=27,1°C 00000001+10101010+00000001+00001111
вологість температура контрольна сума.

Значення вологості визначається у %, а значення температури у °C, при цьому перший біт температури це її знак ("0" означає "+", "1" означає "-").

5. Принципи побудови бездротових сенсорних мереж

5.1. Ієрархія мережевих технологій, що використовуються в IoT

Одним із головних питань організації Інтернету речей є реалізація взаємодії між: інтернет-речами, користувачами та інтернет-речами, віддаленим сервером та інтернет-речами. IoT використовує велику кількість варіантів мереж зв'язку для передачі даних, починаючи від мереж, які працюють на

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 66

відстані кілька десятків сантиметрів, аж до всесвітньої мережі Інтернет. По території охоплення телекомунікаційні мережі, що використовуються в IoT, можна поділити на 4 основні типи (рис. 5.1):

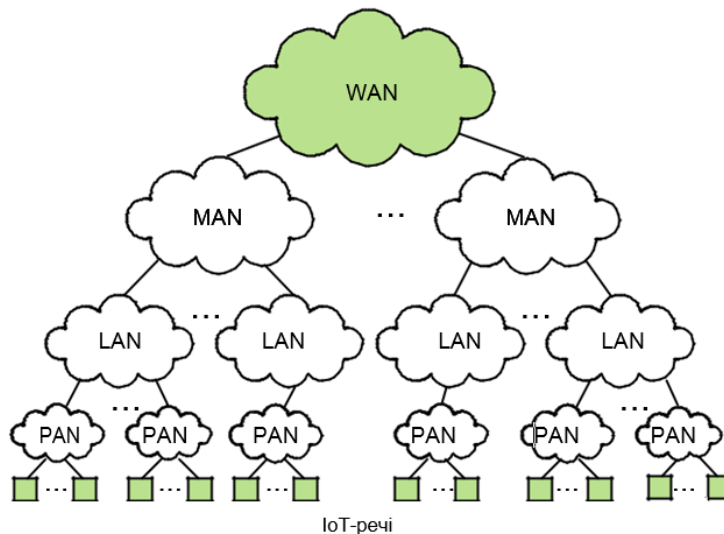


Рис.5.1 - Ієрархія мережевих технологій, що використовуються в IoT

1. *Персональна мережа PAN (Personal Area Network)* - це мережа, побудована "навколо" людини. Дані мережі мають об'єднувати всі персональні пристрої користувача (телефони, смартфони, ноутбуки, гарнітури та ін.). Стосовно IoT така мережа будується «навколо» пристрою («речі»).

2. *Локальна мережа LAN (Local Area Network)* – мережа, що зазвичай покриває відносно невелику територію або невелику групу будівель (будинки, офіс, фірму). До локальних мереж можна віднести і мережу контролерів CAN (Controller Area Network) - промислову мережу, орієнтовану насамперед на об'єднання в єдину мережу різних виконавчих пристроїв і датчиків в рамках окремого підприємства.

3. *Міська мережа MAN (Metropolitan Area Network)* – об'єднує окремих користувачів та локальні мережі в межах міста, являє собою мережу за розмірами більшу, ніж LAN, але меншу, ніж WAN.

4. *Глобальна мережа WAN (Wide Area Network)* – пов'язує користувачів та мережі, розосереджені на відстані сотень та тисяч кілометрів.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 67

Всі технології передачі даних в інтернеті речей, залежно від використовуваного середовища передачі, можна розділити на два великі класи: дротові та бездротові. Дротові технології передачі даних в IoT можуть використовувати металевий (мідний) кабель зв'язку, електропроводку (технологія PLC – Power Line Communication) або волоконно-оптичний кабель. Однак через складності фізичної реалізації ліній зв'язку провідні технології для комунікацій інтернет-речей застосовуються меншою мірою, ніж бездротові. Бездротові комунікації великого радіусу дії реалізуються на основі різних стільникових мереж, мереж бездротового широкосмугового доступу WiMAX та ін.

Бездротові мережі малого радіусу дії, що використовуються в IoT, можна розділити на три види:

1. *Бездротові персональні мережі WPAN (Wireless Personal Area Network).* Радіус дії WPAN становить від кількох десятків сантиметрів до кількох метрів. Такі мережі використовуються як для об'єднання окремих пристроїв між собою, так і для зв'язку їх із мережами вищого рівня, наприклад, глобальною мережею Інтернет.

2. *Бездротові сенсорні мережі WSN (Wireless Sensor Network)* це розподілені мережі безлічі датчиків (сенсорів) та виконавчих пристроїв, об'єднаних між собою за допомогою радіоканалу. За розмірами фізичної зони розміщення БСС належать до класу бездротових персональних обчислювальних мереж WPAN. Однак, за рахунок можливості ретрансляції повідомлень від одного елемента до іншого, область покриття подібних мереж може становити від кількох метрів до кількох кілометрів.

3. *Малі локальні мережі TAN (Tiny Area Network).* Обчислювальні мережі, що розгортаються у межах невеликого офісу або окремого житла. Їх часто називають домашніми мережами, оскільки вони поєднують комп'ютери, побутову електроніку та прилади сигналізації, що належать одній сім'ї.

5.2. Особливості реалізації бездротової сенсорної мережі

Бездротові сенсорні мережі, по суті, є такими, що самоорганізуються, оскільки в них здійснюється автоматичний вибір схеми організації мережі та маршрутів передачі даних.

Переваги бездротових сенсорних мереж:

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 68

здатність передавати інформацію на значні відстані при малій потужності передавачів (шляхом ретрансляції);
 низька вартість вузлів та їх малий розмір;
 низьке енергоспоживання та можливість електроживлення від автономних джерел;
 простота установки, відсутність необхідності у прокладанні кабелів (завдяки бездротовій технології та живленню від батарейки);
 можливість встановлення таких мереж на вже існуючий та експлуатований об'єкт без проведення додаткових робіт;
 здатність до самовідновлення та самоорганізації;
 низька вартість технічного обслуговування.

Найчастіше сенсорний вузол повинен мати можливість самостійно визначити своє місцезнаходження, принаймні стосовно того іншого сенсора, якому він буде передавати дані. Тобто спочатку відбувається ідентифікація всіх сенсорів, а потім формується схема маршрутизації. Сенсорні вузли можуть закріплюватися стаціонарно, а також мати відносну мобільність, тобто довільно переміщуватися один щодо одного в деякому просторі, не порушуючи при цьому логічного зв'язку мережі. В останньому випадку сенсорна мережа не має фіксованої постійної топології, та її структура динамічно змінюється з часом.

У сенсорній мережі вузли зазвичай спілкуються за допомогою бездротового зв'язку. Зв'язок може здійснюватися за допомогою радіо, інфрачервоного випромінювання (ІЧ-порту) або оптичних сигналів. ІЧ-зв'язок доступний без ліцензії та захищений від перешкод електричних приладів. ІЧ-передавачі дешевші та простіші у виробництві. Багато сьогоdnішніх ноутбуків та мобільних телефонів використовують ІЧ-інтерфейс для передачі даних. Основним недоліком такого зв'язку є вимога прямої видимості між відправником та отримувачем. Одним з найпоширеніших варіантів радіозв'язку є використання смуг частот для промислових, наукових та медичних цілей ISM, які визначені Сектором радіозв'язку Міжнародного союзу електрозв'язку ITU-R та доступні без ліцензій у більшості країн і наведені в табл.5.1. Основними перевагами використання радіочастот ISM є широкий спектр частот та доступність у всьому світі. Вони не прив'язані до конкретного стандарту, цим дають велику свободу для реалізації енергозберігаючих стратегій у сенсорних мережах.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 69

Таблиця 5.1 – Смути частот ISM

Діапазон частот		Смуга	Центральна частота
6,765 МГц	6,795 МГц	30 КГц	6,78 МГц
13,553 МГц	13,567 МГц	14 КГц	13,56 МГц
26,957 МГц	27,283 МГц	326 КГц	27,12 МГц
40,66 МГц	40,7 МГц	40 КГц	40,68 МГц
433,05 МГц	434,79 МГц	1,84 МГц	433,92 МГц
902 МГц	928 МГц	26 МГц	915 МГц
2,4 ГГц	2,5 ГГц	100 МГц	2,45 ГГц
5,725 ГГц	5,875 ГГц	150 МГц	5,8 ГГц
24 ГГц	24,25 ГГц	250 МГц	24,125 ГГц
61 ГГц	61,5 ГГц	500 МГц	61,25 ГГц
122 ГГц	123 ГГц	1 ГГц	122,5 ГГц
244 ГГц	246 ГГц	2 ГГц	245 ГГц

Найважливішим чинником під час роботи бездротових сенсорних мереж є обмежена ємність батарей, що встановлені у сенсорному вузлі. Найбільш енерговитратною операцією для сенсорних вузлів є передача даних у бездротове оточення. Тому енергозберігаючі форми передачі є ключовим чинником продовження терміну служби сенсорів, оскільки він майже повністю залежить від терміну служби батарей. Для вирішення цього завдання розроблено спеціальні *комунікаційні протоколи*. Для зменшення енергоспоживання зазвичай передбачається відключення передавачів сенсорних вузлів, коли не потрібно передачі інформації. На мережному рівні використовуються оптимальні шляхи передачі інформації від сенсорного вузла до координатора з огляду на кількість проміжних вузлів, необхідну енергію та доступну енергію. Окрім мережевого протоколу на споживання енергії впливає конструкція вузлів (наприклад, маленький розмір пам'яті, ефективність перемикань між завданнями), програмне забезпечення, механізми захисту та навіть робочі додатки. У зв'язку з цим необхідно виконувати на сенсорному

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 70

вузлі тільки найпростішу первинну обробку, орієнтовану на зменшення обсягу інформації, що передається, і, що найголовніше, мінімізувати число циклів прийому і передачі даних.

Залежно від того, яким чином відбувається збір даних, БСМ можна поділити на проактивні, реактивні та гібридні мережі.

Сенсорні вузли *проактивної мережі* періодично включають свої сенсори та передавачі, знімають показання та передають їх на базову станцію. Таким чином, вони роблять "моментальну фотографію" свого оточення з деякою періодичністю і використовуються зазвичай для регулярного моніторингу деяких значень.

Сенсорні вузли *реактивних мереж* з деякою періодичністю знімають показання, проте не передають їх, якщо отримані дані потрапляють до певної області припустимих показань. Водночас відомості про несподівані та різкі зміни у показаннях датчиків або їхньому виході за діапазон припустимих значень негайно передаються до координатора. Цей вид мережі призначений для роботи з вимірами у реальному часі.

Сенсорні вузли *гібридної мережі* не тільки періодично відправляють зняті дані, але і реагують на різкі зміни в значеннях.

Енергію, що необхідної для роботи електронних схем, можливо отримати з навколишнього середовища. Існують чотири основні джерела енергії: механічна енергія (вібрації, деформації), теплова енергія (температурні перепади або зміни), енергія випромінювання (сонце, інфрачервоні промені, радіочастоти) та хімічна енергія. Ці джерела характеризуються різними щільностями потужності (рис. 5.2). Малюнок показує, що значення вихідної потужності 10-100 мкВт є прийнятним при розмірах джерела 1 см² або 1 см³. Одержання енергії від сонця вважається найпотужнішим (навіть якщо значення, наведені на рис. 1, мають бути помножені на вагові коефіцієнти із врахуванням того, що ККД рідко перевищує 20% для фотоелемента). Для живлення вузлів сенсорної мережі від навколишньої енергії необхідно знизити споживання енергії датчиками (сенсорами/актуаторами), мікроконтролером та радіопередавачем. В останні роки значний прогрес у цьому напрямку було досягнуто виробниками мікроконтролерів та радіочастотних чіпів (Atmel, Microchip, Texas Instruments та ін.). Приклад типового споживання енергії вузлом бездротових сенсорних мереж наведено на рис. 5.3.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 71

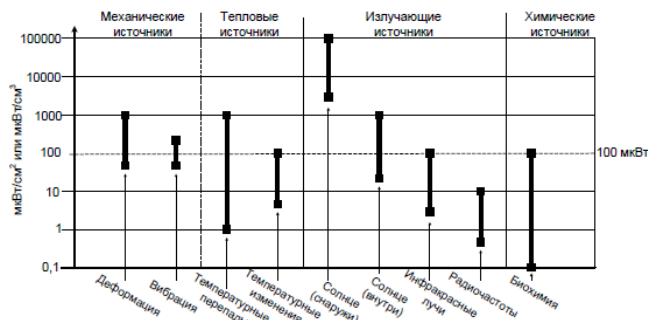


Рис. 5.2 - Щільність потужності різних типів джерел енергії

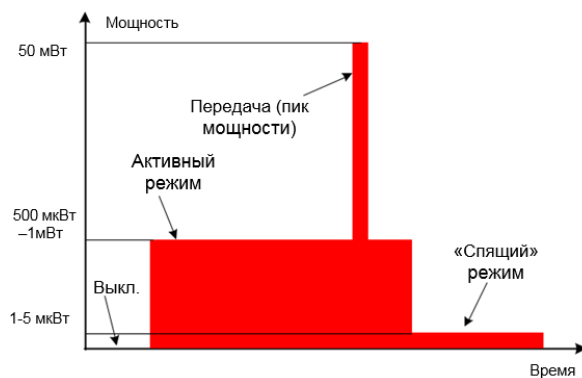


Рис. 5.3 - Графік споживання енергії вузлом БСМ

Аналіз наведеної діаграми дозволяє зробити такі висновки. По-перше, мінімальна потужність джерела енергії із зовнішнього середовища для побудови життєздатних бездротових вузлів повинна бути близько 1-5 мкВт, що відповідає достатній величині для «сплячого» режиму мікропроцесора і радіочастотного чіпа. По-друге, сучасні джерела енергії із зовнішнього середовища не можуть забезпечувати бездротові сенсорні мережі енергією, достатньою для активного режиму (споживання енергії 500 мкВт - 1 мВт проти 10-100 мкВт для вихідної потужності таких джерел). Однак, завдяки ультранизькому споживанню енергії в режимі сну, бездротові сенсорні мережі, що живляться від зовнішнього середовища, можуть використовувати переривчастий робочий цикл, зображений на рис. 5.4. Енергія зберігається в буфері (а) (конденсатори, батареї) і використовується для виконання

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 72

вимірювального циклу, як тільки енергії в буфері стає достатньо (б і в). Далі система знову повертається до сплячого режиму (г), очікуючи на новий вимірювальний цикл.

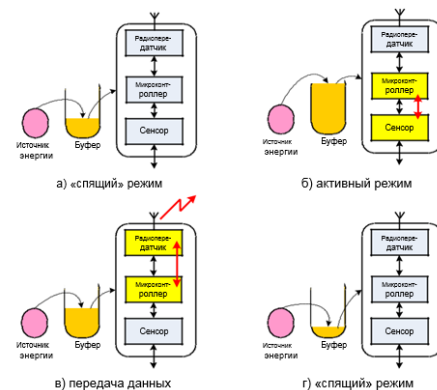


Рис. 5.4 – Робочий цикл бездротового сенсорного вузла

Таким чином, при використанні енергії зовнішнього середовища основною проблемою є адаптація частоти вимірювального циклу до енергії, що безперервно виробляється. Середнє енергоспоживання сенсорних вузлів (P) відповідає добутку загальної кількості енергії, що необхідна для одного вимірювального циклу (W), та частоти цієї дії (f) $P = W * f$.

Віддалене розташування сенсорів та їхня автоматична робота збільшує їх незахищеність від сторонніх вторгнень та атак. При бездротовому з'єднанні досить легко для порушника перехопити пакети, що передаються сенсорним вузлом. Наприклад, найбільша загроза здійснення атаки "відмови в обслуговуванні", мета якої порушити коректне функціонування сенсорної мережі. Це може бути досягнуто за допомогою різних способів, наприклад, при подачі потужного сигналу, який заважає сенсорним вузлам обмінюватися інформацією. Отже, сенсорні бездротові мережі вимагають нових рішень для створення ключів, їх розповсюдження, ідентифікації та захисту вузлів. Комунікації малої дальності використовують такі технології, як RFID, NFC, Bluetooth, ZigBee, Z-Wave, 6LoWPAN та ін. Реалізація бездротових персональних мереж WPAN великої ємності з низьким енергоспоживанням та низькою швидкістю передачі даних визначається стандартом IEEE 802.15.4.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 73

5.3. Стандарт IEEE 802.15.4

IEEE 802.15.4 - стандарт, який визначає фізичний (PHY) та канальний (англ. Data Link layer) рівні доступу до середовища для бездротових персональних мереж із низьким рівнем швидкості. Специфікація IEEE 802 розділяє канальний рівень на два підрівні: MAC (англ. media access control), що регулює доступ до фізичного середовища, та LLC (англ. logical link control), який забезпечує обслуговування мережевого рівня. Основним призначенням фізичного рівня є прийом і передача даних через радіоканал. Фізичний рівень визначає спосіб передачі даних, інтерфейс організації зв'язку, апаратні особливості та параметри, необхідні для побудови мережі. Насправді фізичний рівень управляє роботою трансивера, виконує вибір каналів, рівня потужності передавача та оцінює якість зв'язку. Дозволяється використання радіопристроїв без отримання окремих дозволів від організацій нагляду за частотами з максимальною еквівалентною ізотропно-випромінюючою потужністю 100мВт. У стандарті 802.15.4 фізично під обмін даними зарезервовані 27 каналів у трьох частотних діапазонах: 868 МГц, 910 МГц і 2,4 ГГц. Перша версія стандарту 802.15.4 визначала два фізичні рівні з широкосмуговою модуляцією з прямим розширенням спектру DSSS (Direct Sequence Spread Spectrum): перший – у смузі 868/915 МГц зі швидкістю передачі відповідно 20 та 40 кбіт/с з BPSK маніпуляцією, а другий – у смузі 2,45 ГГц із швидкістю 250 кбіт/с та з OQPSK маніпуляцією. У 2006 року допустимі швидкості передачі на частотах 868/915 МГц було збільшено до 100 і 250 кбіт/с. При збереженні широкосмугової модуляції DSSS стало можливо використання в діапазоні 868/915 МГц як BPSK, так і QPSK маніпуляції. З 2007 року згідно стандарту IEEE 802.15.4a кількість фізичних рівнів було збільшено до шести за рахунок включення рівня з надширокосмуговою радіотехнологією UWB (Ultra WideBand) для високошвидкісної передачі даних, а також специфікації з радіотехнологією розширення спектру методом лінійної частотної модуляції CSS (Chirp Spread Spectrum). Фізичний рівень UWB визначений виділеними частотами в трьох діапазонах: нижче 1 ГГц, 3-5 ГГц і 6-10 ГГц, а для CSS виділений спектр у смузі 2,45 ГГц. Використання надширокої смуги частот дозволяє UWB досягти швидкості передачі до 480 Мбіт/с на відстані до 3 м. На дистанціях до 10 м технологія дозволяє досягти лише 110 Мбіт/с.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 74

У 2009 році у версіях стандартів IEEE 802.15.4с та IEEE 802.15.4d була визначена можливість використання на фізичному рівні приймально-передавальних пристроїв QPSK маніпуляцією або з фазовою маніпуляцією більш високих порядків на частоті 780 МГц, а на частоті 950 МГц – з BPSK або гаусівською частотною маніпуляцією (GFSK).

