МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Б.Ю. Жураковський, І.О. Зенів

ТЕХНОЛОГІЇ ІНТЕРНТУ РЕЧЕЙ

НАВЧАЛЬНИЙ ПОСІБНИК

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського як навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Інформаційне забезпечення робототехнічних систем» за спеціальністю 126 «Інформаційні системи та технології»

Київ
КПІ ім. Ігоря Сікорського
2021

Рецензент: Манько О.О., д.т.н., професор, професор кафедри телекомунікацій Одеської академії зв'язку ім. О.С. Попова
Марков С.Ю., д.т.н., доцент, доцент кафедри телекомунікаційних систем та мереж Державного університету телекомунікацій

Відповідальний редактор: Ткач М.М. канд. техніч. наук, доцент

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 8 від 24.06.2021 р.) за поданням Вченої ради факультету (протокол №8 від 29.03.2021 р.)

Електронне мережне навчальне видання

Жураковський Богдан Юрійович, доктор техн. наук, професор
Зенів Ірина Онуфріївна, кандидат техн. наук, доцент

ТЕХНОЛОГІЇ ІНТЕРНТУ РЕЧЕЙ

НАВЧАЛЬНИЙ ПОСІБНИК

Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

Посібник розроблений на підставі робочої програми кредитного модуля бакалавра з дисципліни “Технології інтернету речей”, для опанування теоретичних та практичних навичок, які необхідні майбутнім фахівцям для вивчення дисципліни «Технології інтернету речей». Для кожної теми наведено перелік питань для самоконтролю, задачі для роботи в аудиторії різного рівня складності та вказано питання, що будуть включені в модульну контрольну роботу.

Призначений для студентів, які навчаються за освітньою програмою «Інформаційне забезпечення робототехнічних систем» підготовки бакалаврів за спеціальністю 126 – «Інформаційні системи та технології» денної та заочної форм навчання.

Спрямований на формування у студентів умінь та набуття практичних навичок, пов’язаних з технологіями інтернету речей, а також аналізом та обробленням “великих” даних.

Забезпечує студентів необхідними теоретичними знаннями для опанування відповідної теми комп’ютерного практикуму та виконання завдань, запланованих впродовж семестру. Містить короткий теоретичний опис, методичні поради виконання комп’ютерних практикумів, а також додаткові самостійні завдання, контрольні питання.

ЗМІСТ

ВСТУП

Глобалізація інформатизації суспільства і активний процес науково-технічного розвитку в області інформаційних систем сприяють формуванню єдиного світового інформаційного простору. Однією з основних тенденцій розвитку сучасних інформаційних систем та технологій стає розширення доступності інформаційно-обчислювальних ресурсів мереж для окремих абонентів, в тому числі і речей.

Сьогодні пристрої Інтернету речей не лише масово використовуються у щоденному вжитку, але й у сучасному бізнес-середовищі. Зокрема Інтернет речей (*Internet-of-Things* або IoT) активно впроваджується в різних галузях — від промислової сфери до сільського господарства, рітейлу та будівництва. Поступово пристрої IoT стають невід'ємною частиною багатьох галузей, і зростання їх кількості спричиняє виникнення нових проблем проектування, застосування, експлуатації та безпеки.

Бурхливий розвиток технічних засобів і підвищення активності доступу до інформаційно-обчислювальних ресурсів підвищили інтерес до проблеми ефективного використання мережевих ресурсів інтернету речей і забезпечення оперативного доступу до них.

У даному читачеві навчальному посібнику розглядаються архітектура інтернету речей, різновиди датчиків, що використовуються, моделі та платформи інтернету речей, технології інтернету речей, мережі та протоколи інтернету речей, методи обробки даних, загрози і безпека в інтернеті речей, принципи побудови і технології сенсорних мереж, робота з великими даними, хмарними та туманними обчисленнями, управління маршрутизацією, потоками даних і обчислювальними ресурсами з метою підвищення оперативності обміну інформацією в інтернеті речей.

Автори виражають глибоку подяку рецензентам, які, ознайомившись з начальним варіантом рукопису, висловили ряд корисних зауважень і рекомендацій, що дозволили поліпшити виклад матеріалу посібника.

Метою навчального посібника є формування системи знань в області Інтернет речей та цифрових технологій, та більш широкої категорії, яка називається цифровим перетворенням на базі яких дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких системи на виробництві та в науковій сфері. В посібнику основний акцент робиться на розумінні фундаментальних концепцій і механізмів які лежать в основі функціонування інтернет-речей.

Даний навчальний посібник призначений для викладачів, інженерно-технічних працівників, що займаються розробкою технічних засобів і проектуванням в області інтернету речей та інформаційних систем та технологій, а також для аспірантів і студентів, які цікавляться даними питаннями.

Сподіваємося, що дана книга знайде зацікавлених читачів, яких ми заздалегідь дякуємо за всі побажання і зауваження щодо змісту навчального посібника.

РОЗДІЛ 1. СКЛАДОВІ МАЙБУТНЬОГО ІНТЕРНЕТУ

1.1. Основні поняття Інтернету речей

Інтернет речей — одна з найпопулярніших наукових ідей сучасної інформатики, яка зараз активно втілюється в життя. Він здатний серйозно вплинути на розвиток сучасного суспільства, оскільки дасть змогу багатьом процесам відбуватися без участі людини.

Інтернет речей (Internet of Things, скорочено IoT) — це глобальна мережа підключених до Інтернету речей — пристроїв, оснащених сенсорами, датчиками, засобами передавання сигналів. Ці цифрові пристрої можуть сприймати датчиками різноманітні сигнали з навколишнього світу, вступати у взаємодію з іншими пристроями, обмінюватися даними з метою віддаленого моніторингу за станом об'єктів, аналізу зібраних даних і прийняття на їх основі рішень. Прикладом можуть бути гаражні двері, кавоварки, телевізори, мобільні телефони, відеокамери, датчики світла та температури тощо.

Термін «*Інтернет речей*» запропонував у 1999 році засновник дослідницького центру *AutoID Center* в Массачусетському технологічному інституті *Кевін Ештон*. Він висловив припущення, що згодом у кожної з речей реального фізичного світу в IoT буде цифровий двійник, її віртуальне представлення.

Напрямок IoT став активно розвиватися, коли на початку 2000-х років кількість пристроїв, підключених до мережі Інтернет, перевищила кількість користувачів Інтернету. Тобто Інтернет речей перевищив Інтернет людей.

Рис. 1.1. Робот-гуманоїд

За даними компанії Ericsson (Швеція), сьогодні у світі налічується понад 16 млрд підключених до Інтернету пристроїв. Уже в 2018 році їх кількість перевищила кількість мобільних телефонів у світі. До 2022 року це число досягне 29 млрд, 18 млрд з яких будуть пристроями світу IoT.

1.2. Використання Інтернету речей

Інтернет речей об'єднує реальні речі в віртуальні системи, здатні вирішувати абсолютно різні завдання. Ключова ідея — з'єднати між собою всі об'єкти, які можна з'єднати, підключити їх до мережі для збирання даних і прийняття рішень на їх основі. Наприклад, відкрити гаражні двері, включити кавоварку або кондиціонер, виключити світло тощо.

У такому середовищі створюються якісно інші, ніж сьогодні, умови для бізнесу, для охорони здоров'я, для забезпечення екологічної безпеки, трансформуються особисті та соціальні аспекти життя.

В Австралії вже зараз за допомогою переносних датчиків лікарі можуть віддалено відслідковувати стан здоров'я пацієнтів і реагувати на його зміни в режимі реального часу. А телефонна компанія AT&T в США розробила систему, покликану вирішити одну з найнебезпечніших проблем для літніх людей — несподівані падіння. Невеликий пристрій автоматично визначає різку зміну положення тіла власника і зв'язується з call-центром для надання негайної допомоги.

У житті людей стане менше побутових проблем, а значить — більше часу можна буде приділяти сім'ї, творчості, хобі. Підключення пристроїв до Інтернету також дадуть людям більше можливостей для раціонального управління ресурсами: витрачання газу, води, світла, видобуток газу, ядерної енергії тощо

Рис. 1.2. Використання Інтернету речей

Smart технологія

Smart технологія — це процес взаємодії об'єктів з оточуючим середовищем, що наділяє цю систему здатністю адаптації до нових умов, саморозвитку та самонавчання, ефективного досягнення цілей.

Smart речі

Популярними сьогодні стають так звані «розумні речі», або Smart речі (Smart — розумний, енергійний, кмітливий). Наприклад, гаджети, які зручно носити з собою, мають невеликі розміри і незначну масу — «розумний» годинник, фітнес-трекери, смарт-окуляри, гнучкі екрани .

Уже сьогодні «розумні будинки» дають змогу ефективно керувати всіма системами функціонування будівлі за допомогою дистанційних пультів і мобільних телефонів, оптимально витрачати тепло, воду, світло й економити на оплаті комунальних послуг тощо. Усе це створює у світі умови для нового явища — Інтернету майбутнього, що включає в себе, крім *нинішнього Інтернету людей (Internet of People, IoP),* ще й *Інтернет речей (Internet of Things, IoT), Інтернет медіаконтенту (Internet of Media, IoM), Інтернет сервісів (Internet of Services, IoS)*

1.3. Складові майбутнього Інтернету

Безперечно, для активного використання цих ідей суспільству потрібний дуже швидкісний Інтернет, який може забезпечити впровадження мереж п'ятого покоління 5G. Це сприятиме зменшенню затримки під час передавання даних з датчиків, одночасній підтримці дуже великої кількості підключень, подовженню терміну придатності «розумних» пристроїв до 10 років, а також дасть підґрунтя для неймовірних швидкостей мобільної передачі даних.

У той самий час украй важливим у світі «розумних» пристроїв стає питання безпеки. Експерти запевняють, що до 80 % пристроїв будуть уразливі ззовні. Для пристроїв буде потрібна абсолютна надійність мережі, адже найменший збій може призвести до травм або загибелі людей.

На основі розвитку Smart-технологій останнім часом стали виникати нові поняття: Smart-міста, Smart-країни, Smart-освіта, Smart-економіка, і це найближчим часом призведе до створення Smart-суспільства. В основі цього «розумного суспільства» лежить розвиток «суспільства знань», цифрових технологій, усього того, що приведе до цифрової ери розвитку нашої цивілізації.