Стандарт IEEE 802.15.4 забезпечує двосторонню напівдуплексну передачу даних (кадрів), перевірку та виправлення помилок, відправку кадрів на мережевий рівень. При цьому рівень MAC канального рівня регулює множинний доступ до фізичного середовища з поділом за часом і забезпечує безпеку, підтримуючи при цьому шифрування AES (Advanced Encryption Standard) — симетричний алгоритм блокового шифрування (довжина блоку вхідних даних 128 біт, а довжина ключа шифру становить 128, 192, або 256 біт). Доступ до каналу заснований на принципі Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) – багатостанційний доступ з контролем несучої та запобігання конфліктам. CSMA/CA – це мережевий протокол, у якому використовується принцип прослуховування несучої частоти. Пристрій, який готовий до передачі даних, посилає jam signal (сигнал затора) і прослуховує ефір. Якщо виявляється "чужий" jam signal, то передавач "засинає" на випадковий проміжок часу, а потім знову намагається розпочати передачу кадру. Таким чином, передачу може здійснювати лише один пристрій, що підвищує продуктивність мережі. При цьому дані передаються відносно невеликими пакетами, що характерно для трафіку сигналів управління та моніторингу БСС. Важливою особливістю стандарту є обов'язкове підтвердження доставки повідомлень. Особливістю пристроїв, об'єднаних у мережу за цим стандартом є низьке енергоспоживання за рахунок переходу трансивера в режим «засипання» за відсутності даних для пересилання та збереження підключення в цьому режимі. Зокрема, перехід приймача до активного стану триває близько 10-15 мс, а підключення до мережі нових пристроїв – від 30 мс.

Стандарт визначає два типи вузлів мережі:

Пристрій із повним набором функцій FFD (Fully Function Device):

підтримка стандарту IEEE 802.15.4;

додаткова пам'ять та енергоспоживання дозволяють виконувати роль координатора мережі;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 75

підтримка всіх типів топологій («точка-точка», «зірка», «дерево», «коміркова мережа»);

здатність виконувати роль координатора мережі та звертатися до інших пристроїв у мережі.

Пристрій з обмеженим набором функцій RFD (Reduced Function Device):

підтримує обмежений набір функцій IEEE 802.15.4;

підтримка топологій «точка-точка» та «зірка»;

не виконує функції координатора;

звертається до координатора мережі та маршрутизатора.

Координатори та маршрутизатори завжди відносяться до пристроїв FFD, а кінцеві пристрої можуть бути FFD або RFD. У будь-якій мережі повинен бути принаймні один FFD, що реалізує функцію координатора. Кожен пристрій має 64-розрядний ідентифікатор, але для з'єднань в персональній мережі PAN з обмеженою областю зв'язку може використовуватися короткий 16-розрядний ідентифікатор.

5.4. Стандарт ZigBee

На основі стандарту IEEE 802.15.4 ZigBee Alliance розробив специфікацію протоколів *мережевого і прикладного рівня*, які анонсував в грудні 2004 року під назвою "ZigBee". Мета технології ZigBee — це створення недорогої мережі, що самоорганізується, призначеною для вирішення широкого кола завдань. Основною областю застосування ZigBee є передача інформації в системах охорони, від рухомих і обертових частин механізмів (конвеєрів, роботів) промислових систем управління та моніторингу, відстеження маршрутів руху та місць розташування майна та інвентарю, створення бездротових сенсорних мереж. ZigBee створювався за критеріями малої дальності дії, низької ціни, низької споживаної потужності, низької швидкості передачі і малих габаритів. Ці властивості ідеально відповідають вимогам до більшості промислових датчиків. Тому ZigBee часто ототожнюють з промисловими бездротовими сенсорними мережами. ZigBee забезпечує максимальну швидкість передачі 250 кбіт/с з використанням OQPSK модуляції у діапазоні частот 2,4-2,483 ГГц, що розділений на канали шириною по 5 МГц кожен. Найбільшого поширення набули передавачі з потужністю 1 мВт, які забезпечують зв'язок на відстані до

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 76

10 м в приміщенні, а також передавачі з потужністю 10 мВт, що збільшують цю відстань до 80 м в приміщенні і до 1 км в умовах прямої видимості.

Модель OSI мережі ZigBee включає в себе фізичний і канальний рівні, які визначаються стандартом IEEE 802.15.4, а також мережевий рівень NWK (NetWoRK) і рівень підтримки додатків APL (Application Support Level).

Рівень NWK забезпечує:

- реєстрацію в мережі нового пристрою і виключення його з мережі;
- забезпечення безпеки при передачі фреймів;
- вказівку маршруту фрейму до місця призначення;
- прокладку маршрутів між пристроями в мережі;
- виявлення в мережі найближчих сусідів;
- запам'ятовування необхідної інформації про сусідні вузли.

У ZigBee є три типи пристроїв:

- координатор - формує топологію мережі і може встановлювати мости з іншими мережами. У кожній ZigBee мережі є тільки один координатор;
- маршрутизатор - працює як проміжна ланка, передаючи в потрібному напрямку дані від інших пристроїв;
- кінцевий пристрій - передає дані координатору або маршрутизатору і не може зв'язуватися з аналогічними йому пристроями.

Рівень NWK координатора відповідає за організацію нової мережі, коли це потрібно і призначення адрес нових пристроїв, що підключаються до мережі.

Рівень підтримки додатків APL забезпечує:

- визначення ролі пристроїв в мережі (координатор, маршрутизатор або кінцевий пристрій);
- обслуговування таблиць для зв'язування пристроїв мережі на основі інформації про необхідність і можливість зв'язування;
- передачу повідомлень між пов'язаними пристроями, фрагментацію, перекомпонування і транспортування даних;
- ініціювання або відповідь на запит з'єднання.

Основна особливість технології ZigBee полягає в тому, що вона при малому енергоспоживанні підтримує не тільки прості топології мережі («точка-точка», «дерево» і «зірка»), але і коміркову топологію, що самоорганізується і самовідновлюється, з ретрансляцією і маршрутизацією повідомлень. Типовою топологією мережі, що використовується за стандартом ZigBee є мережа з

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 77

кластерною архітектурою (рис. 5.5), сформованою зі звичайних вузлів, об'єднаних у кластери за допомогою маршрутизаторів. Маршрутизатори кластерів запитують сенсорні дані від пристроїв і, ретранслюючи їх один одному, передають координатору, який зазвичай має зв'язок із зовнішньою IP-мережею, куди і відправляє інформацію для накопичення та остаточної обробки.

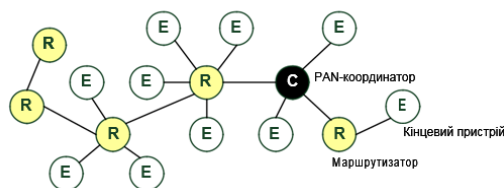


Рис. 5.5 - Мережа з кластерною архітектурою

Всі пристрої в мережі незалежно від топології повинні мати унікальну 64-бітну розширену адресу. Ця адреса використовується для комунікації в межах мережі або може бути змінена на коротку 16-бітову адресу, що виділяється координатором в процесі підключення пристроїв до мережі. Пристрої ZigBee мережі завдяки вбудованому програмному забезпеченню мають здатність при включенні живлення самі знаходити один одного і формувати мережу, а у разі виходу з ладу будь-якого з вузлів можуть встановлювати нові маршрути передачі повідомлень. Передавати інформацію між вузлами мережі можливо незалежно від відстані між ними, використовуючи проміжні вузли в якості ретрансляторів. Кілька мереж можуть взаємодіяти одна з одною. Для цього кожна мережа повинна мати унікальний мережевий ідентифікатор. Завдяки йому всередині мережі можуть використовуватися скорочені адреси. Тому повна адреса пристрою для доступу ззовні (з іншої мережі) складається з адреси мережі і короткої адреси пристрою.

В IEEE 802.15.4 існує три типи *передачі даних*:

- передача від кінцевого пристрою до мережевого координатора;
- передача від мережевого координатора до кінцевого пристрою;
- передача між двома одноранговими пристроями.

Підрівень MAC управляє доступом до каналу, формує *фрейм маячка* (маячок), перевіряє достовірність передачі фреймів, передає *фрейм*

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 78

підтвердження про отримання, виділяє гарантовані часові слоти та здійснює шифрування інформації.

Передбачається два механізми доступу до каналу CSMA/CA, в залежності від типу конфігурації мережі. У мережі з маячками використовується слотовий механізм доступу CSMA/CA, в якому початок часового слота для кожного пристрою має бути синхронізований з початком передачі маячка мережевим координатором. Суперфрейм з двох сторін обмежується маячками і ділиться на 16 рівних по довжині слотів (рис.5.6).

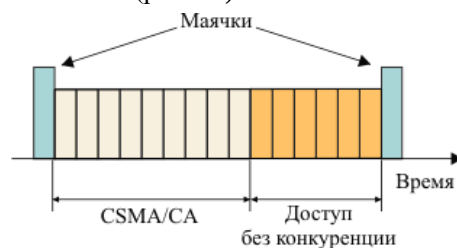


Рис. 5.6 - Структура суперфрейму

Фрейм маячка поміщається на місце першого слота кожного суперфрейму і використовується для синхронізації приєднаних пристроїв, для ідентифікації мережі і для опису структури суперфрейму. Будь-які пристрої, які бажають розпочати процес комунікації в проміжок часу між двома маячками, повинні використовувати слотовий механізм доступу CSMA/CA. Передача повідомлень повинна бути закінчена до приходу наступного маячка.

Оскільки пристрій не може почати передачу, поки не знайде маячок, а маячки розсилаються тільки мережевим координатором, то мережевий координатор за допомогою маячків виконує синхронізацію обміну в мережі. При цьому РНУ рівень повинен забезпечити, щоб всі передачі в мережі починалися одночасно з початком слотів. Введення описаної синхронізації дозволяє зменшити ймовірність одночасної передачі повідомлень декількома вузлами мережі.

Для пристроїв, які вимагають термінової доставки або великої пропускну здатності каналу, мережевий координатор може зарезервувати частину суперфрейму, в якому буде відсутня конкуренція за канал (рис. 5.6), оскільки в цей час мережевий координатор забороняє будь-яку передачу всім іншим

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 79

пристрою. Ця частина слотів суперфрейму називається *гарантованими часовими слотами*.

Коли пристрій збирається передати дані координатору в мережі з маячками, він спочатку намагається виявити маячок. Коли маячок знайдений, пристрій підлаштовується до структури суперфрейму. Пристрій передає дані координатору, використовуючи слотовий механізм CSMA/CA. У відповідь координатор відсилає *фрейм підтвердження* про отримання. На цьому цикл обміну закінчується.

Коли координатор бажає передати дані пристрою в мережі з маячками, він поміщає в маячок інформацію про те, що є дані, готові до передачі. Пристрій періодично аналізує вміст маячка і, якщо в ньому є інформація про наявність повідомлення, готового до передачі, пристрій передає команду запиту даних, використовуючи слотовий метод CSMA / CA. Координатор підтверджує прийом запиту даних за допомогою фрейму повідомлення. Слідом за цим координатор відсилає дані, використовуючи слотовий метод доступу CSMA/CA. Пристрій підтверджує прийом даних відправкою *фрейма підтвердження* про отримання.

Координатор може відключити режим повідомлень з маячками. У мережі без маячків використовується звичайний (безслотовий) механізм доступу CSMA/CA. Кожен раз, коли пристрій збирається почати передачу, він повинен витримати паузу випадкової величини після того, як канал звільниться. Випадкова затримка потрібна тому, що дуже ймовірно, що багато пристроїв мережі чекають звільнення каналу і тому після його звільнення можуть почати передачу одночасно. Якщо канал зайнятий, то пристрій може повторити спробу після повторної випадкової затримки.

Якщо координатор збирається передати дані без використання маячка, він запам'ятовує дані і чекає запиту від пристрою. Пристрій може передати команду запиту даних координатору, використовуючи безслотовий метод CSMA / CA. Координатор спочатку посиляє повідомлення про отримання (в тому ж циклі обміну), а потім, використовуючи CSMA / CA, відсилає дані та отримує повідомлення про отримання від пристрою. *Фрейми підтвердження* про отримання надсилаються відразу, без використання описаного алгоритму.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 80

Фрейм даних (рис. 5.7) починається з преамбули, яка спільно з полем "Старт" служить для синхронізації даних в приймачі, поле "Довжина" містить довжину поля MAC-підрівня в байтах.

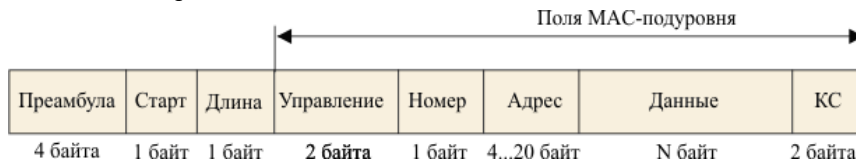


Рис. 5.7. Формат фрейму даних

Поле "Управління" містить службову інформацію про управління кадрами, поле "Номер" містить порядковий номер даних, поле "Адреса" містить адресну інформацію, в тому числі 16-бітну коротку або 64-бітну розширену адресу. Завершується фрейм полем контрольної суми КС.

5.5. Стандарт 6LoWPAN

6LoWPAN (IPv6 Low-Power Wireless Personal Area Network) – стандарт, який забезпечує взаємодію малих бездротових мереж з мережами IP за протоколом IPv6 із малим енергоспоживанням. Технологія використовується в основному для організації мереж датчиків та автоматизації житлового та офісного приміщення з можливістю керування через інтернет, проте може використовуватись і автономно для реалізації простих бездротових мереж датчиків. Цей протокол дозволяє передавати IP-пакети поверх стандарту IEEE 802.15.4 способом, що відповідає відкритим стандартам (протокол IPv6). Передача даних у стандарті 6LoWPAN забезпечує швидкість передачі від 50 до 200 Кбіт/с на відстань до 800 метрів. При цьому забезпечується взаємодія з іншими IP-каналами та пристроями. Протокол 6LoWPAN створений для малопотужних бездротових персональних мереж. В архітектурі мережі 6LoWPAN (рис. 5.8) визначено три типи логічних пристроїв (кінцевий вузол, маршрутизатор і шлюз), а також три види мереж: "Проста LoWPAN", "Розширена LoWPAN" та "Ad hoc LoWPAN". Як видно з рис. 5.8, "Ad hoc LoWPAN" не підключена до мережі зв'язку загального користування (МЗЗК), "Проста LoWPAN" підключена до МЗЗК через один шлюз, а "Розширена LoWPAN" включає кілька шлюзів, пов'язаних МЗЗК і один з одним за допомогою магістральної лінії зв'язку.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 81

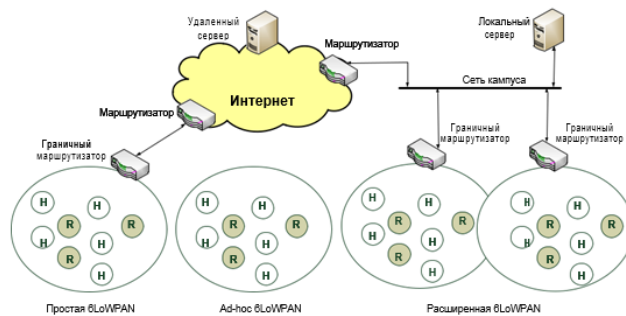


Рис. 5.8 - Архітектура мережі 6LoWPAN

Насамперед, мережі 6LoWPAN є підмережами IPv6-мереж, тобто, вони можуть взаємодіяти з іншими мережами та вузлами IP-мережі, але не є транзитними для її мережного трафіку. Вузол, що здатний виконувати маршрутизацію в межах 6LoWPAN, називається *роутером* або *маршрутизатором* R. Граничний маршрутизатор відповідає за взаємодію підмережі 6LoWPAN з мережею IPv6, бере участь у процедурі ініціалізації та маршрутизації у підмережі 6LoWPAN, здійснює компресію/декомпресію заголовків IPv6 при обміні із зовнішньою мережею, у разі підключення до мережі IPv4 може грати роль шлюзу IPv4. Мережі 6LoWPAN складаються з вузлів, які можуть виконувати роль маршрутизаторів, крім цього в мережі може бути один або більше так званих граничних маршрутизаторів. Участь у маршрутизації не є обов'язковою вимогою для вузла мережі і він може відігравати роль, аналогічну ролі кінцевого пристрою в мережах ZigBee. Вузли підмережі використовують 64-бітний префікс IPv6, який є частиною мережевої адреси граничного маршрутизатора. Для адресації всередині мережі використовується укорочена 16-бітна схема адресації. Як і мережі ZigBee, мережі 6LoWPAN є такими, що самоорганізуються.