Діяльність людини в такому суспільстві стає більш направленою на використання знань та інновацій. Найефективнішою стає колективна робота, співпраця з іншими, використання так званого колективного інтелекту. Психологи вже давно помітили, що здатність групи знаходити рішення краща, ніж здатність кожного члена поодинці. У групі досвід її членів, їх рівень розуміння проблеми можуть бути досить різним, і це дасть змогу розглянути проблему з різних точок зору та прийняти найоптимальніше рішення.

Рис. 1.4. Складові майбутнього Інтернету

Уже сьогодні технології колективного інтелекту використовуються в корпоративному управлінні, у бізнес-плануванні, у сфері фінансів, політиці, соціології для генерації ідей, для прогнозування розвитку, визначення стратегій дій тощо. Результатом діяльності колективного інтелекту, наприклад, є вікіпедія, статті для якої можуть підготувати будь-які користувачі. Широке розповсюдження сьогодні мають і віртуальні професійні спільноти, форуми тощо.

Прикладом колективного інтелекту є також поведінка мурашника, рою бджіл. Наприклад, компанія *Estimize* для прогнозування прибутковості організацій збирає та обробляє думки 20 000 різнорідних професійних аналітиків зі всього світу. Зрозуміло, що для автоматичної обробки такого великого обсягу даних використовують цифрові технології, мережеві сервіси Інтернету Веб 2.0, відповідні математичні методи обробки, інтелектуальні комп'ютерні системи (штучний інтелект).

IoT з технологічної точки зору – це, по суті, мережа мереж, що складаються з унікально ідентифікованих об’єктів (по факту «речей»), які можуть взаємодіяти між собою через IP-підключення без втручання людини.

Слід зазначити, що, вживаючи термін «IoT», ми говоримо про куди більш складне явище, ніж просто набір давачів. Практика збору і аналізу даних про об’єкт – чи то механізм, будівля або людина, – за допомогою давачів існує давно. Промисловий інтернет радикально відрізняється тим, що давачі об’єднуються в єдину мережу з аналітичними і/або керуючими системами. Таким чином, у об’єкта формується самостійна мережа. Усередині мережі йде обмін даними, на основі яких автоматично приймаються рішення і здійснюються дії з управління об’єктом. Так з’являються елементи штучного інтелекту і принципи саморегулювання.

Нині IoT відноситься до мільярдів фізичних пристроїв по всьому світу, які тепер підключені до Інтернету, аналізують і оброблюють величезну кількість даних. Передбачається, що в майбутньому інтернет-речі стануть активними учасниками бізнесу, інформаційних і соціальних процесів, де зможуть взаємодіяти між собою, обмінюючись інформацією про навколишнє середовище, не потребуючи при цьому втручання людини. Завдяки процесорам і бездротовим мережам в частину IoT можна перетворити все що завгодно – від пігулки до літака. Це додає рівень цифрового інтелекту пристроям, які в іншому випадку були б неактивними, дозволяючи їм спілкуватися без участі людини і поєднання цифрових і фізичних світів.

Ключові поняття IoT

«Інтернет речей»: представляє мережу зв’язаних через інтернет об’єктів, здатних збирати дані і обмінюватися даними, які надходять із вбудованих сервісів.

«Пристрої IoT»: входять до системи інтернету речей і представляють будь-які автономні пристрої, підключені до інтернету, якими можна керувати дистанційно.

«Екосистема IoT»: включає всі компоненти, які дозволяють бізнесу, урядам і користувачам приєднувати свої пристрої IoT, включаючи пульти управління, панелі інструментів, мережі, шлюзи, аналітику, зберігання даних і безпеку.

«Фізичний рівень»: представляє апаратне забезпечення, яке використовується в IoT-пристроях, включаючи сенсори та мережеве обладнання. Відповідає за передачу даних, зібраних у фізичному шарі, до різних пристроїв.

«Рівень додатки»: включає протоколи та інтерфейси, які використовують пристрої для ідентифікації та зв’язку між собою.

«Пульти управління»: дозволяють людям використовувати IoT-пристрої, з’єднуючись з ними і контролюючи їх за допомогою панелі інструментів – наприклад, за допомогою мобільних додатків. До пультів управління відносяться смартфони, планшети, ПК, розумні годинники, телевізори і нетрадиційні пульти.

«Панелі інструментів»: забезпечують відображення інформації про екосистему IoT для користувачів, дозволяючи нею керувати (як правило, дистанційно).

«Аналітичний фактор»: представляє програмні системи, які аналізують дані, отримані від IoT-пристроїв. Аналітика використовується у великій кількості сценаріїв – наприклад, для прогнозування технічного обслуговування.