Основні галузі застосування стандарту 6LoWPAN:

керування вуличним освітленням та промислова автоматика;
логістичні системи, відстеження товарів чи об'єктів інвентаризації;
охоронні системи і системи контролю та управління доступом.

Деякі області застосувань 6LoWPAN перекликаються з низкою стандартів ZigBee, проте в даному випадку конкуренція відсутня, швидше – взаємодія та

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 82

доповнення один одного, особливо щодо інтеграції сервісів, розширення зон дії мережі.

5.6. Радіомодуль ISM діапазону частот NRF24L01

При розробці електронних пристроїв нерідко виникає потреба в передачі даних на деяку відстань, наприклад, виміри вуличного датчика температури необхідно передати до засобу відображення, що знаходиться у приміщенні. У цих випадках зручно використовувати радіомодулі NRF24L01, що працюють в ISM діапазоні частот. Модуль NRF24L01 можливо використати при створенні системи бездротового доступу, мережевої системи збору даних, бездротової системи охорони, спостереження і моніторингу та ін. На рис.5.9 показаний зовнішній вигляд радіомодуля NRF24L01, з якого передусє, що модуль підключається до контролера через інтерфейс SPI. Принципова схема модуля у базовій комплектації наведена на рис. 5.10. Комплектація плати є базовою і містить сам чіп, штиркову колодку і антену у вигляді звивистої доріжки. Такий набір забезпечує дальність зв'язку до 100м при прямій видимості або до 30м у приміщенні.

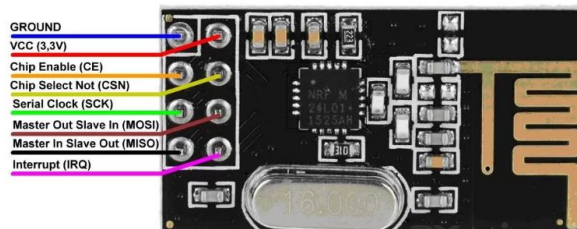


Рис. 5.9 - Зовнішній вигляд NRF24L01

Технічні характеристики модуля NRF24L01:

- напруга живлення 1,9В - 3,6;
- струм живлення: при вихідній потужності 0 дБм - 11,3 мА;
при вихідній потужності -18 дБм - 7,0 мА;
у режимі приймання на швидкості 2 Мбіт/сек - 12,3 мА;
у режимі Standby- 32 мкА;
- частота прийому та передачі 2,4,...,2,525 ГГц;
- час перемикання між каналами 130 мкс;
- тип модуляції: GFSK;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 83

- девіація частоти : ± 160 кГц при швидкості передачі даних 1Мбіт/с;
 ± 320 кГц при швидкості передачі даних 2Мбіт/с ;
- швидкість передачі даних: 0.25, 1, 2 Мбіт/с (задається програмно);
- потужність передавача: -18, -12, -6, 0 дБм (задається програмно);
- ширина одного радіоканалу 1МГц (на швидкості 2 Мбіт/сек використовується 2 канали);
- чутливість приймача: -82 dBm;
- коефіцієнт посилення антени: 2dBi;
- діапазон робочої температури -40°C , ..., 85°C .

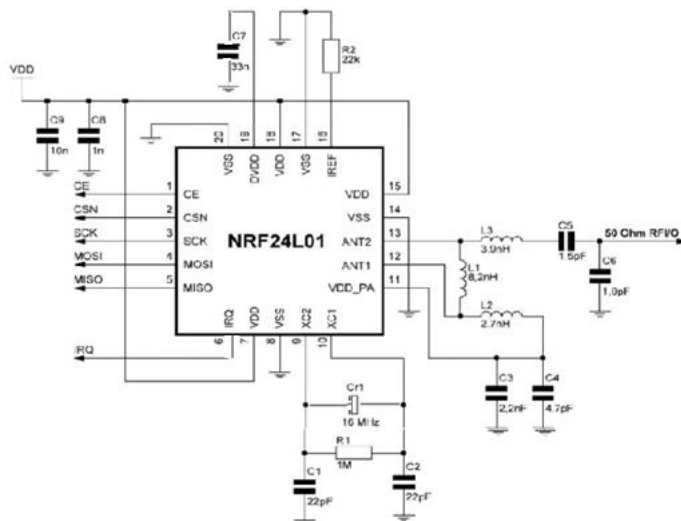


Рис. 5.10 - Принципова схема NRF24L01

Дальність зв'язку можна збільшити до 1000м, якщо придбати такі ж модулі, тільки з додатковим підсилювачем і зовнішньою антеною (рис.5.11).



Рис. 5.11 - NRF24L01 з підсилювачем і зовнішньою антеною

На одному частотному каналі одночасно можуть працювати 7 пристроїв (1 приймач і 6 передавачів) з різними адресами. Для організації двостороннього

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 84

зв'язку використовується два модуля NRF24L01, один з яких працює в режимі передавача, а інший як приймач на однаковій частоті. Якщо на одному каналі необхідно контролювати відразу кілька датчиків, наприклад, температуру в різних кімнатах, то в цьому випадку радіомодуль NRF24L01 передбачає можливість організації міні-мережі (рис.5.12). А саме, на одній частоті можуть працювати до 6 передавачів і 1 приймач. При цьому кожному передавачу присвоюється свій унікальний ідентифікатор («Pipe ID» або «Ідентифікатор труби»), а приймачу необхідно привласнити всі ідентифікатори тих передавачів, від яких він буде приймати дані.

Кожен ідентифікатор представляє з себе довільне число, що складається з 5 байт, але він повинен задаватися за певними правилами, а саме:

- на одному і тому ж каналі ідентифікатор кожного передавача повинен бути обов'язково унікальним;
- щоб приймач міг приймати дані від передавачів, йому повинні бути вказані їх ідентифікатори;
- ідентифікатори Pipe0 і Pipe1 повинні відрізнятися всіма п'ятьма байтами, наприклад, Pipe0= 0x7878787878 , а Pipe1= 0xB4B5B6B7F1;
- ідентифікатори Pipe2 - Pipe5 повинні відрізнятися від Pipe1 тільки останнім байтом, наприклад: Pipe1= 0xB4B5B6B7F 1;

Pipe2 = 0xB4B5B6B7CD; Pipe3 = 0xB4B5B6B7A3;

Pipe 4 = 0xB4B5B6B70F; Pipe 5 = 0xB4B5B6B705.

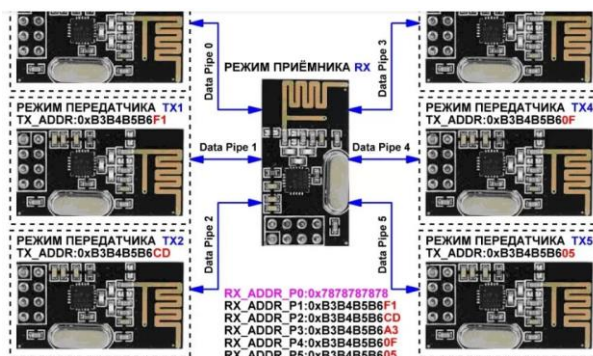


Рис. 5.12 - Організації міні-мережі NRF24L01

NRF24L01 можна зустріти в таких пристроях, як бездротова клавіатура, миша, джойстик; системи охорони та бездротового доступу; системи спостереження і моніторингу; радіокеровані іграшки та багато іншого.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 85

5.7. Технологія ESP-NOW для мікроконтролерів ESP8266 і ESP32

ESP-NOW - це спрощений протокол зв'язку WiFi з передачею коротких пакетів між парами пристроїв, розроблений для мікроконтролерів ESP8266 і ESP32 компанією Espressif в 2016р. Додаткові процедури, пов'язані з підтримкою протоколу WiFi, не використовуються, що прискорює процес обміну пакетами. ESP-NOW підтримує такі функції:

зашифрований і незашифрований зв'язок між не більше ніж 20 парами пристроїв;

використовується протокол з низьким енергоспоживанням для передачі до 250 байт корисної інформації із швидкістю передачі не більше 1 Мбіт/с;

настроювання зворотнього виклику для інформування прикладного рівня, зокрема, про успішність або збій передачі.

Для забезпечення безпеки ESP-NOW застосовує протокол шифрування 802.11i Counter/CBC-MAC (CCMP - протокол зчепленого блочного шифрування Cipher Block Chaining з кодом автентичності повідомлення Message Authentication Code (MAC) в режимі лічильника). Протокол CCMP складається із двох алгоритмів:

AES (Advanced Encryption Standard) – шифрування з використанням 128-бітного ключа в режимі лічильника;

CBC-MAC - використовується для перевірки цілісності повідомлення.

З ESP-NOW кожна плата може бути відправником та одержувачем одночасно (рис. 5.13). Щоб надсилати повідомлення через ESP-NOW, потрібно знати унікальну MAC-адресу плат.



Рис. 5.13 - Відправлення даних по структурі «one-slave- one –master»

Якщо потрібно зібрати дані з декількох плат на одну, наприклад, для відображення на Web-сервері даних від декількох датчиків, то можна використати конфігурацію «one-slave - multiple-master» (рис. 5.14,а). Також можливо утворити конфігурацію «one-master - multiple-slaves» (рис.5.14,б). При цьому одна плата ESP32 надсилає команди на різні плати ESP32. Ця

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 86

конфігурація ідеальна для створення чогось на зразок пульта дистанційного керування, коли потрібно управляти з однієї основної плати ESP32 декількома платами.



Рис. 5.14 - Відправлення даних за різними конфігураціями

Також можна створити конфігурацію, у якій плати ESP32 взаємодіятимуть одна з одною та отримати щось схоже на мережу (рис.5.15).



Рис. 5.15 - Відправлення даних по структурі «multiple -master-multiple-slaves»

Технологія ESP-NOW може застосовуватися в IoT для керування інтелектуальними джерелами світла, реле, розетками, іншими пристроями дистанційного керування, отримання інформації від датчиків та т. і.

6. Технології передачі даних в IoT

6.1. Стандарт Z-Wave

Z-Wave – це перший відкритий бездротовий стандарт домашньої автоматизації (системи «розумний» будинок), в основі якої лежить мережа. Він заснований на специфікації Z-Wave ITU G.9959 та визначає всі аспекти взаємодії пристроїв, що підтримують цей протокол, а також забезпечує їхню

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 87

сумісність. Технологія використовує малопотужні та мініатюрні радіочастотні модулі, які вбудовуються у побутову електроніку та різні системи, такі як освітлення, опалення, контроль доступу, розважальні системи та побутову техніку. На відміну від Wi-Fi та інших стандартів передачі даних IEEE 802.11, призначених в основному для великих потоків інформації, стандарт Z-Wave використовує модуляцію GFSK в діапазоні частот до 1 ГГц (869,0 МГц - Росія; 908,42 МГц - США; 868,42 МГц - Європа; 919,82 МГц - Гонконг; 921,42 МГц - Австралія) та оптимізований для передачі простих керуючих команд (пропускна спроможність: 9,6, 40 або 100 кбіт/с). Вибір низького радіочастотного діапазону для Z-Wave обумовлюється малою кількістю потенційних джерел перешкод (на відміну від завантаженого діапазону 2,4 ГГц, в якому доводиться вдаватися до заходів, що зменшують можливі перешкоди від різних побутових бездротових пристроїв, що працюють – Wi-Fi, ZigBee, Bluetooth. Радіус дії залежить від виду антени і складає приблизно 30 метрів за умов прямої видимості, а у приміщенні зменшується залежно від форми та матеріалу стін.

Z-Wave використовує коміркову (mesh) топологію мережі з маршрутизацією повідомлень від джерела (англ. source routing) і має один основний контролер і нуль або більше вторинних контролерів, які управляють маршрутизацією і безпекою. У комірковій мережі Z-Wave кожен вузол або пристрій може приймати та передавати керуючі сигнали іншим пристроям мережі, використовуючи сусідні проміжні вузли. Це мережа з маршрутизацією, що самоорганізується, залежною від зовнішніх факторів – наприклад, при виникненні перешкоди між двома найближчими вузлами мережі, сигнал піде через інші вузли мережі, що знаходяться в радіусі дії. Як алгоритм шифрування використовується алгоритм AES-128.

Таким чином, мережа Z-Wave може мати радіус передачі набагато більший, ніж дальність передачі одного вузла. Однак через переприйом (hops) може бути отримана невелика затримка між командою управління та бажаним результатом. Для того щоб Z-Wave пристрої мали можливість маршрутизувати дані, що ними не запитуються, вони не можуть знаходитися в сплячому режимі. Отже пристрої з живленням від батарейок не призначені як пристрої ретрансляції. Мережа Z-Wave може включати до 232 пристроїв з можливістю розширення мережі, якщо потрібно ще кілька пристроїв. Додаткові пристрої в

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 88

мережу можуть бути додані в будь-який час, так само як і кілька контролерів, що управляють. Хоча технологія Z-Wave є простим та дешевим рішенням, низька швидкість передачі даних виключає передачу зображень, звуку та високошвидкісних даних. Крім того, для рішень, де потрібні більше 30 пристроїв, Z-Wave-система є більш дорогою, ніж кабельні системи. Через свої конструктивні особливості такі системи мають обмежені масштаби і радіус дії, і вимагають використання повторювачів або навіть кабельних з'єднань.

6.2. Стандарт Bluetooth

Bluetooth (IEEE 802.15.1) — технологія бездротового зв'язку, основним призначення якої є забезпечення економного (з точки зору споживаного струму) і дешевого радіозв'язку між різноманітними типами електронних пристроїв, таких як мобільні телефони та аксесуари до них, портативні та настільні комп'ютери, принтери та інші. Причому, велике значення приділяється компактності електронних компонентів, що дає можливість застосовувати Bluetooth у малогабаритних пристроях розміром з наручний годинник.

Інтерфейс Bluetooth дає змогу передавати як голос (зі швидкістю 64 Кбіт/с), так і дані. Для передачі даних можуть бути використані асиметричний (721 Кбіт/с в одному напрямку і 57,6 Кбіт/с в іншому) та симетричний (432,6 Кбіт/с в обох напрямках) методи. Працюючи на частоті 2,4 ГГц, прийомопередавач Bluetooth дає змогу встановлювати зв'язок у межах від 10 до 100 метрів. Різниця у відстані, безумовно, велика, однак з'єднання в межах 10 метрів дає змогу зберегти низьке енергоспоживання (малопотужний передавач споживає всього 0,3 мА в режимі standby і в середньому 30 мА під час обміну інформацією), компактний розмір і досить невисоку вартість компонентів. У стандарті Bluetooth передбачене шифрування даних, що передаються з використанням ключа ефективною довжини від 8 до 128 біт і можливістю вибору односторонньої або двосторонньої аутентифікації. Додатково, до шифрування на рівні протоколу, може бути використано шифрування на програмному рівні.

Bluetooth використовує GFSK- модуляцію та технологію FHSS (англ. Frequency-hopping spread spectrum) з відстанню 1 МГц між каналами. При цьому передавач розбиває дані на пакети і передає їх за псевдовипадковим

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 89

алгоритмом стрибкоподібної перебудови частоти (1600 разів в секунду), або за шаблоном, складеним з 79 підчастот. «Зрозуміти» один одного можуть тільки ті пристрої, які налаштовані на один і той самий шаблон передачі — для сторонніх приладів передана інформація буде звичайним шумом.

Основним напрямком використання Bluetooth має стати створення PAN мереж, які включають такі різнопланові пристрої, як мобільні телефони, MP3-плеєри, комп'ютери, клавіатура або мишу. Можливість передачі голосу дає змогу вбудовувати інтерфейс Bluetooth в бездротові гарнітури для телефонів. Інтерфейс дає змогу з невеликими витратами організувати домашню мережу. Причому вузлами цієї мережі можуть бути будь-які пристрої, що мають потребу в інформації або володіють необхідною інформацією. Основним структурним елементом мережі Bluetooth є так звана «пікомережа» — сукупність від 2 до 8 пристроїв, що працюють на одному і тому ж шаблоні. У кожній пікомережі один пристрій працює як активний, а інші як пасивні. Активний пристрій визначає шаблон, на якому працюватимуть усі пасивні пристрої його пікомережі, і синхронізує її роботу. Стандарт Bluetooth передбачає з'єднання до 10 незалежних і навіть не синхронізованих між собою пікомереж. Для цього кожна пара пікомереж повинна мати як мінімум один спільний пристрій, який буде активним в одній і пасивним в іншій.

Радіус роботи пристроїв BT2 не перевищує 15 метрів, для BT1 до 100 м (клас A). Ці числа декларуються стандартом для прямої видимості, в реальності не варто очікувати роботу на відстані понад 10-20 м.

Перед початком процедури сполучення на обох сторонах необхідно ввести PIN-код, а у процесі встановлення зв'язку відбувається генерація ключа зв'язку, який містить унікальну MAC-адресу (аналог IP-адреси) BT-пристрою, довжиною 48 біт, що встановлюється виробником, PIN -код і випадкову 128-бітову величину.

Технологія *Bluetooth Low Energy (BLE)* є технологією бездротового зв'язку для ближніх комунікацій та, на відміну від попередніх стандартів – Bluetooth, орієнтований на застосування у системах забезпечення безпеки, управління електроприладами та передавання показань датчиків, медичних приладів, спортивних тренажерів з автономним живленням. BLE забезпечує швидкість передавання 1 Мбіт/с і при цьому споживає в 10 разів менше енергії, ніж класичні Bluetooth-рішення. Пристрої BLE працюють у діапазоні 2,4 ГГц. У

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 90

стандарті визначено 40 частотних каналів з відстанню 2 МГц між каналами. Фізично застосована GFSK-модуляція з індексом модуляції в межах від 0,45 до 0,55, що дозволяє зменшити пікове споживання енергії. Технологія адаптивної стрибкоподібної перебудови частоти, що використовується в BLE, дозволяє пристроям швидко змінювати робочу частоту широкому діапазоні робочих частот. Це не тільки дозволяє знизити інтерференцію, а й зменшити або повністю уникнути переповнення робочого частотного діапазону.

На відміну від технологій сенсорних мереж, таких як ZigBee, 6LoWPAN або Z-Wave, орієнтованих на розгалужені розподілені мережі з численними передачами даних між вузлами мережі, стандарт BLE розрахований на топології типу «точка-точка» та «зірка». Поряд із широкомовним режимом, BLE пропонує спосіб передачі даних, орієнтований на встановлене між окремими пристроями з'єднання.

Незважаючи на те, що деякі функції контролера BLE запозичені у класичного Bluetooth, вони не сумісні між собою. Для взаємодії з-поміж них хоча б одне із пристроїв має бути дворежимним, тобто. підтримувати обидва протоколи. Однорежимні пристрої мають найменше енергоспоживання і в основному є кінцеві виконавчі пристрої. Дворежимні пристрої передбачають можливість періодичного отримання енергії, розташовуються на різних мобільних пристроях, а також можуть функціонувати як звичайні Bluetooth-пристрої.

Однорежимні пристрої можуть застосовуватися як бездротовий інтерфейс датчиків з батарейним живленням, що застосовуються як окремо, так і у складі інших пристроїв - у годинниках, пульсометрах, крокомірах, домашніх тонометрах, термометрах тощо. У складі мобільних пристроїв BLE може бути використаний для керування домашньою автоматикою, пристроями освітлення або охорони щонайменше в межах одного приміщення. Для управління пристроями в межах всього будинку можливе використання BLE як шлюзу між керуючим пристроєм та мережею домашньої автоматики.

6.3. Стандарт Wi-Fi

Основне призначення технологи Wi-Fi (IEEE 802.11) - бездротове розширення мереж Ethernet. Wi-Fi – одна з найпопулярніших груп стандартів і повсюдно використовується для організації домашніх та офісних мереж,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 91

публічного доступу до Інтернету в готелях, кафе, магазинах та інших публічних місцях. Набув широкого поширення завдяки використанню в мобільних пристроях та ноутбуках. Стек протоколів стандарту IEEE 802.11 складається з фізичного рівня та канального рівня з підрівнями управління доступом до середовища MAC та логічної передачі даних LLC (Logical Link Control). Технологія 802.11 визначається двома нижніми рівнями, тобто фізичним рівнем і рівнем MAC, а рівень LLC виконує свої стандартні загальні для всіх технологій LAN функції.

Рівень MAC забезпечує доступ до середовища, мобільність станцій за наявності декількох базових станцій та забезпечення безпеки локальної мережі.

На фізичному рівні існує кілька варіантів специфікацій, які відрізняються використанням частотним діапазоном, методом кодування і як наслідок – швидкістю передачі даних.

Спочатку стандарт IEEE 802.11 передбачав можливість передачі даних по радіоканалу в діапазоні частот 2,4 ГГц з використанням технології FHSS на швидкості не більше 1 Мбіт/с при GFSK-модуляції радіосигналу або на швидкості до 2 Мбіт/с – при використанні 4GFSK-модуляції. Також передбачалось використовувати технологію прямого розширення спектру (DSSS) та DBPSK-модуляцію при передачі даних на швидкості не більше 1 Мбіт/с або на швидкості не більше 2 Мбіт/с з використанням DQPSK-модуляції.

Стандарт IEEE 802.11b у діапазоні частот 2,4 ГГц передбачає використання кодування за допомогою комплементарних кодів CCK (Complementary Code Keying), забезпечуючи швидкість передачі до 11 Мбіт/с.

Стандарт IEEE 802.11a на частоті 5 ГГц передбачає використання BPSK, QPSK, 16-QAM та 64QAM модуляції з ортогональним частотним мультиплексуванням каналів OFDM (Orthogonal frequency-division multiplexing) та забезпечує швидкість передачі від 6 до 54 Мбіт/с.

Стандарт IEEE 802.11g передбачає використання діапазону частот 2,4 ГГц, забезпечуючи швидкість з'єднання до 54 Мбіт/с.

Стандарт IEEE 802.11n теоретично здатний забезпечити швидкість передачі даних до 600 Мбіт/с, застосовуючи передачу даних відразу за чотирма антенами. Під час роботи з однієї антени – швидкість до 150 Мбіт/с. Пристрої 802.11n працюють у діапазонах частот 2,4 ГГц або 5,0 ГГц.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арк. ___ / 92

До складу стандарту IEEE 802.11 входить також технологія IEEE 802.11s, яка дозволяє організувати ієрархічні бездротові mesh-мережі з мобільними та статичними вузлами та розширює функціональність бездротового доступу в Інтернет.

Як перспективу цієї технології можна розглядати стандарт IEEE 802.11ac для бездротових локальних мереж, що працюють на частотах 5,...,6 ГГц. Максимальна теоретична пропускна здатність становить 6933,3 Мбіт/с і забезпечується при ширині каналу 160 МГц та використанні технології просторового мультиплексування MU-MIMO (Multi-User Multiple-Input/Multiple-Output) з формуванням адаптивної діаграми спрямованості антени (“beamforming”) за допомогою восьми антен. А стандарт IEEE 802.11ad передбачає можливість «кімнатного» використання пристроїв передачі даних зі швидкістю до 6,76 Гбіт/с, що застосовують технологію “beamforming” у діапазоні частот 60 ГГц при ширині каналу передачі 2160 ГГц. Для зручності порівняння різні специфікації стандарту IEEE 802.11 зведені до табл.6.1.

Таблиця 6.1 - Характеристики стандартів IEEE 802.11

Стандарт	Діапазон, ГГц	Смуга каналу, МГц	Вид модуляції	Антенна технологія	Максимальна швидкість передачі
802.11b	2,4	20	ССК	-	11 Мбіт/с
802.11g	2,4	20	ССК, OFDM	-	54 Мбіт/с
802.11a	5	20	OFDM (до 64 QAM)	-	54 Мбіт/с
802.11n	2,4; 5	20, 40	OFDM (до 64 QAM)	MU-MIMO, до 4 потоків Beamforming	600 Мбіт/с
802.11ac	5	40, 80, 160	OFDM (до 256 QAM)	MU-MIMO - 8 потоків Beamforming	6,93 Гбіт/с
802.11ad	60	2160	SC/OFDM	Beamforming	6,76 Гбіт/с

У таблиці SC-OFDMA (Single Carrier Orthogonal Frequency Division Multiple) – це множинний доступ з ортогональним частотним розділенням каналів з одною несучою.

Стандарт IEEE 802.11 встановлює *три варіанти топології мереж*:

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 93

- незалежні базові зони обслуговування (Independent Basic Service Sets, IBSS);
- базові зони обслуговування (Basic Service Sets, BSS);
- розширені зони обслуговування (Extended Service Sets, ESS).

Під зоною обслуговування тут розуміється набір логічно згрупованих пристроїв. Кожна зона обслуговування має свій ідентифікатор (Service Set Identifier, SSID). Станція-приймач використовує SSID для визначення того, з якої зони обслуговування приходить сигнал. В архітектурі IBSS станції зв'язуються безпосередньо одна з одною, без використання точки доступу, у якості якої виступає центральний вузол зв'язку, що підключається до дротової локальної мережі Ethernet. IBSS використовується зазвичай для об'єднання в мережу малої кількості станцій, оскільки в ній не передбачена можливість ретрансляції сигналу для збільшення дальності зв'язку. При використанні BSS станції спілкуються одна з одною через точку доступу. Розширена зона обслуговування ESS виходить при об'єднанні кількох BSS в єдину систему за допомогою розподільної системи, в якості якої може виступати дротова мережа Ethernet.

Wi-Fi використовує метод доступу до мережі CSMA/CA, в якому для зниження ймовірності колізій використані наступні принципи:

- перш, ніж станція почне передачу, вона повідомляє, як довго вона буде займати канал зв'язку;
- наступна станція не може почати передачу, поки не закінчиться зарезервованний раніше час;
- учасники мережі не знають, чи прийнятий їх сигнал, поки не отримають підтвердження про це;
- якщо дві станції почали працювати одночасно, вони зможуть дізнатися про це тільки по тому факту, що не отримають підтвердження про прийом;
- якщо підтвердження не отримане, учасники мережі вичікують випадковий проміжок часу, щоб почати повторну передачу.

Запобігання, а не виявлення колізій, є основним в бездротових мережах, оскільки в них, на відміну від провідних мереж, передавач трансивера заглушає сигнал, що приймається. У табл.6.2 зведені основні характеристики розглянутих бездротових технологій.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 94

Таблиця 6.2 - Бездротові технології IoT

Стандарт	Частота, МГц	Швидкість, Мбіт/с	Дальність, м
Wi-Fi	2400	1- 54	до 100
ZigBee	2400	0,25	10-100
6LoWPAN	-	до 0,2	до 800
Z-Wave	До 1000	до 0,1	до 30
Bluetooth	2400	0,72	10-100

6.4. Технологія LPWAN

LPWAN (англ. Low-power Wide-area Network) - бездротова технологія передачі невеликих за обсягом даних на дальні відстані, розроблена для розподілених мереж телеметрії, M2M та «Інтернету речей». Її особливість - низьке енергоспоживання і широке територіальне охоплення. LPWAN є однією з бездротових технологій, що забезпечують середовище збору даних з різного устаткування. Використовуючи підхід LPWAN, створюються пристрої, здатні передавати інформацію на десятки кілометрів і при цьому працювати протягом декількох років на одній батареї. В основі принципу передачі даних за технологією LPWAN на фізичному рівні *PHY* лежить властивість радіосистем - збільшення енергетики, а значить і дальності зв'язку при зменшенні швидкості передачі. Чим нижче бітова швидкість передачі, тим більше енергії вкладається в кожен біт і тим легше виділити його на тлі шумів в приймальній частині системи. Таким чином, низька швидкість передачі даних дозволяє домогтися більшої дальності їх прийому.

Підхід, який використовується для побудови LPWAN-мережі, схожий з принципом роботи мереж мобільного зв'язку. LPWAN-мережа використовує топологію «зірка», де кожен пристрій взаємодіє з базовою станцією безпосередньо.

Пристрій з LPWAN-модулем передає дані по радіоканалу на базову станцію. Станція приймає сигнали від всіх пристроїв в радіусі своєї дії, оцифровує і передає на віддалений сервер, використовуючи доступний канал зв'язку: Ethernet, стільниковий зв'язок. Отримані на сервері дані використовуються для відображення, аналізу, побудови звітів та прийняття рішень. Управління пристроями, оновлення програмного забезпечення

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 95

відбувається з використанням зворотного каналу зв'язку. Для передачі даних через мережу, як правило, застосовується неліцензований спектр частот, дозволених до вільного використання в регіоні побудови мережі. Місце LPWAN серед інших бездротових технологій показано на рис. 6.1.

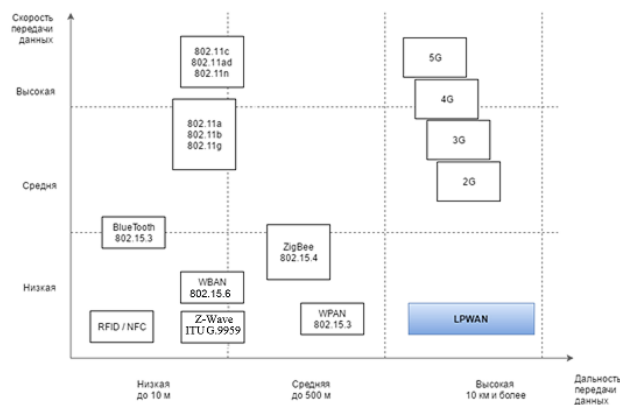


Рис. 6.1 - Порівняння LPWAN з іншими бездротовими технологіями

Переваги LPWAN. Дальність передачі сигналу досягає 10-15 км. Низький рівень споживання енергії у кінцевих пристроїв, завдяки мінімальним витратам енергії на передачу невеликого пакета даних. Висока масштабованість мережі на великих територіях. Відсутність необхідності отримання частотного дозволу та плати за радіочастотний спектр, внаслідок використання неліцензованого ISM діапазону частот.

Недоліки LPWAN. Відносно низька пропускна здатність, в залежності від використовуваної технології передачі даних на фізичному рівні, становить від кількох сотень біт/с до декількох десятків кбіт/с. Затримка передачі даних від датчика до кінцевого додатка, пов'язана з часом передачі сигналу, може досягати від декількох секунд до декількох десятків секунд. Відсутність єдиного стандарту, який визначає фізичний шар і управління доступом до середовища для бездротових LPWAN-мереж.

Області застосування. Технологія LPWAN орієнтована на програми, що вимагають гарантованої передачі невеликого обсягу даних, можливості тривалої роботи мережевих пристроїв від автономних джерел живлення, великого територіального охоплення бездротовою мережею. Основними областями застосування технології LPWAN є бездротові сенсорні мережі,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 96

автоматизація збору показників приладів обліку, системи промислового моніторингу та управління.

Коли говорять про технології LoRa, то найчастіше мають на увазі метод модуляції LoRa, розроблений Semtech, і відкритий протокол LoRaWAN.

Якщо модуляція LoRa є, фізичним рівнем, то LoRaWAN - це MAC протокол канального рівня для мереж з великою кількістю вузлів з великим радіусом дії і низьким власним енергоспоживанням.

Фізичний радіоінтерфейс LoRa заснований на використанні широкосмугових радіосигналів з великою базою В, що багато більше одиниці. Даний вид радіосигналів має дві головні особливості:

- ширина спектра радіосигналу BW значно більше швидкості передачі даних;
- кореляційна функція істотно вузька кореляційної функції вузькосмугового сигналу.

Частотна надмірність широкосмугового радіосигналу обумовлює його високу стійкість перед перешкодами, а вузька кореляційна функція - високу точність часової синхронізації. Широкосмуговий радіосигнал LoRa є сигналом з лінійною частотною модуляцією CSS (Chirp Spread Spectrum). Частота CSS радіосигналу може як збільшуватися, так і зменшуватися. Передавачі LoRa формують CSS радіосигнали з шириною спектра $BW = 125,25$ або 500 кГц. За рахунок зміни тривалості символу T_{sym} , при фіксованій ширині спектру радіосигналу BW, можлива зміна бази радіосигналу $V = BW \cdot T_{\text{sym}} = 2^{\text{SF}}$, що демонструється рис.6.2.

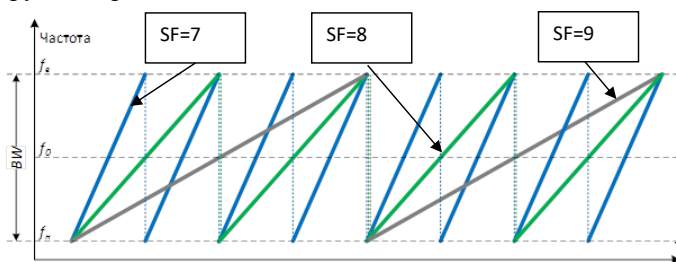


Рис. 6.2 – CSS радіосигнал

Технологія LoRa використовує асинхронний режим прийому-передачі при якому передавач може почати генерацію радіосигналу в будь-який момент часу. В цьому випадку потрібно мати механізм, що забезпечує синхронізацію

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 97

приймача по сигналу від передавача (аналог "старт-біта" протоколу RS232). В якості такого механізму використовується преамбула, що передуює кожному сеансу зв'язку (рис.6.3). Преамбула включає в себе послідовність символів, що дозволяють приймачу виявити активність передавача, визначити використовуваний передавачем коефіцієнт розширення спектра SF і виконати символну синхронізацію. По завершенні преамбули слідує слово синхронізації, що визначає початок блоку даних і безпосередньо блок даних фізичного рівня. Довжина слова синхронізації налаштовується в діапазоні від 1 до 8 байт.

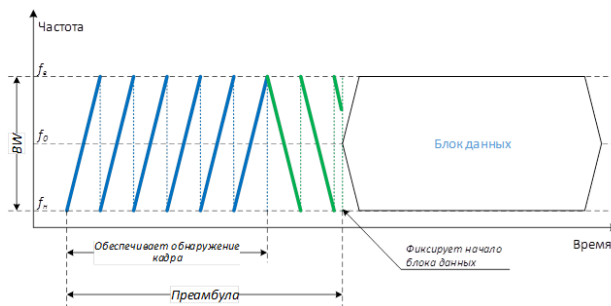


Рис. 6.3 – Кадр CSS радіосигналу

Принцип передачі символів інформації блоку даних фізичного рівня за допомогою широкосмугового радіосигналу LoRa полягає у частотному зміщенні $k\Delta\omega$ прийнятого сигналу відносно опорного CSS радіосигналу, де $k=0,1,2,\dots,2^{SF}$ – інформаційний символ розмірністю SF біт (рис. 6.4). При цьому при різних

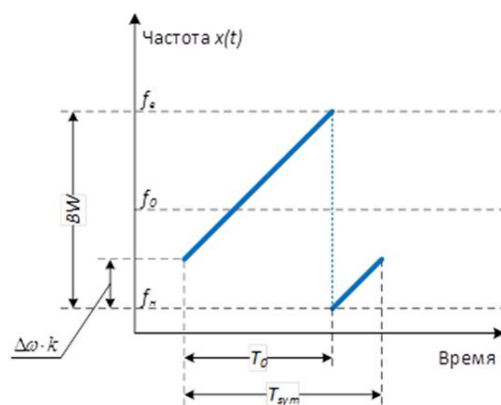


Рис. 6.4 – Принцип передачі символів CSS радіосигналу

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 98

значеннях k повинна виконуватись нерівність $\Delta\omega < \frac{BW}{2 \cdot k}$. Отже, виходячи з того,

що $\Delta\omega = \frac{BW}{2^{SF+1}}$, а $T_0 = \frac{(2^{SF+1} - k)}{2^{SF+1}} \cdot T_{sym}$, визначивши значення k інформаційного символу розмірністю SF біт, можна визначити значення бітів символу, що були передані на інтервалі часу $T_{sym} = 2^{SF}/BW$.