Деякі історичні факти, що сформували сучасне поняття IoT

- Ще у 1926 *Нікола Тесла* в інтерв'ю журналу «*Collier's*» заявив, що одного разу в майбутньому радіо буде перетворено у певний «великий мозок», і, в результаті, всі речі стануть частиною єдиного цілого, а інструменти, завдяки яким це стане можливим, будуть легко поміщатися у кишені.
- У 1990 році один із творців протоколу TCP/IP *Джон Ромки* підключив до мережі свій тостер, що, на думку багатьох експертів, ознаменувало початок епохи Інтернет-речей.
- Сам термін IoT був вперше запропонований і озвучений у 1999 році співзасновником дослідного центру Auto-ID в Масачусетському технологічному інституті *Кевіном Ештоном.* В цьому ж році був створений сам дослідний центр, який займався радіочастотною ідентифікацією (RFID) і сенсорними технологіями. Саме завдяки цим напрямкам концепція і отримала широке поширення.
- У 2008-2009 роках кількість підключених до мережі предметів перевищило кількість підключених до мережі людей.
- Багато експертів відзначили справжній початок ери технології IoT у 2013 році, хоча її поява не викликала у громадськості особливого інтересу. Втім, це було пов'язано з тим, що спочатку IoT стартувала як технологія міжмашинної взаємодії без людської участі (machine-to-machine, M2M) для безпроводових систем моніторингу. І лише дещо згодом до неї почали підключати все, що так чи інакше пов'язане із вбудованими обчислювальними системами (наприклад, високопродуктивні мережі – *high-end networking*, обладнання для цифрових вивісок, робототехніку, дрони, автомобільні комп'ютери і переносні пристрої).

Глобальність IoT і прогноз у цифрах

- Згідно з даними світового аналітичного агентства *Gartner*, у 2017 році було використано пристроїв IoT на суму близько 8,4 млрд.дол., що на 31% більше у порівнянні з 2016-м, а вже до 2020 року ця цифра, ймовірно, зросте до 20,4 млрд.дол.
- Загальні витрати на кінцеві точки і послуги IoT у 2017 році досягли майже 2 трлн.дол., причому дві третини із цих пристроїв – у Китаї, Північній Америці та Західній Європі. Більше 8 млрд. з усіх пристроїв – такі споживчі товари, як смарт-телевізори і смарт-динаміки.
- Згідно зі статистичними даними, серед найбільш популярних пристроїв IoT, які використовують підприємства, – інтелектуальні електричні лічильники і комерційні камери відеоспостереження.
- За даними аналітичної компанії IDC, у 2018 році світові витрати на IoT складуть 772,5 млрд.дол. При цьому, в IDC прогнозують, що загальні витрати на IoT складуть 1 трлн.дол. у 2020 році і 1.1 трлн.дол. у 2021 році.
- За підрахунками консалтингової агенції *McKinsey*, до 2025 року обсяг IoT-ринку складе 6,2 трлн.дол., притому більшість експертів сходяться на тому, що в кінцевому підсумку IoT повністю трансформує існуючий IT-ландшафт.
- Консультанти *IDC* припускають, що апаратне забезпечення стане найбільшою технологічною категорією, стартуючи з 2018 року: основні витрати підуть на модулі і давачі – більше 200 млрд.дол., з яких частина буде спрямована на інфраструктуру і безпеку. Послуги стануть другою за величиною технологічною категорією, за якою крокують програмне забезпечення та можливості підключення.

Сфери застосування IoT і його переваги для бізнесу

Застосування технологій IoT успішно проявили себе у наступних напрямках:

- Виробництво;
- Інфраструктура;

- Логістика;
- Транспорт;
- Військово-оборонний комплекс;
- Агро-сектор;
- Торгівля, включаючи роздрібні продажі;
- Банківська і страхова системи;
- Нафто-газова промисловість і видобуток корисних копалин;
- Напрямки Smart home і Smart city;
- Виробництво і реалізація продуктів харчування;
- Сфера обслуговування;
- Медицина;
- IT-індустрія.

Переваги IoT для бізнесу залежать від конкретної реалізації та напрямків діяльності, але суть полягає в тому, що підприємства можуть отримувати доступ до більшої кількості даних про свої продукти, власні внутрішні системи і статус їхньої роботи. Конкретніше про переваги:

Своєчасне отримання вичерпної інформації і можливість прогнозування подій.

- Формування комплексного бачення виробничих циклів і можливість керувати ними на всіх рівнях і етапах.
- Ефективність і точність структурування наявних даних.
- Підвищення індексу конкурентної переваги на ринку за рахунок зниження витрат шляхом їх оптимізації.
- Можливість віддаленого моніторингу географічно далеко розташованих об'єктів, що виключає масштабні збої і критичні поломки на виробництвах.
- Веб-розвідка та аналіз даних про клієнтів. Численні приклади бізнесу показують, що цільова аудиторія продукту, що аналізується продавцями, часом не збігається з його реальним призначенням. Набагато більшої ефективності в цьому напрямку можна досягти, корегуючи особливості продукту, що випускається у напрямку реальної групи потенційних споживачів або клієнтів.
- Власна безпека компанії, яка забезпечується за допомогою віддаленого відеоспостереження за процесами, що відбуваються в офісах.
- Автоматизація певних етапів замовлення послуги або продукту – знижує число операцій введення даних вручну (ПІБ, платіжні реквізити клієнтів тощо) і допомагає забезпечувати завчасне планування і резервування товару на складі.