Мережа LoRaWAN має просту архітектуру типу "зірка" без ретрансляторів і mesh-зв'язків (рис. 6.5). Протокол LoRaWAN оптимізований для кінцевих пристроїв і включає в себе різні класи вузлів, забезпечуючи компроміс між швидкістю доставки інформації і часом роботи пристроїв при використанні живлення від акумулятора. Протокол забезпечує повний двосторонній зв'язок, а архітектура, за допомогою спеціальних методів шифрування, забезпечує загальну надійність і безпеку всієї системи.

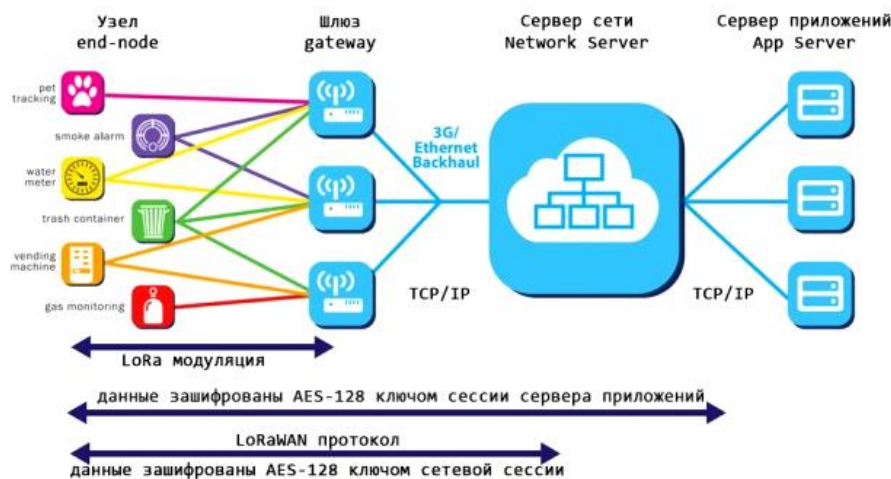


Рис. 6.5 – Архітектура мережі LoRaWAN

У типовій LoRaWAN мережі шлюзи передають зашифровані дані, отримані від кінцевих пристроїв (end-node) на центральний сервер мережі провайдера (Network Server) і далі на сервер додатків (App Server) сервіс-провайдера, з якого дані надходять кінцевому користувачеві.

Мережевий стек LoRaWAN іноді ще називають LoRaMAC, щоб підкреслити, що він працює на другому рівні моделі OSI.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арх. ___ / 99

Кінцеві пристрої LoRa виконують такі функції, як вимір або управління і контроль. Вони розташовуються віддалено і мають, як правило, батарейне живлення. Використовуючи мережевий протокол LoRaWAN, ці кінцеві пристрої налаштовані для зв'язку з шлюзом LoRa (концентратором або базовою станцією).

Дані в LoRaWAN мережі можуть передаватися в обидві сторони, як від кінцевих пристроїв до сервера, так і назад. Кінцеві пристрої передають дані не постійно, а включають передачу лише на деякий проміжок часу (як правило на 1-5 секунд), після закінчення якого відкривається два часових вікна для прийому даних. Решту часу трансивери кінцевих вузлів знаходяться або в неактивному стані (sleep), або в стані прийому, в залежності від класу пристрою (А, В або С).

Вузол класу А передає дані на шлюз короткими посилками за заданим графіком. Ініціатором обміну виступає сам кінцевий вузол. Кінцевий пристрій, як правило, не вимагає отримання підтвердження свого повідомлення додатком (повідомлення без квитанцій), однак протокол передбачає і повідомлення, на які сервер додатків формує спеціальну відповідь, "квитанцію", а мережевий сервер вибирає найкращий маршрут (шлюз) для відправки підтвердження в момент відкриття вузлом вікна прийому (повідомлення з квитанціями). Кінцевий пристрій переходить в режим прийому (відкриває вікно прийому) відразу після відправки даних на деякий нетривалий час, в іншому випадку, більш тривалий час, знаходиться в режимі енергозбереження або сну. Сервер накопичує для кінцевих пристроїв повідомлення і пересилає їх відразу, як кінцевий пристрій виходить на зв'язок. Цей клас кінцевих вузлів найбільш економічний у використанні енергії та найбільш поширений на практиці.

Вузол класу В включає приймач за графіком, заданому сервером. Сервер відправляє повідомлення вузлу відповідно до розкладу. Ініціатором обміну може бути і сервер LoRaWAN мережі. Пристрої цього класу синхронізують внутрішній час з часом мережі за допомогою маяків, які пристрій регулярно отримує від шлюзу. Вузли цього класу мають відносно низьку часову затримку в обміні даними і відкривають більш широке часове вікно прийому в порівнянні з класом А. Вузли класу В також мають всі можливості пристроїв класу А.

У вузла класу С вікно прийому відкрито постійно і закривається тільки на період короткочасної передачі даних. Сервер може ініціювати обмін в будь-

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 100

який час і передати повідомлення вузлу відразу, у міру їх появи. Цей клас пристроїв споживає найбільшу кількість енергії (в порівнянні з класами А і В), тому зазвичай не використовує батарейне живлення, але отримує дані від сервера LoRaWAN мережі з найменшими затримками. Пристрої класу С мають всі можливості пристроїв класу А і В.

Вузли можуть проводити обмін як з одним, так і з декількома шлюзами. Узли можуть працювати в двох режимах: точка-точка (від англ. P2P - point to point), коли обмін відбувається між кінцевим пристроєм і шлюзом (також цілком реалізуємий обмін тільки між двома вузлами без використання концентраторів і навіть сервера) і в гібридному режимі, коли один з вузлів підключений, з одного боку, по радіоканалу до інших вузлів, а з іншого боку, має дротове підключення до мережі по TCP/IP і виступає в ролі шлюзу. Такий одноканальний міні-шлюз може обслуговувати від одного до декількох десятків кінцевих пристроїв, які будуть конкурувати між собою за вільні тайм слоти міні-шлюзу для прийому і передачі даних.

Шлюзи (Gateway) LoRa призначені для використання в радіальних зіркоподібних мережевих архітектурах великого радіусу дії в системі LoRaWAN. Шлюзи можуть являти собою багатоканальні трансивери, які здатні виконувати демодуляцію відразу декількох каналів одночасно. Шлюзи служать в якості інтерфейсу у вигляді прозорого моста для передачі повідомлень між кінцевими вузлами і центральним сервером.

Зв'язок між шлюзами і центральним сервером LoRaWAN мережі оператора (транспортна мережа backhaul) здійснюється за допомогою традиційних технологій (Ethernet, GSM) по протоколу TCP/IP.

Якщо шлюзи підключаються до мережевого сервера через стандартні IP-з'єднання, то кінцеві вузли використовують бездротове підключення до одного або кількох шлюзів. Всі кінцеві вузли, як правило, є дуплексними, але вони також підтримують і функціонування в режимі, що забезпечує можливість здійснення групового оновлення програмного забезпечення через стільникову мережу або передачу інших масових повідомлень, що дозволяє скоротити час на їх передачу. Шлюзи можуть встановлюватися як всередині приміщень, так і на вишках або будівлях.

Вузли LoRaWAN мережі можуть бути в зоні покриття як одного шлюзу так і декількох. Шлюзом в мережах з високою щільністю кінцевих вузлів

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 101

виступають спеціальні багатоканальні концентратори, які мають можливість приймати дані від декількох вузлів одночасно. Саме ця можливість шлюзу безпосередньо впливає на максимальну щільність пристроїв на ділянці місцевості, яка обслуговується одним шлюзом (концентратором).

Концентратори на базі Semtech SX1301 мають можливість обслуговувати до 5 тисяч абонентських пристроїв на один квадратний кілометр. Ємність мережі залежить від того числа пакетів, які можуть бути отримані в даний момент часу. Один шлюз на SX1301 з 8 каналами, використовуючи протокол LoRaWAN, здатний отримати близько 1,5 млн. пакетів в день. Так що, якщо вузол відправляє один пакет на годину, то один шлюз на SX1301 може з успіхом обслуговувати до 62500 таких кінцевих пристроїв.

Якщо ємності сегмента мережі недостатньо, то LoRaWAN мережа масштабується: більш висока щільність вузлів досягається шляхом установки додаткових шлюзів. При появі нового шлюзу, центральний сервер мережі перерозподіляє навантаження, відправляючи кінцевим вузлам "новий графік" включення режиму передачі.

Проблему можливих колізій при одночасній передачі даних декількома точками вирішує *центральний сервер мережі* (Network Server), який адресно відправляє вузлам мережі керуючі команди через шлюзи, виділяючи тайм-слоти для передачі і прийому індивідуально для кожного кінцевого пристрою. Адресація відбувається по 32-бітному адресу, унікальному для кожного вузла.

Щоб продовжити термін служби батареї (акумулятора) в кінцевому вузлі і оптимізувати загальну пропускну здатність мережі, мережевий сервер LoRaWAN управляє швидкістю передачі даних і потужністю радіочастотного виходу кожного кінцевого пристрою окремо на підставі відстані від шлюзу. Управління здійснюється за допомогою алгоритму адаптивної швидкості передачі даних ADR (від англ. Adaptive Data Rate). ADR представляє собою метод, при якому фактична швидкість передачі даних регулюється таким чином, щоб забезпечити надійну доставку пакетів і забезпечити оптимальну продуктивність мережі. Так, наприклад, вузли ближчі до шлюзу використовуватимуть більш високу швидкість передачі даних (більш короткий час активної передачі по радіоканалу) і меншу вихідну потужність. А найвіддаленіші вузли будуть використовувати низьку швидкість передачі даних і високу вихідну потужність передавача.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 102

Кожен LoRaWAN пакет даних, що відправляються кінцевим вузлом, має в своєму складі унікальний ідентифікатор AppEUI, що належить додаткам на сервері сервіс-провайдера, для якого він призначений. Цей ідентифікатор використовується центральним сервером LoRaWAN мережі для подальшої маршрутизації пакета і його обробки на сервері додатків (App Server) сервіс-провайдера. На практиці, як правило, послуги сервіс-провайдера надає виробник кінцевих пристроїв, який підтримує сервіс для обробки даних.

Швидкість передачі даних залежить від параметрів трансивера, що використовується. Наприклад, для SX1276 (137 MHz to 1020 MHz Low Power Long Range Transceiver), максимальна швидкість передачі даних складає 37,5кбіт/с при використанні циклічного кодування (CR=4/5) з фактором розширення спектру SF=7 і ширині спектру радіосигналу BW=500 кГц. При зменшенні ширини спектру радіосигналу у два рази та при значенні фактору розширення спектру SF=7, швидкість передачі даних для цього трансиверу буде складати 11 кбіт/с, що цілком достатньо для розв'язуваних даною технологією завдань.

LoRaWAN мережах забезпечується повна конфіденційність даних при проходженні всіх задіяних в ланцюжку пристроїв від відправника до одержувача. Вміст пакета даних доступний тільки відправнику (кінцевому вузлу) і одержувачу, для якого воно призначене, тобто додатку сервіс-провайдера. Сервер мережі поводить аутентифікацію і перевіряє цілісність кожного пакету, але оперує даними в зашифрованому вигляді і не має доступу до інформації від підключених до вузла сенсорів. Для захисту від несанкціонованого доступу і спотворення або перехоплення даних, переданих кінцевими пристроями, стандартом передбачено обов'язкове шифрування даних алгоритмом AES-128.

7. Топологія хмарних обчислень в IoT

7.1. Модель хмарних сервісів

Інтернет речей радикальним чином збільшує обсяг даних, що збираються, що є наслідком величезної кількості джерел інформації (насамперед різні сенсори). Гігантські сенсорні мережі вже зараз виробляють величезні потоки даних, які треба вміти не тільки зберігати, а й обробляти, робити висновки, приймати рішення – і все це з урахуванням неточності як оригінальних даних,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арк. ___ / 103

так і процедур обробки. Якщо обробка даних переміщується близько до того місця, де генеруються дані, то такі обчислення отримали назву *граничні обчислення*. У разі IoT граничним пристроєм може бути сам датчик із невеликим мікроконтролером або вбудованою системою, здатною до WAN-зв'язку. Гранична обробка також зазвичай згадується в контексті «машина-машина», де існує щільна кореляція між краєм (клієнтом) та сервером, розташованим в іншому місці. Граничні обчислення дозволяють усунути проблеми із затримкою і непотрібним надмірним завантаженням каналу передачі даних.

Наприкінці 2000-х років для обробки великого обсягу даних сформувався підхід, який називається «великі дані» (англ. Big Data) – це серія інструментів та методів обробки структурованих та неструктурованих даних величезних обсягів та значного різноманіття для отримання необхідних результатів обробки. Основна відмінність великих даних від «звичайних» полягає в тому, що ці дані неможливо обробити традиційними системами управління базами даних (СУБД) через їх великий обсяг та різноманітний склад. Інша важлива їхня властивість – феноменальне прискорення накопичення даних та постійна зміна. Такі популярні завдання, як зведення даних, отриманих із різних джерел, вимагають спеціальних методів аналізу у разі неточних даних, особливо даних великих розмірів. У зв'язку з цим і був розроблений набір інструментів, що отримав назву «великі дані», що дозволяють працювати з даними незалежно від їхнього типу та обсягу. Інтернет речей породжує «великі дані», тому виникає закономірне питання: де їх зберігати та чим обробляти? Відповіддю на це питання є перспективна інфокомунікаційна технологія – хмарні обчислення (CC, Cloud Computing). Хмарні обчислення мають на увазі оренду послуг та ресурсів для зберігання та обробки даних у глобальній мережі замість власної інфраструктури. У систем CC повинні бути п'ять основних характеристик: самообслуговування на вимогу, широкосмуговий мережевий доступ, пул ресурсів, можливість швидкого переналаштування або розширення та обслуговування.

Без хмарних технологій ринок IoT-пристроїв не існував би. Хмара забезпечує можливість мати прості датчики, камери, перемикачі, маяки і виконавчі механізми, які розмовляють спільною мовою один з одним.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 104

Поняття «хмара» відноситься до інфраструктури обчислювальних служб, які зазвичай необхідні відповідно до запиту. Набір ресурсів (обчислень, мереж, сховищ і пов'язаних з ними програмних сервісів) може динамічно масштабуватися в бік збільшення або зменшення в залежності від середнього навантаження і якості обслуговування. Хмари, як правило, представляють собою великі центри обробки даних, які надають клієнтам послуги, орієнтовані на зовнішнього споживача, і модель оплати за використання. Ці центри створюють ілюзію єдиного хмарного ресурсу, в той час як насправді може бути використано багато географічно розподілених ресурсів. Це дає користувачеві відчуття незалежності від місця розташування. Ресурси є еластичними (що означає масштабуємість), а сервіси - це еквівалент плати за використання, незмінний дохід для провайдера. Сервіси, які працюють в хмарі, відрізняються від традиційного програмного забезпечення своєю конструкцією та реалізацією.

Існують чотири моделі розгортання хмарної інфраструктури, так званих «хмар» (рис.7.1):

1. Приватна хмара (англ. private cloud) – інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад, підрозділів однієї організації), можливо також клієнтами та підрядниками цієї організації. Приватна хмара може перебувати у власності, управлінні та експлуатації як самої організації, так і третьої сторони (або будь-якої їх комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника.



Рис. 7.1 - Моделі розгортання хмарної інфраструктури

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 105

2. Публічна хмара (англ. public cloud) - інфраструктура, призначена для вільного використання широкою публікою. Публічна хмара може бути у власності, управлінні та експлуатації комерційних, наукових та урядових організацій (або будь-якої їх комбінації). Публічна хмара фізично існує у юрисдикції власника – постачальника послуг.

3. Громадська хмара (англ. community cloud) – вид інфраструктури, призначений для використання конкретним співтовариством споживачів з організацій, що мають спільні завдання (наприклад, місії, GNU Radio, Arduino IDE). Громадська хмара може бути у кооперативній (спільній) власності, управлінні та експлуатації однієї або більше організацій співтовариства або третьої сторони (або будь-якої їх комбінації) і вона може фізично існувати як усередині, так і поза юрисдикцією власника.

4. Гібридна хмара (англ. hybrid cloud) – це комбінація з двох або більше різних хмарних інфраструктур (приватних, публічних або громадських), що залишаються унікальними об'єктами, але пов'язані між собою стандартизованими або приватними технологіями передачі даних та додатків.

Різні послуги хмарних обчислень, що, входять до архітектури IoT, можна віднести до таких основних класів (рис.7.2):

«мережа як послуга» (NaaS, Network as a Service) – орендовані хмарні організовані механізми для забезпечення оверлейних мереж і безпеки підприємств. Замість того, щоб створювати глобальну інфраструктуру і виділяти капітал для підтримки корпоративних комунікацій, при створенні віртуальної мережі може використовуватися хмарний підхід;

«інфраструктура як послуга» (IaaS, Infrastructure as a Service) – оренда потужності серверів та ємності систем зберігання центрів обробки даних (ЦОД). У цій моделі постачальник створює масштабовані апаратні служби в хмарі і надає модифікацію програмних фреймворків для створення клієнтських віртуальних машин. Це забезпечує максимальну гнучкість при розгортанні, але вимагає більших зусиль з боку клієнта;

«платформа як послуга» (PaaS, Platform as a Service) – оренда платформи розробки ПЗ колективними або індивідуальними розробниками. PaaS використовує базове устаткування і програмні засоби нижнього рівня, що надаються хмарию. В такому випадку кінцевий користувач просто використовує апаратне забезпечення ЦОД, операційну систему, проміжне ПО і

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 106

різні бази даних постачальника для розміщення свого приватного додатка або сервісів. Проміжне ПО може складатися з систем баз даних;

"програмне забезпечення, як послуга" (SaaS, Software as a Service) - оренда програмного забезпечення (ПЗ), яке запускається "з хмари". У провайдера зазвичай є пропонувані додатки або послуги, які пропонуються кінцевим користувачам. З точки зору користувача, віртуальний SaaS фактично працює на обладнанні користувача (мобільні пристрої, комп'ютери, тонкі клієнти). Під терміном «тонкий клієнт» мається на увазі ряд *пристроїв та програм*, які переносять усі або більшу частину завдань з обробки інформації на сервер і мають можливість роботи в *термінальному режимі*.

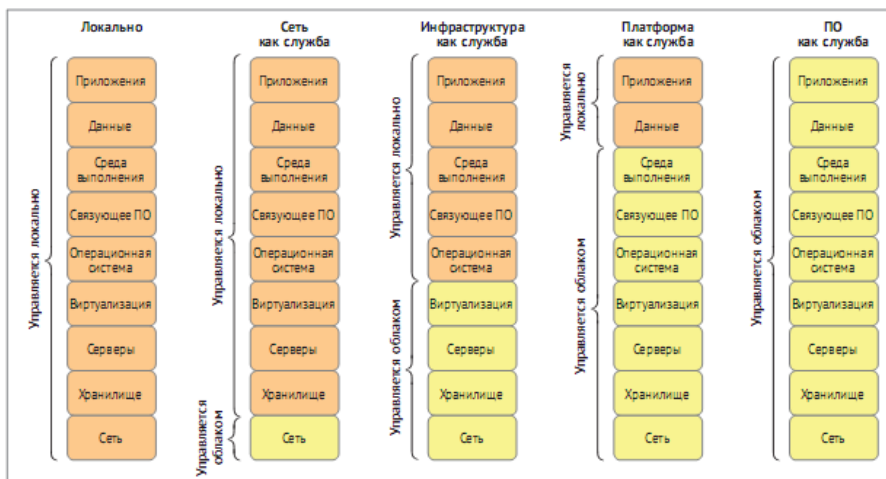


Рис. 7.2 - Моделі хмарної архітектури

Таким чином, для роботи тонкого клієнта потрібний термінальний сервер. Цим тонкий клієнт відрізняється від *товстого клієнта*, який, навпаки, обробляє інформацію незалежно від сервера, використовуючи останній переважно лише для зберігання даних. Прикладом тонкого клієнта може бути комп'ютер із браузером, який використовується для роботи з веб-програмами. Даним терміном може також називатися P2P-клієнт, який використовує як сервер інші вузли мережі. Тонкий клієнт в більшості випадків має мінімальну апаратну конфігурацію, замість жорсткого диска для завантаження локальної спеціалізованої ОС використовується DOM (DiskOnModule) - модуль з роз'ємом IDE, флеш-пам'яттю та мікросхемою, що реалізує логіку звичайного жорсткого

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 107

диска - в BIOS визначається як звичайний жорсткий диск розмір його зазвичай у 2-3 рази менше. У деяких конфігураціях системи тонкий клієнт завантажує операційну систему через мережу з сервера.

7.2. Модель туманних сервісів

Для роботи технологій Інтернету речей використовують і «туманні обчислення» (Fog Computing) — це різновид хмарних сервісів, розташованих не деє у недоступних висотах, а у навколишньому середовищі. Туманні обчислення доповнюють хмарні обчислення та забезпечують взаємодію «розумних речей» між собою та хмарними ЦОД у вигляді трирівневої ієрархічної структури (рис.7.3). Верхній рівень займають тисячі хмарних ЦОД, що надають ресурси, необхідні для виконання серйозних, наприклад, аналітичних програм IoT. Рівнем нижче розташовуються десятки тисяч розподілених керуючих ЦОД, у яких міститься «інтелект» Fog Computing, а в нижньому рівні перебувають мільйони обчислювальних пристроїв розумних речей. Туманні вузли є розширеннями хмари, тоді як граничні пристрої можуть використовувати або не використовувати хмару.

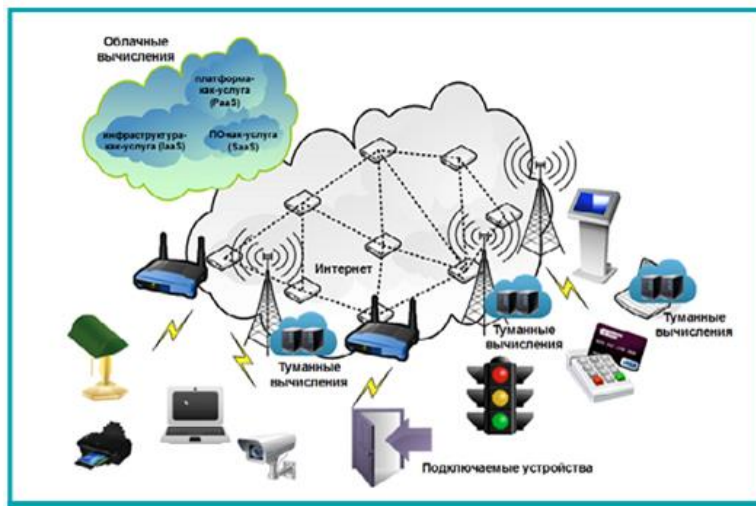


Рис. 7.3 - Місце хмарних обчислень в архітектурі IoT

Fog Computing можна визначити як максимально віртуалізовану платформу, що підтримує три основних типи сервісів, що утворюють міжмашинні комунікації M2M: обчислення, зберігання і мережу. Завдання Fog

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 108

Computing полягає у забезпеченні взаємодії мільярдів пристроїв між собою та з хмарними ЦОД.

Значні обчислювальні ресурси можуть бути розміщені на периферії мережі і при цьому робота в режимі реального часу передбачає низький рівень затримок при обміні даними.

Туманна мережа може бути простою, як граничний маршрутизатор з підтримкою туману, що з'єднує датчики з хмарним сервісом. Вона також може ускладнюватися в багаторівневу туманну ієрархію туману з різним ступенем здатності обробки в кожному шарі і ролями на кожному рівні, одночасно перерозподіляючи навантаження обробки.

Найпростішим рішенням для туману є блок обробки на краю (шлюз, тонкі клієнти, маршрутизатор), розташовані поруч з матрицею датчиків (рис. 7.4). На рис. 7.4 гранично-туманний пристрій управляє масивом датчиків і може взаємодіяти з іншим туманним вузлом на основі M2M. Тут туманний вузол може використовуватися в якості шлюзу для мережі або mesh-мережі WPAN і обмінюватися даними з іншим туманним вузлом - хостом (будь-який пристрій, що надає послуги формату «клієнт-сервер» в режимі сервера за будь-якими інтерфейсами та унікально визначений на цих інтерфейсах).

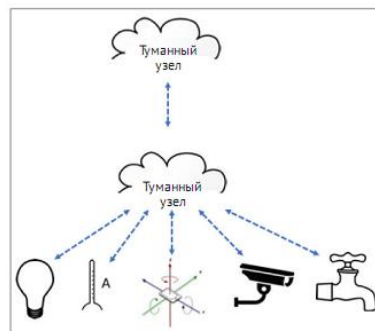


Рис. 7.4 - Проста туманна топологія

Наступна базова туманна топологія включає хмару як батька по туманній мережі (рис. 7.5). Тут туманний вузол встановлює відносини з постачальником хмари. Туманний вузол в цьому випадку буде збирати дані і виконувати обробку, необхідну для зв'язку з хмарою. Цю модель відокремлює від граничних обчислень те, що сервісні і програмні рівні туманного вузла поділяють відносини з хмарним фреймворком (від framework - каркас,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 109

структура) - *програмна платформа*, що визначає структуру програмної системи; *програмне забезпечення*, що полегшує розробку та об'єднання різних компонентів великого програмного проекту.

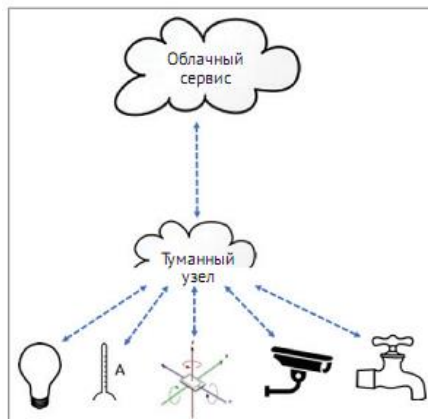


Рис. 7.5 - Туман до хмарної топології

Наступна модель використовує кілька туманних вузлів, відповідальних за послуги і обробку на краю, і кожен з них підключається до набору датчиків (рис. 7.6). Батьківська хмара забезпечує кожен туманний вузол, так як якщо б він був єдиним вузлом. Кожен вузол має унікальний ідентифікатор,

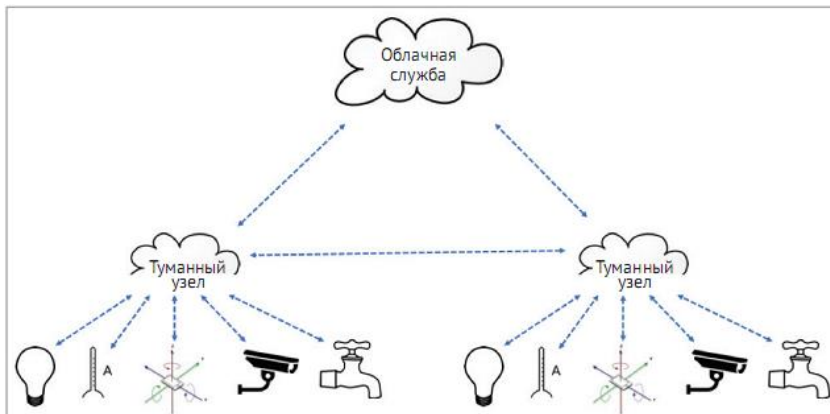


Рис. 7.6 - Кілька туманних вузлів з однією основною хмариною щоб забезпечити унікальний набір сервісів на основі розташування. Наприклад, кожен туманний вузол може перебувати в іншому місці для роздрібної мережі.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 110

Туманні вузли також можуть пов'язувати і передавати дані між граничними вузлами. Прикладом можуть служити умови холодного зберігання, коли необхідно підтримувати і управляти вентиляторами і морозильниками, щоб запобігти псуванню продуктів харчування. У роздрібного продавця може бути кілька вентиляторів в різних місцях, все управляється єдиною хмарною службою, але працюють з туманними вузлами на краю.

Наступна модель розширює попередню топологію, додаючи можливість надійно і конфіденційно спілкуватися декільком постачальникам хмар з декількома туманними вузлами (рис. 7.7). У цій моделі можуть бути розгорнуті кілька батьківських хмар. Туманні вузли також можуть при необхідності з'єднуватись між собою, що зв'язує датчики з хмарами «один до одного».

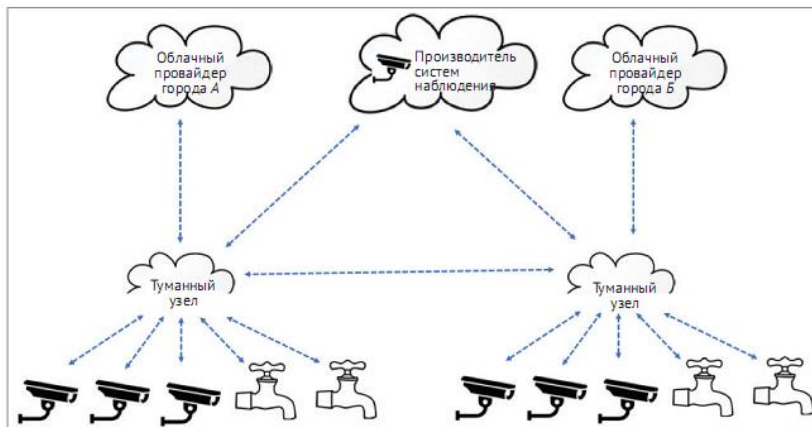


Рис. 7.7 - Кілька туманних вузлів з кількома хмарними провайдерами.

Наприклад, в розумних містах можуть існувати численні географічні райони, і вони можуть охоплюватися різними муніципалітетами. Кожен муніципалітет може вибрати одного хмарного провайдера, порівнявши його з іншими, але всі муніципалітети управляються з використанням одного затвердженого та бюджетного виробника камер і датчиків. У цьому випадку виробник камер і датчиків матиме один екземпляр хмари, що співіснує з декількома муніципалітетами. Туманні вузли повинні мати можливість доставляти дані декільком постачальникам хмарних обчислень.

Ієрархія рівнів туманних вузлів один над одним може здаватися суперечливою, якщо ми намагаємося зменшити затримки, але, як згадувалося

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 111

раніше, вузли можуть бути спеціалізованими. Наприклад, вузли, розташовані ближче до датчиків, можуть надавати послуги в режимі реального часу або мати обмеження за вартістю, що вимагає від них мінімального обсягу даних для зберігання і обчислення.

Рівні над ними можуть надавати обчислювальні ресурси, необхідні для агрегованого зберігання, машинного навчання або розпізнавання зображень з використанням додаткових пристроїв, що запам'ятовують. Наступний приклад ілюструє подібне використання на прикладі освітлення міста (рис. 7.8).

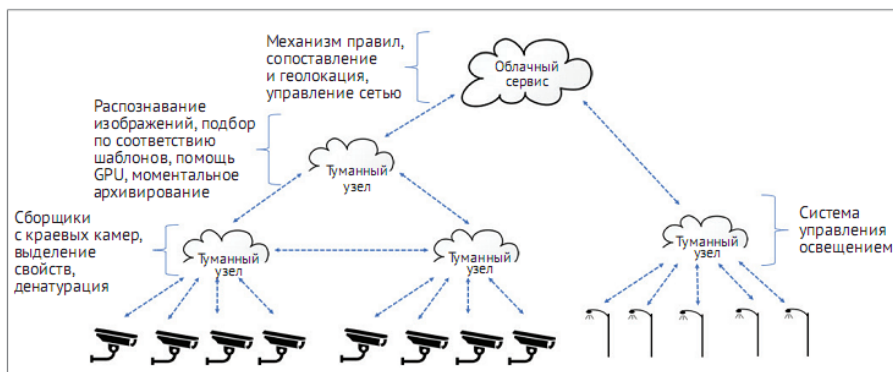


Рис. 7.8 - Багаторівнева туманна топологія. GPU-графічний процесор.

Тут кілька камер відчувують рух пішоходів, а туманні вузли, які мають найтісніший контакт з камерами, виконують агрегацію і витяг ознак і передають ці дані вгору до наступного рівня. Батьківський туманний вузол отримує дані і виконує необхідне розпізнавання зображень за допомогою алгоритму глибокого навчання. Якщо буде спостерігатися цікава подія (наприклад, пішохідна прогулянка вночі вздовж шляху), подію буде відправлено в хмару. Компонент хмари реєструє подію і сигналізує множині вуличних ліхтарів в околиці пішохода, щоб вони збільшили освітленість. Ця картина буде тривати до тих пір, поки туманні вузли бачать рух пішохода. Кінцевою метою є загальна економія енергії, щоб кожна вулична лампочка не працювала на повну інтенсивність весь час.

8. Принципи взаємодії інтернет речей із хмарними платформами

Основним аспектом Інтернету речей є M2M технологія (рис.8.1). Для зв'язку кінцевих пристроїв та шлюзів із хмарними платформами

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 112

використовуються певні протоколи взаємодії. Протоколи визначають модель обміну повідомленнями, щоб визначити, як вищевказані суб'єкти спілкуються між собою, роль кожної з цих складових та структуру обміну повідомленнями між ними.

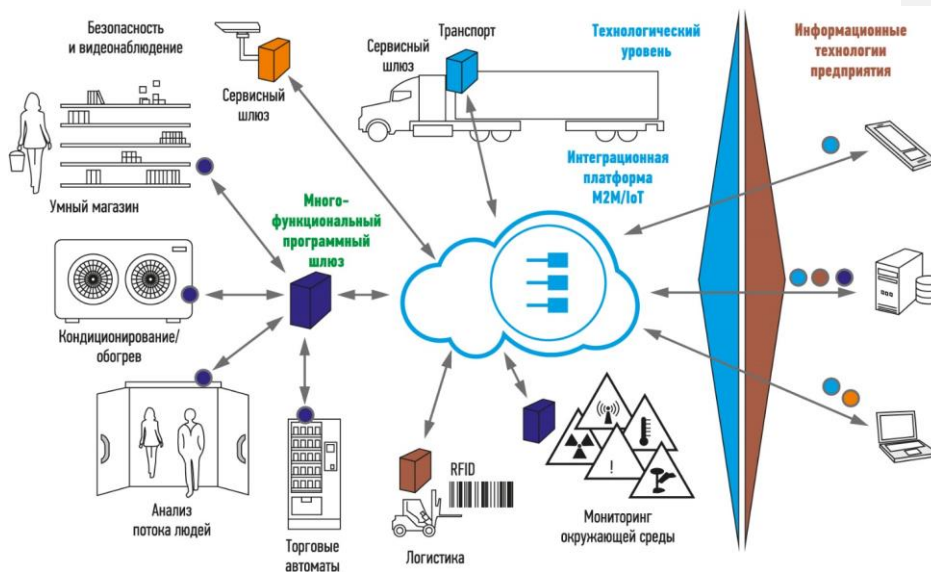


Рис. 8.1 - Интернет вещей та M2M технологія

На основі моделі обміну повідомленнями всі протоколи поділяють на два типи, а саме протоколи *відповіді на запит* та *протоколи передачі повідомлення*.

8.1. Протоколи відповіді на запит

У протоколах типу *відповідь на запит* учасники протоколів спілкуються один з одним за допомогою набору запитів та відповідей. Модель взаємодії для такого роду протоколів визначається на основі двох об'єктів, сервера та клієнта. Сервер - це елемент, що надає набір послуг або ресурсів, якими користується клієнт. Клієнт запитує сервер на певний ресурс, а сервер слухає вхідні запити, обробляє запит і відповідає клієнту.

Найбільш часто використовуються два протоколи, що засновані на моделі запит-відповідь - це протокол передачі гіпертекстів (HTTP) та протокол обмеженого застосування (CoAP).