Консалтингова компанія IDC виділяє три основні галузі, де очікуються найбільші фінансові вливання у технології IoT у 2018 році: виробничий комплекс (189 млрд.дол.), транспортний сектор (85 млрд.дол.) і сфера комунальних послуг (73 млрд. дол.):

- Передбачається, що виробники будуть в основному зосереджені на підвищенні ефективності своїх процесів і відстеженні активів.
- Дві третини витрат на IoT у транспортному секторі будуть спрямовані на моніторинг вантажоперевезень.
- Витрати IoT у галузі комунальних послуг будуть переважати в інтелектуальних мережах для планомірного і оптимального використання електрики, газу та води.

Деякі приклади переваг IoT для споживачів і вплив Інтернету речей на загальне сприйняття звичних процесів

- IoT обіцяє зробити наше навколишнє середовище – будинки, офіси і транспортні засоби – більш розумними і більш прогнозованими.

- Смарт-динаміки, такі як, наприклад, *Echo Amazon* і *Google Home*, полегшують відтворення музики, установку таймерів або отримання необхідної інформації.
- Системи домашньої безпеки спрощують контроль за тим, що відбувається всередині будинку і на прилеглій до нього території, дають можливість бачити відвідувачів і спілкуватися з ними.
- Розумні термостати можуть допомогти нагріти будинок, перш ніж ми повернемося додому, а, наприклад, розумні ліхтарі можуть освітлювати простір у нашу відсутність, імітуючи перебування людей у будинку.
- Давачі спостереження за будинком можуть допомогти зрозуміти, наскільки гучно або брудно навколо.
- Автономні автомобілі і розумні міста можуть змінити принцип управління нашим особистим чи громадським простором.

По мірі того, як кількість підключених пристроїв продовжує зростати, наше середовище для життя і роботи стане наповнюватися розумними продуктами – за умови, що ми готові прийняти компроміси щодо безпеки та конфіденційності. Адже ризики існують завжди і всюди. Наявність величезної мережі, яка контролює весь навколишній світ, глобальна відкритість даних та інші особливості можуть носити не лише позитивний, а й негативний характер. Однак, технології продовжать активно розвиватися, поглинаючи всі сумніви щодо доцільності та безпеки їх застосування в цілому.

Контрольні питання до розділу

1. Дайте визначення поняттю *Інтернету речей***.**
2. Хто і коли запропонував термін «*Інтернет речей*»?
3. Скільки сьогодні у світі налічується пристроїв, підключених до Інтернету?
4. Назвіть сфери використання Інтернету речей.
5. Наведіть складові майбутнього Інтернету.
6. Дайте визначння поняттю «Пристрої IoT».
7. Дайте визначння поняттю «Екосистема IoT».
8. Дайте визначння поняттю IoT «Фізичний рівень».
9. Дайте визначння поняттю IoT «Рівень додатки»
10. Дайте визначння поняттю IoT «Пульти управління».
11. Дайте визначння поняттю IoT «Панелі інструментів».
12. Дайте визначння поняттю IoT «Аналітичний фактор».
13. Дайте визначння поняттю IoT
14. В яких напрямках застосування технологій IoT успішно проявили себе.
15. У чому полягають переваги IoT для бізнесу?

Список рекомендованої літератури

1. Tripathy B. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. – Florida: CRC Press, 2017. – 334 c.
2. The 2nd Annual Internet of Things 2010 (англ.) [ЕлектроЕлектронний ресурс]. - Режим доступу: https://eu-ems.Com/summary.asp?event_id=55&page_id=342
3. Интернет вещей в научных исследованиях // електрон. текст. Дані URL: https://cyberleninka.ru/article/v/internet-veschey-v-nauchnyh-issledovaniyah (дата звернення: 01.06.2019)
4. АНАЛИЗ ТРАФИКА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ // електрон. текст. дані URL: https://cyberleninka.ru/article/v/analiz-trafika-ustroystv-interneta-veschey (дата звернення: 01.06.2019)
5. История появления технологии LoRa // електрон. текст. дані URL: *https://nekta.tech/technology/*

РОЗДІЛ 2. ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ

2.1. Історія Інтернету Речей

Термін «інтернет речей», зобов'язаний своєю появою *Кевіну Ештону*, який в 1997 р, працюючи на компанію Proctor and Gamble, застосував технологію ***радіочастотної ідентифікації (RFID)*** для керування системою поставок. Завдяки цій роботі в 1999 році його запросили в Масачусетський технологічний інститут, де він з групою однодумців організував дослідний консорціум Auto-ID Center (більш детальну інформацію можна знайти на сайті www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749).

З тих пір Інтернет речей звершив перехід від простих радіочастотних міток до екосистеми і індустрії. Аж до 2012 р ідея підключення речей до Інтернету переважно відносилася до смартфонів, планшетів, ПК і ноутбуків.

По суті, до тих пристроїв, які в усіх відношеннях виступають в якості комп'ютера. До цього, з моменту появи перших боязких зачатків Інтернету (таких як створена в 1969 р мережу ARPANET), більшості технологій, на яких будується Інтернет речей, просто не існувало. До 2000 року більшість пристроїв, які можна було підключити до Інтернету, представляло собою комп'ютери різних розмірів. Нижче показаний поступове підключення речей до Інтернету.