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 113

Протокол передачі гіпертексту HTTP (Hyper Text Transfer Protocol) - протокол рівня додатків, заснований на моделі повідомлення-відповіді на запит. Основою HTTP є технологія «клієнт-сервер», яка передбачає існування наступних елементів:

клієнти — кінцеві споживачі послуг сервера, які ініціюють з'єднання та надсилають запит;

сервери як основні постачальники послуг, зберігання та *обробки запитів*, які чекають на з'єднання для отримання запиту, роблять необхідні дії і повертають назад повідомлення з результатом;

проксі-сервер, що отримує запити від клієнта і пересилає запит на сервер шляхом *переформатування запиту*.

У мережі Інтернет виклик віддаленої процедури може бути звичайним HTTP-запитом (зазвичай GET або POST, такий запит називають «REST-запит»), а необхідні дані передаються як параметри запиту. REST (від англ. Representational State Transfer - "передача репрезентативного стану" або "передача "самоописуваного" стану") - *архітектурний стиль* взаємодії компонентів розподіленого додатка в мережі. Іншими словами, REST — це набір правил написання (узгоджений набір обмежень) коду серверного додатку, щоб усі системи легко обмінювалися даними та додаток можна було масштабувати (нарошувати додаткові ресурси без структурних змін центрального вузла системи). Система називається такою, що *масштабується*, якщо вона здатна збільшувати продуктивність пропорційно додатковим ресурсам. Для веб-служб, побудованих з урахуванням REST, застосовують термін «RESTful».

Обмеження, що накладаються, визначають роботу сервера в тому, як він може обробляти і відповідати на запити клієнтів. Діючи в рамках цих обмежень, система набуває таких бажаних властивостей як продуктивність, масштабованість, простота, здатність до змін, надійність. Існує шість *обов'язкових обмежень* для побудови розподілених REST-додатків:

1. Приведення архітектури до моделі клієнт-сервер. Розмежування потреби інтерфейсу клієнта від потреб сервера, що зберігає дані, підвищує переносимість коду клієнтського інтерфейсу на інші платформи, а спрощення серверної частини поліпшує масштабованість.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 114

2. Протокол взаємодії між клієнтом та сервером вимагає дотримання наступної умови: у період між запитами клієнта жодна інформація про стан клієнта на сервері не зберігається («Stateless protocol» або «протокол без збереження стану»). Всі запити від клієнта повинні бути складені так, щоб сервер отримав усю необхідну інформацію для виконання запиту. Стан сесії при цьому зберігається на боці клієнта. Клієнт ініціює надсилання запитів, коли він готовий (виникає потреба) перейти в новий стан.

3. Клієнти, а також проміжні вузли можуть виконувати кешування відповідей сервера. Кешування (англ. cache - «ховати») – використання проміжного буферу зі швидким доступом до нього, що містить інформацію, яка може бути запитана з найбільшою ймовірністю. Доступ до даних у кеші здійснюється швидше, ніж вибірка вихідних даних з повільнішої пам'яті або віддаленого джерела, однак її обсяг істотно обмежений у порівнянні зі сховищем вихідних даних. Правильне використання кешування здатне частково або повністю усунути деякі клієнт-серверні взаємодії, ще більше підвищуючи продуктивність та масштабованість системи.

4. Усі ресурси ідентифікуються у запитах, наприклад, із використанням уніфікованого ідентифікатора ресурсів URI (Uniform Resource Identifier). Клієнт має достатню інформацію для модифікації чи видалення ресурсу. Кожне повідомлення містить достатньо інформації, щоб зрозуміти, як його обробляти.

5. Клієнти змінюють стан системи лише через події, які динамічно визначені в гіпермедіа на сервері (наприклад, гіперпосилання в гіпертексті).

6. Застосування проміжних серверів в ієрархічній багат шаровій структурі мереж здатне підвищити масштабованість за рахунок балансування навантаження та розподіленого кешування.

Сервер пропонує послуги у вигляді спільних ресурсів, наприклад, файлів, які однозначно ідентифіковані URI. Щоб скористатися послугами, пропонованими сервером, клієнт відправляє на сервер повідомлення із запитом, включаючи URI ресурсу, версію протоколу та метод запиту разом з іншими параметрами та тілом повідомлення.

Метод запиту GET використовується для зчитування ресурсу, метод запиту PUT використовується для створення ресурсу, метод запиту POST використовується для оновлення ресурсу, а метод видалення запиту - DELETE.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06-05.01/172.00.1/Б/ОК25-2022
	Екземпляр № 1	Арк. ___ / 115

Сервер відповідає на запит рядком стану та кодом вірності чи помилки. Наприклад, якщо клієнт надсилає GET-запит на читання ресурсу, сервер відповідає кодом 200 - «вірно» та запитуваним ресурсом в тілі або відповідає помилками різних типів, включаючи недоступність ресурсу чи сервера.

Основними реалізаціями клієнтів є браузери (агенти користувача). Для перегляду збереженого вмісту сайтів на комп'ютері без підключення до Інтернету були придумані офлайн-браузери. При нестабільному з'єднанні для завантаження великих файлів використовуються менеджери завантажень, які дозволяють у будь-який час докачати вказані файли після втрати з'єднання з веб-сервером. Деякі віртуальні атласи (такі як Google Earth та NASA World Wind) також використовують HTTP.

Проксі-сервери є найпопулярнішим способом виходу в Інтернет із локальних мереж підприємств та організацій. *Проксі-сервер* - проміжний сервер (комплекс програм) в комп'ютерних мережах, що виконує роль посередника між користувачем і цільовим сервером (при цьому про посередництво можуть як знати, так і не знати обидві сторони), що дозволяє клієнтам як виконувати непрямі запити (приймаючи та передаючи їх через проксі-сервер) до інших мережеслужб, так і отримувати відповіді (рис. 8.2.)

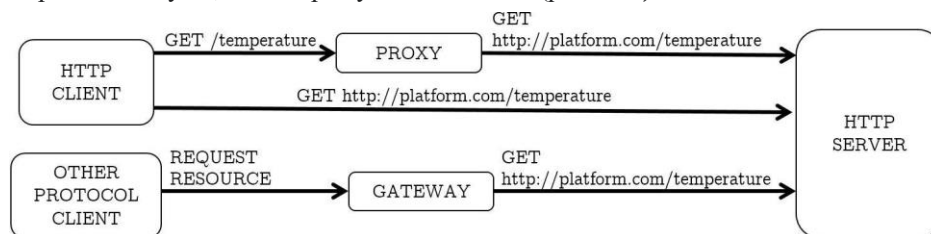


Рис. 8.2 - Архітектура повідомлень HTTP

Спочатку клієнт підключається до проксі-сервера і запитує будь-який ресурс (наприклад, e-mail), розташований на іншому сервері. Потім проксі-сервер або підключається до вказаного сервера та отримує ресурс у нього, або повертає ресурс із власного кешу.

Найчастіше проксі-сервери застосовуються для таких цілей:

забезпечення доступу комп'ютерів локальної мережі до Інтернету;
кешування даних;

стиснення даних: проксі-сервер завантажує інформацію з Інтернету та передає інформацію кінцевому користувачеві в стислому вигляді для економії

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 116

зовнішнього мережного трафіку клієнта або внутрішнього - організації, в якій встановлено проксі-сервер;

захист локальної мережі від зовнішнього доступу: наприклад, можна налаштувати проксі-сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі (вони бачать тільки проксі-сервер);

обмеження доступу з локальної мережі до зовнішньої: наприклад, можна забороняти доступ до певних веб-сайтів, обмежувати використання інтернету якимось локальним користувачам, встановлювати квоти на трафік, фільтрувати рекламу та віруси;

анонімність доступу до різних ресурсів: проксі-сервер може приховувати інформацію про джерело запиту або користувача. У такому разі цільовий сервер бачить лише інформацію про проксі-сервер, наприклад IP-адресу, але не має можливості визначити справжнє джерело запиту; існують також спотворюючі проксі-сервери, які передають цільовому серверу неправдиву інформацію про справжнього користувача;

обхід обмежень доступу: використовується, наприклад, користувачами країн, де доступ до деяких ресурсів обмежений законодавчо та фільтрується.

Клієнтський комп'ютер має налаштування (конкретної програми або операційної системи), відповідно до яких всі мережеві з'єднання за деяким протоколом здійснюються не на IP-адресу сервера (ресурсу), що виділяється з DNS-імені ресурсу або безпосередньо задану, а на IP-адресу (інший порт) проксі-сервера.

При необхідності звернення до будь-якого ресурсу за цим протоколом клієнтський комп'ютер відкриває мережне з'єднання з проксі-сервером і здійснює звичайний запит, якби він звертався безпосередньо до ресурсу.

Розпізнавши дані запиту, перевіривши його коректність та дозволи для клієнтського комп'ютера, проксі-сервер, не розриваючи з'єднання, сам відкриває нове мережне з'єднання безпосередньо з ресурсом і робить той самий запит. Отримавши дані (або повідомлення про помилку), проксі сервер передає їх клієнтському комп'ютеру.

Таким чином, проксі-сервер має повний контроль над усіма деталями реалізації мережевого протоколу, має можливість застосування заданих адміністратором політик доступу на кожному етапі роботи протоколу.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 117

Мережевий шлюз - це точка мережі, яка є виходом в іншу мережу. Мережевий шлюз (англ. Gateway) - апаратний маршрутизатор або програмне забезпечення для сполучення комп'ютерних мереж, що використовують різні протоколи. Маршрутизатор (роутер) є одним з прикладів апаратних мережевих шлюзів. Шлюз може бути спеціальним апаратним роутером або програмним забезпеченням, встановленим на звичайний сервер або персональний комп'ютер. Мережевий шлюз конвертує протоколи одного типу фізичного середовища на протоколи іншого фізичного середовища (мережі). Наприклад, при з'єднанні локального комп'ютера з Інтернетом зазвичай використовується мережевий шлюз. У великих мережах сервер, що працює як мережевий шлюз, зазвичай інтегрований з проксі-сервером та міжмережевим екраном.

Міжмережевий екран (Брандмауер, або Firewall - протипожежна стіна) — програмний або програмно-апаратний елемент комп'ютерної мережі, що здійснює контроль і фільтрацію мережного трафіку, що проходить через нього, відповідно до заданих правил. Міжмережеві екрани пропускають або забороняють трафік, порівнюючи його характеристики із заданими шаблонами. Найбільш поширене місце для встановлення міжмережевих екранів - межа периметра локальної мережі для захисту внутрішніх хостів від атак ззовні. *Хост* (від англ. host - "власник, що приймає гостей") - будь-який пристрій, що надає послуги формату "клієнт-сервер" в режимі сервера за якими-небудь інтерфейсами і унікально визначений на цих інтерфейсах. У більш широкому розумінні під хостом можуть розуміти будь-який комп'ютер, підключений до локальної чи глобальної мережі.

Модель зв'язку HTTP та відповідність її архітектурі RESTful дає можливість використовувати його як протокол зв'язку для розробки та розгортання систем IoT (рис.8.3).

Протокол CoAP (Constrained Application Protocol) призначений для взаємодії простих пристроїв, наприклад, датчиків малої потужності, вимикачів, клапанів, які керуються або контролюються віддалено через мережу Інтернет. Такі пристрої використовуються в області Інтернету речей, а інформаційний обмін, що породжується ними, називається, як відомо, міжмашинною взаємодією (M2M). Часто такі пристрої називають пристроями з обмеженими ресурсами. Вони зазвичай мають обмежений енергоресурс, невеликий обсяг пам'яті та невисоку потужність, тому в роботі з ними важливо забезпечувати

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 118

низькі енерговитрати, використовувати передачу малого обсягу повідомлень. Мережа, де працюють такі пристрої, називають мережею з обмеженими ресурсами.

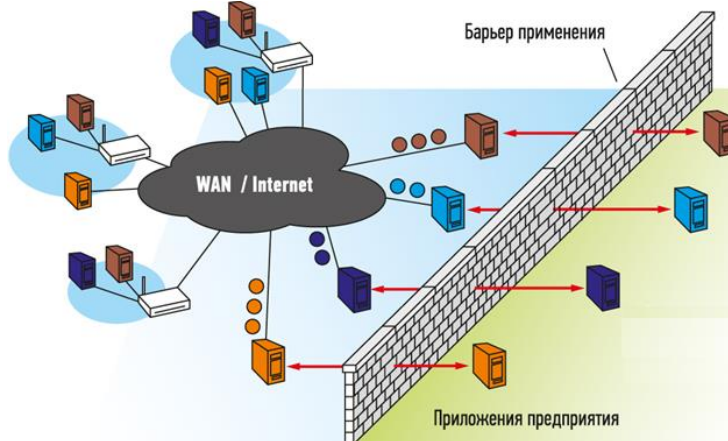


Рис. 8.3 - Міжмережевий екран в IoT

Протокол CoAP було розроблено саме для мережі з обмеженими ресурсами. Концепція CoAP орієнтована на взаємодію клієнт-сервер (рис. 8.4). Клієнт звертається до сервера і посилає йому прості команди типу PUT, POST, GET, DELETE, зміст яких зрозумілий з назви та аналогічний HTTP. З цієї точки зору можна сказати, що COAP - це спрощений HTTP, у якого мало ресурсів. Протокол CoAP відповідає вимогам RESTfull і легко і просто інтегрується с HTTP.

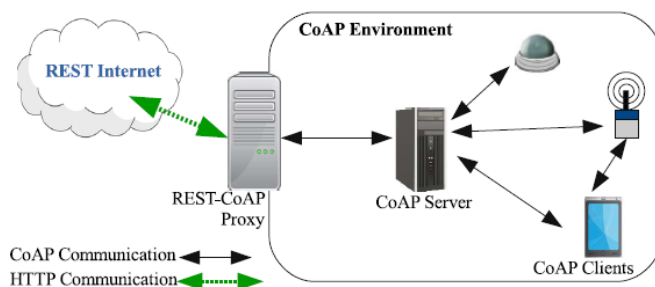


Рис. 8.4 – Взаємодія з використанням протоколу CoAP

Протокол CoAP використовує UDP (User Datagram Protocol) як транспортний протокол за умовчанням, що дозволяє зменшити розмір

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 119

службових даних і збільшити ефективність роботи. У протоколі CoAP визначено лише чотири види повідомлень: Confirmable, Non-confirmable, Acknowledgement, Reset.

Confirmable (CON) – повідомлення, що містить запит або відповідь, що вимагає підтвердження та вважається надійним. Кожне повідомлення Confirmable викликає одне відповідне повідомлення підтвердження або скидання;

Non-confirmable (NON) – повідомлення, що містить запит або відповідь, що не вимагає підтвердження та надійної передачі, оскільки передається регулярно (наприклад, показання від датчика);

Acknowledgement (ACK) – повідомлення, що підтверджує, що надійшло повідомлення Confirmable. При цьому саме повідомлення Acknowledgement не означає успіху чи невдачі будь-якого із запитів, що міститься в повідомленні Confirmable;

Reset (R) – повідомлення скидання, що вказує на те, що конкретне повідомлення (Confirmable або Non-confirmable) було отримано, але деяка частина тексту відсутня і неможливо правильно обробити його.

Усі повідомлення кодуються у бінарному вигляді. Формат повідомлення зображено на рис. 8.5.

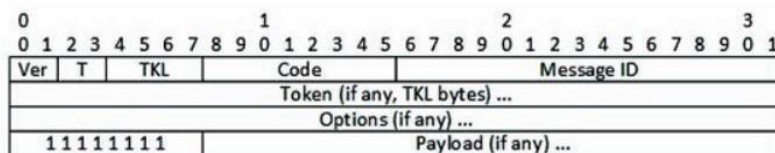


Рис. 8.5 – Формат повідомлення UDP

Повідомлення починається із заголовка, з фіксованим розміром в 4 байти, за ним слідує маркер, опції і корисне навантаження, яке займає всю частину дедтаграми, що залишилася.

Версія (Version) (Ver) – двобитне ціле число, що вказує на номер версії CoAP. На даний момент існує лише одна версія протоколу.

Довжина маркера (TKL - Token Length) - чотирибитне ціле число. Вказує довжину поля маркера (Token) змінної довжини (0-8 байт).

Код (Code) – восьмибітні цілі числа (фіксовані табличні величини), які вказують на метод запиту (наприклад, 0.01 – це запит GET, 0.02 – це запит

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 120

POST), або на код відповіді (наприклад, 2.05 – це відповідь, що містить запитану інформацію (Content), 4.04 – це помилка, коли запитуваний пристрій відсутній або тимчасово недоступний (Not Found)).

Ідентифікатор повідомлення (Message ID) – шістнадцятибітове ціле число, що є унікальним ідентифікатором повідомлення. Message ID ідентифікує повідомлення, щоб визначити, на який запит надійшла інформація або помилка. CoAP-пристрій, надсилаючи повідомлення Confirmable або Non-confirmable, випадково генерує значення ідентифікатора для цього повідомлення. У повідомленнях Acknowledgement або Reset ідентифікатори будуть ті ж, що і в повідомленні, на яке вони відповідають.

Значення маркера (Token) змінної довжини, що визначається полем TKL, випадково генерується пристроєм CoAP і використовується в межах однієї сесії для встановлення відповідності запиту з відповіддю (групування повідомлень по ланцюжку "запит-відповідь"). Пакети маркуються за допомогою 16-бітового ідентифікатора, щоб уникнути дублювання, тоді як маркер змінної довжини використовується для асоціації пакета з певним обміном «запит-відповідь».

Опції (Options), які описуються різні параметри повідомлень, наприклад, формат подання корисного навантаження (текст, або формат xml), максимальний час зберігання інформації у тимчасовій пам'яті, за замовчуванням, цей параметр дорівнює 60 сек. Для адресації URI в протоколі CoAP передбачені опції Uri-Host (визначає адресу інтернет-хосту запитуваного ресурсу), Uri-Port (визначає номер порту транспортного рівня запитуваного ресурсу), Uri-Path (визначає частину шляху до ресурсу) і Uri-Query (визначає параметр, який вимагає ресурс).

Таким чином, CoAP - це протокол обслуговування, який призначений для використання в інтернет-пристроях з обмеженими ресурсами, таких як вузли бездротової сенсорної мережі.