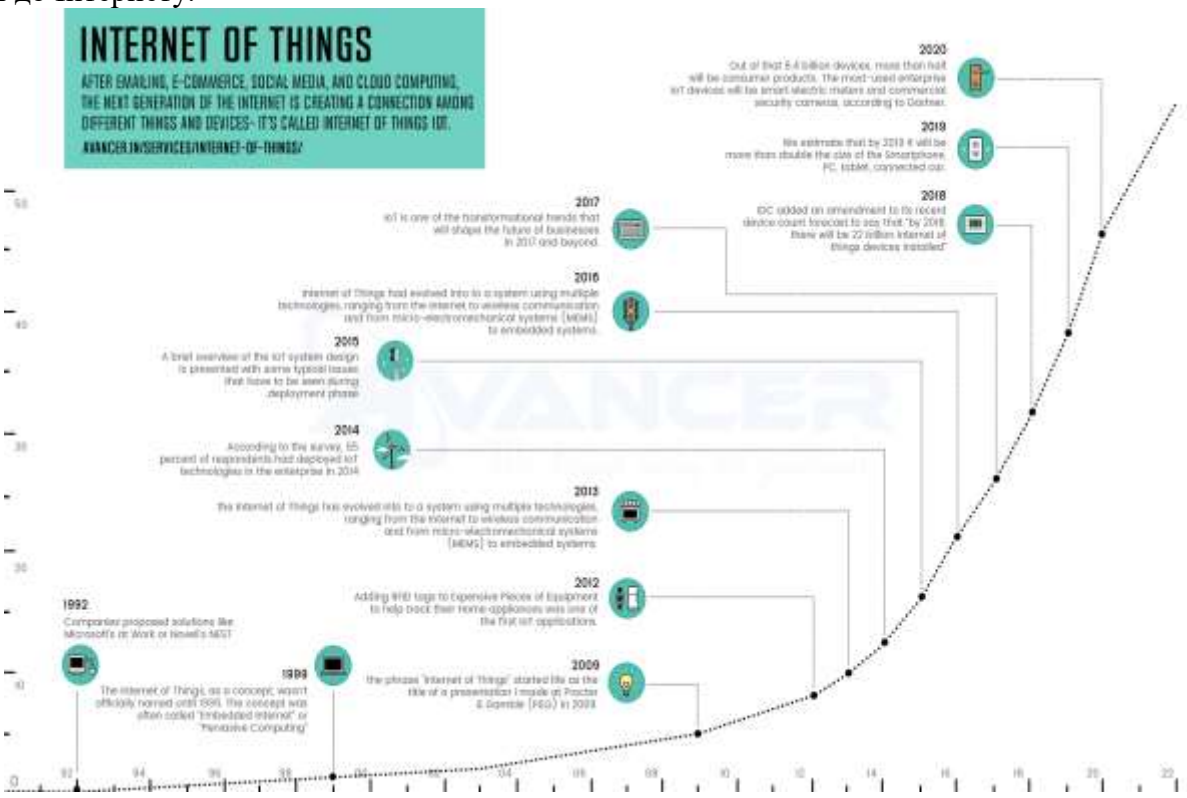


Рис. 2.1. Історія Інтернету речей

- 1973 - Маріо У. Кардулло отримує патент на першу радіо-частотну мітку
- 1982 - Підключений до Інтернету автомат з газованою водою в університеті Карнегі-Меллон
- 1989 - Підключений до Інтернету тостер на конференції Interop '89
- 1991 - Компанія HP представила HP LaserJet IIISi: перший підключений до мережі Ethernet мережевий принтер
- 1993 - Підключена до Інтернету кавоварка в Кембриджському університеті (перша підключена до Інтернету камера)
- 1996 - Підрозділ General Motors OnStar (дистанційна діагностика 2001)

- 1998 - Поява організації Bluetooth SIG
- 1999 - Холодильник LG Internet Digital DIOS
- 2000 - Перші прояви розробленої компанією HP концепції всепроникної комп'ютеризації (Cooltown): HP Labs, система обчислювальних і комунікаційних технологій, які в поєднанні один з одним створюють підключення до Інтернету для людей, місць і об'єктів
- 2001 - Випуск першого пристрою, що використовує технологію Bluetooth: мобільний телефон KDDI з підтримкою Bluetooth
- 2005 - Міжнародний союз електрозв'язку, спеціалізована установа ООН, випустив звіт, в якому вперше були сформульовані прогнози розвитку Інтернету речей
- 2008 - Поява першого IoT-спільноти IPSO Alliance, метою якого було сприяння підключенню речей до Інтернету
- 2010 - Успішна розробка напівпровідникових світлодіодних ламп привела до розвитку концепції розумного освітлення
- 2014 - Компанія Apple створила протокол iBeacon для маячків

Інтернет речей захопив практично кожен сегмент в сфері промисловості, бізнесу, охорони здоров'я і споживчих товарів.