8.2. Протоколи передачі повідомлень

У протоколах передачі повідомлень клієнти, що стежать за протоколом, обмінюються повідомленнями один з одним через центральний брокер, який виступає арбітром для цих клієнтів. Клієнти протоколів передачі повідомлень є або виробники даних або споживачі даних або те і інше. Виробники даних надсилають свої повідомлення брокеру, позначеному символом ідентифікатора.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 121

Брокер розбирає повідомлення відповідно до набору правил, заснованих на ідентифікаторі для переадресації повідомлення відповідним споживачам повідомлень. Таким чином, модель взаємодії для подібного роду протоколів це коли споживач не запитує повідомлення, а повідомлення передається споживачеві від брокера. Два часто використовуваних протоколи передачі повідомлень, які використовуються для Internet of Things, це Message Queuing Telemetry Transport (MQTT) та вдосконалений протокол організації черги повідомлень (AMQP).

Протокол *AMQP* (Advanced Message Queuing Protocol), який іноді розглядають як протокол IoT, створений для того, щоб шляхом стандартизації повідомлень надати можливість широкому колу різних додатків і систем працювати разом незалежно від їх внутрішньої структури (рис. 8.6). Як випливає з назви, AMQP здатний обробляти тисячі організованих в чергу транзакцій між серверами.

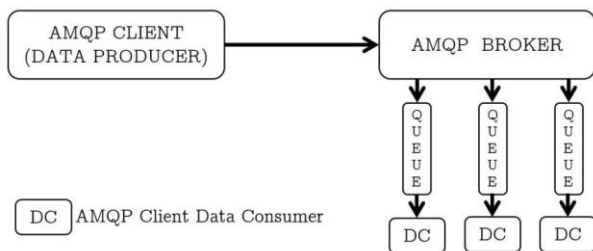


Рис. 8.6 - Архітектура протоколу AMQP

У протоколі AMQP велику увагу приділено боротьбі з втратою повідомлень. Різні комунікаційні лінії – від постачальників контенту до комутаторів каналів і від списків черговості до користувачів – використовують протокол TCP, який забезпечує високонадійне з'єднання «точка-точка». Крім того, кінцеві точки повинні підтверджувати прийняття кожного повідомлення. Протокол AMQP забезпечує асинхронну передачу даних на базі моделі видавець/передплатник. Залишаючись вірним своєму походженню з банківської галузі, протокол AMQP сфокусовано на основі спостереження за всіма повідомленнями і забезпеченні їх доставки за призначенням, незалежно від наявності збоїв і перезавантаження системи. У разі «Інтернету речей» AMQP найкращим чином підходить для реалізації функцій «підсистеми управління»

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 122

або аналітичних функцій на базі серверів. Головною перевагою цього протоколу є функція збереження та пересилання, яка забезпечує надійність, навіть після збою в мережі.

Протокол MQTT використовується протягом багатьох років, але зараз він особливо актуальний завдяки вибуховому зростанню IoT через впровадження розподілених мереж і граничних обчислень, а пристрої з постійною трансляцією даних стають частиною повсякденного життя. MQTT - це протокол обміну повідомленнями за шаблоном видавець-передплатник. У мережі на базі протоколу MQTT розрізняють 3 об'єкти (рис. 8.7): видавець (publisher) – MQTT клієнт, який при виникненні певних подій передає інформацію про нього до брокера; брокер (broker) - MQTT-сервер, який приймає інформацію від видавців і передає її відповідним передплатникам, в складних системах може виконувати також різні операції, пов'язані з аналізом і обробкою даних, що надійшли; передплатник (subscriber) - MQTT-клієнт, який після підписки у відповідного брокера більшу частину часу «слухає» його і постійно готовий до прийому і обробки вхідного повідомлення від брокера. Виходячи з парадигми видавець-передплатник, клієнти в основному є видавцями повідомлень або абонентам повідомлення або одночасно виконують обидві функції. Видавець і передплатник роз'єднані в просторі, отже, їм не потрібно однозначно пізнавати один одного та спілкуватися один з одним. Вони спілкуються один з одним опосередковано через брокера MQTT. Видавці повідомлень публікують повідомлення, адресовані брокеру MQTT. Повідомлення містять тему, що визначена видавцем повідомлення під час публікації. Передплатники повідомлень підписуються на набір тем для отримання повідомлень від брокера MQTT. Брокер MQTT отримує повідомлення від видавців та зберігає повідомлення протягом певного часу, а потім надсилає їх відповідним абонентам, коли вони підключаються до брокера.



Рис. 8.7 - Протокол MQTT

Протокол MQTT відхиляється від загальної конфігурації клієнт-сервер і для своєї роботи він не вимагає постійного з'єднання між клієнтом і сервером. MQTT також добре адаптований до роботи по каналах зв'язку з низькою

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 123

пропускнуою здатністю. Він також забезпечує перевагу перед протоколами клієнт-сервер з точки зору масштабованості, оскільки операції брокера можуть здійснюватися паралельно, оскільки клієнти роз'єднуються як у часі, так і в просторі. MQTT також не використовує черги для зберігання повідомлень, коли вони отримуються від видавця, тим самим обминаючи складність іменування та обробки черг однозначно. Ці переваги сприяли у зростанні MQTT як одного з найбільш широко використовуваних протоколів передачі повідомлень для Інтернету речей.

8.3. Хмарні додатки IoT

Архітектура додатків Інтернету речей, показана на рис.8.8. Кінцеві пристрої в вищенаведеній архітектурі представляють собою «речі», які складають Інтернет речей. Ці пристрої знаходяться на краю мережі і зазвичай оснащені обмеженими можливостями зберігання і обробки. Дані, генеровані кінцевими пристроями, можна збирати на шлюзі залежно від конкретного додатка, а потім відправляти в хмару. Шлюз пропонує такі послуги, як трансляція протоколу, локальне зберігання, перевірка і обробка даних, коли «речі» обмежені в ресурсах. Хмарні платформи пропонують безліч послуг для створення комплексних програм для Інтернету речей. По-перше, хмарні платформи пропонують послуги для збору даних від кінцевих пристроїв і шлюзів, які використовують різні базові протоколи. По-друге, хмарні платформи пропонують різні модулі обробки для обробки даних за допомогою простих модулів, що пропонують базову статистичну обробку як машинне навчання і розпізнавання образів. По-третє, хмарні платформи пропонують віддалений доступ до збережених даних на платформі через різні інтерфейси.

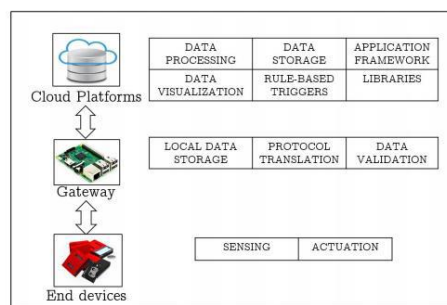


Рис. 8.8 - Архітектура додатків Інтернет речей

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 124

Крім того, деякі хмарні платформи пропонують каркаси додатків для створення додатків поверх платформи, використовуючи дані, що зберігаються на платформах. Крім того, хмарні платформи пропонують такі сервіси, як тригери на основі правил для виконання активацій на основі певних подій, отриманих з оброблюваних даних, візуалізації даних, що зберігаються на платформах, і бібліотек для доступу до послуг, що пропонуються платформою.

Cloud Mosquitto MQTT Broker - це брокер повідомлень для IoT. Керовані сервери Mosquitto у хмарі реалізують транспортний протокол MQTT, який надає спрощені методи обміну повідомленнями з використанням моделі організації черги повідомлень публікації/підписки (рис.8.9).

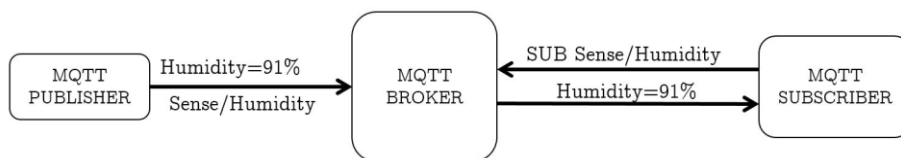


Рис.8.9 - Брокер повідомлень для IoT

MQTT - це міжмашинний протокол для підключених пристроїв IoT. Його мінімалістичний дизайн робить його ідеальним для вбудованих систем, мобільних телефонів та інших програм, з обмеженою пам'яттю та смугою пропускання. Черги повідомлень забезпечують асинхронний протокол зв'язку, відправнику та одержувачу повідомлення не потрібно одночасно взаємодіяти з чергою повідомлень. Повідомлення, розміщені в чергу, зберігаються доти, доки одержувач не отримає їх або поки очікування повідомлень не закінчиться.

Beebotte - це платформа, яка надає ключові будівельні блоки для підтримки IoT та програм, підключених у реальному часі. Підключення всього і вся в реальному часі за допомогою багатого API, що підтримує REST та MQTT, що робить платформу придатною для вбудованих пристроїв і датчиків (рис.8.10). Beebotte пропонує двонаправлену передачу даних між підключеними клієнтами чи пристроями. Комплексний механізм аутентифікації дозволяє контролювати доступ до ваших ресурсів.

ThingSpeak - це хмарна платформа IoT, яка дозволяє збирати, відображати та аналізувати потокові дані. Ви можете надсилати дані до ThingSpeak з різних пристроїв, налаштовувати їх відображення в реальному часі. Зберігання даних у хмарі забезпечує швидкий доступ до них.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 125

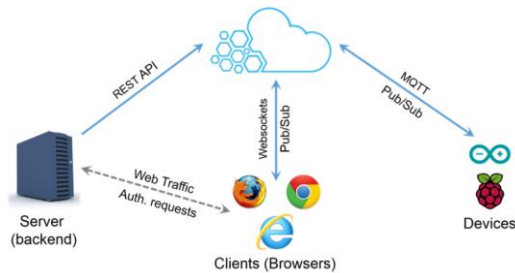


Рис.8.10 - Платформа Beebotte

Можливо налаштування пристроїв та надсилення даних у ThingSpeak через REST API або MQTT, відображення у реальному часі поточних і раніше отриманих даних (рис.8.11), а також попередня обробка та аналіз зібраних даних за допомогою вбудованих функцій MATLAB.

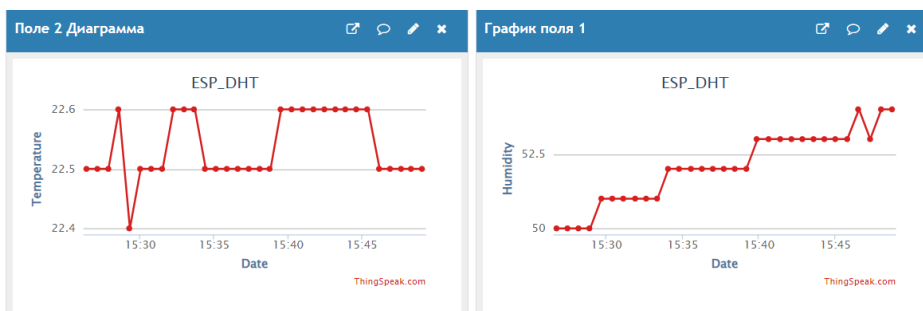


Рис.8.11 – Приклад графіків ThingSpeak

ThingSpeak дозволяє інженерам та вченим будувати IoT-системи без налаштування серверів та розробки веб-додатків. Ви можете будувати різноманітні графіки, створювати нові дані з наявних, а також контролювати віддалено пристрої, наприклад, електронні дверні замки, за допомогою вбудованої програми TalkBack.

Blynk є хмарним сервісом для створення графічних пультів управління і підходить для широкого спектру мікрокомп'ютерів і мікроконтролерів. Там, де раніше для збору інформації з датчиків потрібно було писати повноцінний інтерфейс введення-виводу або придбати додаткові модулі, тепер можна обійтися роботою з хмарним сервісом Blynk.

Для створення власного проекту з керуванням через Blynk потрібно зовсім небагато: встановити програму (доступні версії для iOS та Android) або

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 126

скористатися веб-формою. Тут знадобиться реєстрація одним кроком - введення e-mail і пароля. Реєстрація потрібна з огляду на те, що Blynk - хмарне рішення і без неї контроль над мікроконтролером може отримати будь-який користувач. Робота програми вимагатиме певних навичок. Спочатку необхідно зв'язати комп'ютер або смартфон із програмованою платою. Крім налаштування з'єднання, потрібно лише правильно з'єднати модулі майбутнього пристрою. Після цього в робочій формі додатка потрібно обрати доступні модулі (віджети), налаштувати необхідні адреси віртуальних виводів і вказати бажані параметри. Для керування доступна маса імітаторів керуючих пристроїв - перемикачі, слайдери, дисплеї, для яких можна писати свою логіку. Існують окремі форми для виведення та систематизації інформації з необхідних датчиків у вигляді графіків. На рис.8.12 наведений приклад використання хмарного сервісу Blynk для відображення на смартфоні вимірів рівня кисню в крові оксиметром, реалізованим на базі мікроконтролера ESP32.

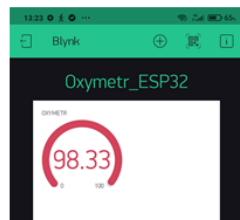


Рис.8.12 - Приклад віджету хмарного сервісу Blynk

Telegram — хмарний месенджер з функціями VoIP для смартфонів, планшетів та ПК, який дозволяє обмінюватися текстовими, голосовими та відео повідомленнями, наліпками та фотографіями, файлами багатьох форматів. Також має функції відео- і аудіо дзвінків, організації відеоконференцій у групах. Клієнтські програми Telegram доступні для Android, Windows, macOS і Linux. Обліковий запис користувача прив'язується до номера мобільного телефону: щоб авторизуватися, потрібно ввести код авторизації з СМС. Такі коди мають обмежені терміни придатності. Таким чином, користувач позбавляється необхідності запам'ятовувати чи зберігати десь свій пароль. У Telegram працює платформа чат-ботів. Чат-бот — це програма штучного інтелекту, яка імітує інтерактивну розмову людини з IoT речами за допомогою ключових, заздалегідь розрахованих текстових сигналів. У спілкуванні беруть участь користувач Telegram та програма мікроконтролера

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ____ / 127

датчика. На рис.8.13,а наведений результат роботи системи сигналізації з датчиком руху на мікроконтролера ESP32 з використанням чат-бота.

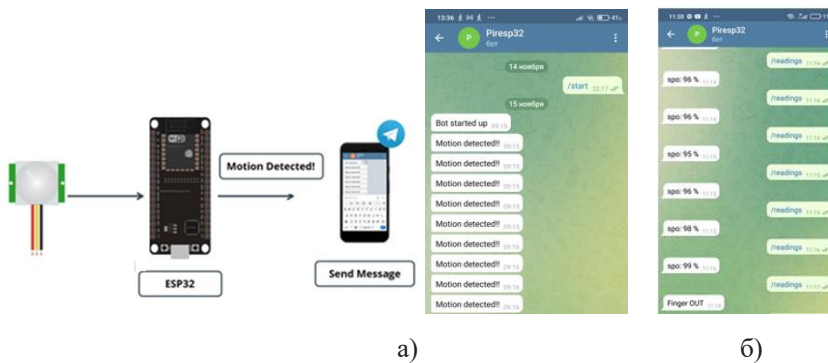


Рис.8.13 – Відображення у чат-боті Telegram

Користувач може взаємодіяти з ботом за допомогою елементів інтерфейсу месенджера: надсилання повідомлень, натискання на команди та кнопки, з використання онлайн-режиму. Наприклад, чат-бот, на запит «reading» (рис.12,б) звертається до датчика вимірів рівня кисню в крові, що реалізований на базі мікроконтролера ESP32, та виводить на екран результат поточного виміру.

Таким чином, розглянуті платформи підійдуть як новачкам, так і більш просунутим користувачам, які не хочуть витрачати час на написання програм для управління проектами: від зчитування даних з метеостанції та управління розумним будинком до управління роботами.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.06- 05.01/172.00.1/Б/ ОК25-2022
	Екземпляр № 1	Арк. ___ / 128

Перелік літератури

1. Ільченко М.Ю., Кравчук С.О. Сучасні телекомунікаційні системи. – К.: Наукова думка, 2008. – 328 с.
2. ITU-T Rec. Y.2060 (06/2012): Overview of the Internet of things [Ел. ресурс] / Режим доступу: [http:// T-REC-Y.2060-201206-I!!PDF-R.pdf](http://T-REC-Y.2060-201206-I!!PDF-R.pdf).
3. ETSI TS 102 690 «Machine-to-Machine communications (M2M); Functional architecture».– 2011. [Ел. ресурс].
4. ISO/IEC 18092:2004. Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol [Ел. ресурс].
5. RFID-метки. [Ел. ресурс] / Режим доступу: <http://rfid-m.ua>.
6. Top 12 most commonly used IoT protocols and standards. [Ел. ресурс] / Режим доступу: <https://www.techtarget.com/iotagenda/tip/Top-12-most-commonly-used-IoT-protocols-and-standards>
7. Wi-Fi Alliance. [Ел. ресурс] / Режим доступу: <http://www.wi-fi.org/>.
8. Ільченко М.Е., Кравчук С.А. Мікрохвильові технології у телекомунікаційних системах .-Київ:Техніка,2000 .-304 с.
9. Андреев О.В. Радіозв'язок: навч. посібн.[електронне видання] / О.В. Андреев, В.Г. Парфенюк, П.П. Топольницький. – Житомир : ЖДТУ, 2015. – 214 с.
10. Fielding R., Gettys J., Mogul J., Frystyk H., Masinter L., Leach P., Berners-Lee T. RFC 2616, Hypertext Transfer Protocol – HTTP/1.1. 1999. [Ел. ресурс].
11. LoRa and LoRaWAN: A Technical Overview, Semtech – 2020. [Ел. ресурс] / Режим доступу: https://lora-developers.semtech.com/uploads/documents/files/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf.
12. IoT Based Pulse Oximeter. G. Sidhartha, Dwarakanath. M. L., Vineeth. K. C., Sukruth R., 2021. - DOI:10.22214/ijraset.2021.37782