2.2. Інтернет речей в промисловості

Промисловий Інтернет речей (**Industrial IoT**, **IIoT**) - це один з найбільш великих сегментів Інтернету речей з точки зору кількості підключених пристроїв і ступеня корисності цих сервісів для виробництва і автоматизації підприємств. Цей сегмент традиційно служить операційно-технологічною базою. Сюди входять апаратні і програмні засоби моніторингу фізичних пристроїв. Традиційні завдання інформаційних технологій вирішуються інакше, ніж операційно-технологічні завдання. **Операційні технології** (**OT**) зосереджені на оцінці продуктивності, часу безвідмовної роботи, зборі даних і відповідної реакції в режимі реального часу, а також безпеки систем. Інформаційні технології спрямовані на безпеку, групування, сервіси та надання даних. Оскільки Інтернет речей починає займати важливе місце в сфері виробництва і промисловості, світи IT і OT об'єднаються, особливо в області діагностичного обслуговування тисяч виробничих машин і верстатів, і зможуть забезпечувати безпрецедентним обсягом даних приватні та публічні хмарні інфраструктури. До характеристик цього сегмента відноситься необхідність надавати операційно-технологічної системи готові рішення в режимі реального часу або майже в режимі реального часу. Це означає, що у всьому, що стосується виробничого цеху, головним параметром для Інтернету речей буде час відгуку. Крім того, важливу роль будуть грати тривалість простою і безпеку. Це має на увазі потребу в запасі потужності і, ймовірно, в наявності приватних хмарних мереж і сховищ даних. Промисловий Інтернет речей - це один з сегментів на цьому ринку що найбільш швидко розвивається. Важливою особливістю цього напрямку є те, що він спирається на старі технології, тобто на апаратні і програмні засоби, які не можна назвати актуальними. Часто 30-річні виробничі станки працюють на послідовних інтерфейсах RS485, а не на сучасній бездротовій комірчастій архітектурі.

Приклади застосування Промислового Інтернету Речей:

- профілактичне обслуговування промислового обладнання;
- зростання продуктивності завдяки попиту в реальному часі;
- енергозбереження;
- системи безпеки, такі як вимірювання температури, вимірювання тиску і контроль над витоком газу;
- експертна система для виробничого цеху.

2.3. Екосистема Інтернету речей

До екосистеми Інтернету речей відносяться усі засоби, сервіси і технології, які використовуються в Інтернеті речей.

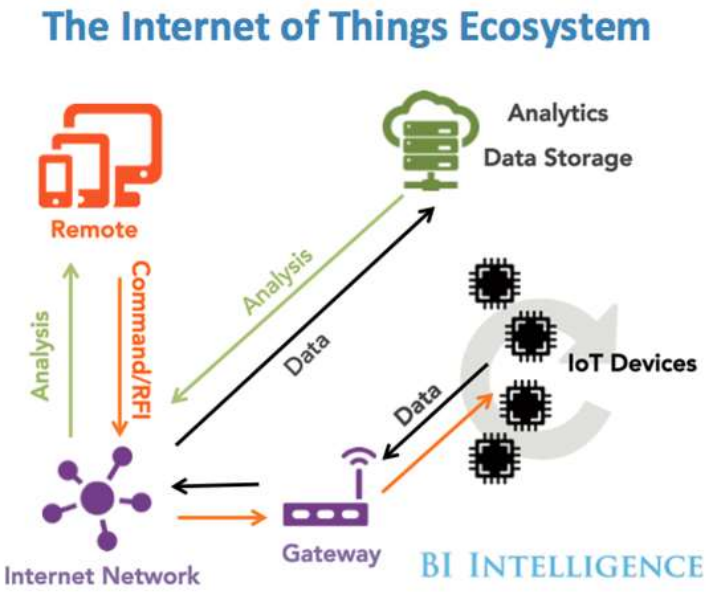


Рис. 2.2. Екосистема Інтернету речей

До них можна віднести:

- **sensors (розумні датчики/виконавчі механізми)**: вбудовані системи, операційні системи реального часу, джерела безперебійного живлення, мікро-електромеханічні системи (МЕМС);
- **системи зв'язку з датчиками**: зона охоплення бездротових персональних мереж становить від 0 см до 100 м. Для обміну даними між датчиками застосовуються низькошвидкісні малопотужні інформаційні канали, які часто побудовані не на протоколі IP;
- **локальні обчислювальні мережі (LAN)**: зазвичай це системи обміну даними на основі протоколу IP, наприклад, 802.11 Wi-Fi-мережу для швидкої радіозв'язку, часто це пірингові або зіркоподібні мережі;
- **агрегатори, маршрутизатори (routers), шлюзи (gateways), пограничні пристрої (Edge Device)** : постачальники вбудованих систем, самі бюджетні складові (процесори, динамічна оперативна пам'ять і система зберігання даних), виробники модулів, виробники пасивних компонентів, виробники тонких клієнтів, виробники стільникових і бездротових радіосистем, постачальники міжплатформового програмного забезпечення, розробники інфраструктури туманних обчислень, інструментарій для граничної аналітики, безпеку граничних пристроїв, системи управління сертифікатами;
- **глобальна обчислювальна мережа**: оператори стільникового зв'язку, оператори супутникового зв'язку, оператори малопотужних глобальних мереж (Low- Power Wide-Area Network, LPWAN). Зазвичай застосовуються транспортні протоколи Інтернету для IoT і мережевих пристроїв (MQTT, CoAP і навіть HTTP);
- **хмара**: інфраструктура в якості постачальника послуг, платформа в якості постачальника послуг, розробники баз даних, постачальники послуг потокової і пакетної обробки даних, інструменти для аналізу даних, програмне забезпечення в якості постачальника послуг, постачальники озер даних, оператори програмно-визначених мереж / програмно-визначених периметрів, сервіси машинного навчання;
- **сервіси аналізу даних**: величезні масиви інформації передаються в хмару. Робота з великими обсягами даних і отримання з них користі - це завдання, що вимагає комплексної обробки подій, аналітики і прийомів машинного навчання;

• **безпека (security)**: при зведенні всіх елементів архітектури воєдино постають питання кібербезпеки. Безпека стосується кожного компонента: від датчиків фізичних величин до ЦПУ і цифрового апаратного забезпечення, систем радіозв'язку і самих протоколів передачі даних. На кожному рівні необхідно забезпечити безпеку, достовірність і цілісність. У цьому ланцюзі не повинно бути слабких ланок, оскільки Інтернет речей стане головною мішенню для атак хакерів в світі.

2.4. Архітектура Інтернету Речей

Архітектура Інтернету речей відрізняється в залежності від реалізації. Тим не менше вона дещо схожа на архітектуру класичних систем АСУТП. Один із прикладів архітектури показаний на рис. 2.3.

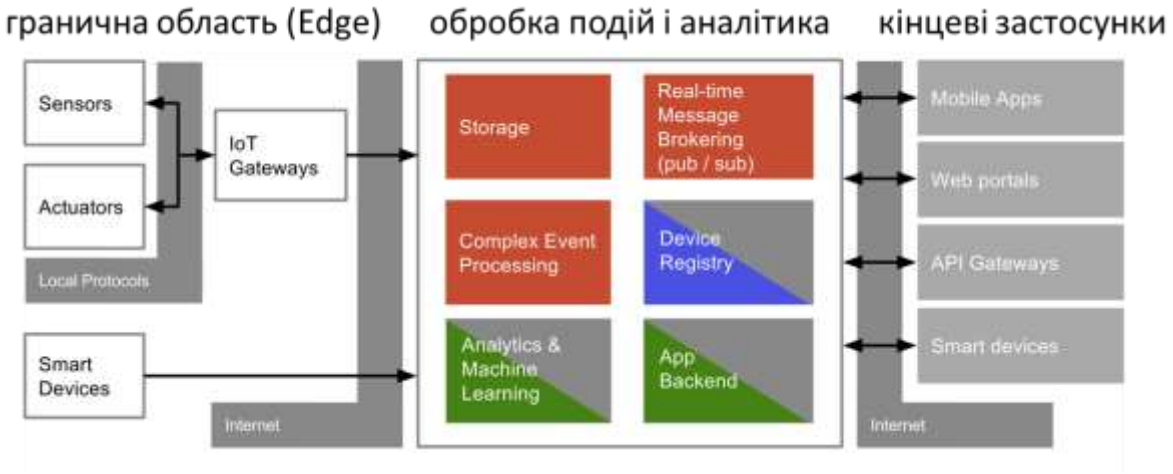


Рис. 2.3. Архітектура Інтернету Речей

Взаємодія з «речами» відбувається через датчики (sensors) та виконавчі механізми (Actuators), аналогічно як це робиться в АСУТП для будь якого об’єкту керування. Ці датчики разом з усією інфраструктурою для інтеграції з рівнем обробки подій через мережу Internet формують так звану граничну область (**Edge**).

Події (дані) що поступають з граничної області зберігаються і обробляються відповідно до задачі (рівень обробки подій і аналітики, **event processing**, **Platform**). На цьому рівні події(дані) зберігаються (storage), обробляються (Event Processing), перенаправляються потрібним додаткам (Real-Time Message Brokering, Stream Processing). Додатково на цьому рівні відбувається адміністрування та керування пристроями з граничної області (Device Registry, Edge Device Management). Події (дані) обробляються з використанням аналітичних сервісів (Analytics) на основі них проводиться машинне навчання (Machine Learning), що дозволяє зробити певні висновки про об’єкт. Цей рівень як правило реалізований з використанням хмарних (Cloud) або туманних (Fog) обчислень. Якщо провести аналогію с АСУТП, то це рівень контролерів та SCADA (за виключенням функцій HMI). Отримання результатів, контроль, віддалене керування та адміністрування системи проводиться через кінцеві застосунки з використанням Internet. Цей рівень можна умовно порівняти з HMI в АСУТП.

На рис.2.4. показана подібна наведеній вище архітектура, однак у вигляді сервісів. На ньому область Edge представлений у вигляді датчиків (Sensors), Device Hub/Gateway (збір та маршрутизація даних) та Device Management (керування пристроями). Останні частково виконуються як хмарні обчислення так і на граничних пристроях. Усі функції збереження та первинної обробки подій (даних) зведені до Data Management. Усі інші функції обробки, в тому числі аналітичні показані як додатки PaaS, що взаємодіють з сервісами керування даних через API (Application Program Interface).

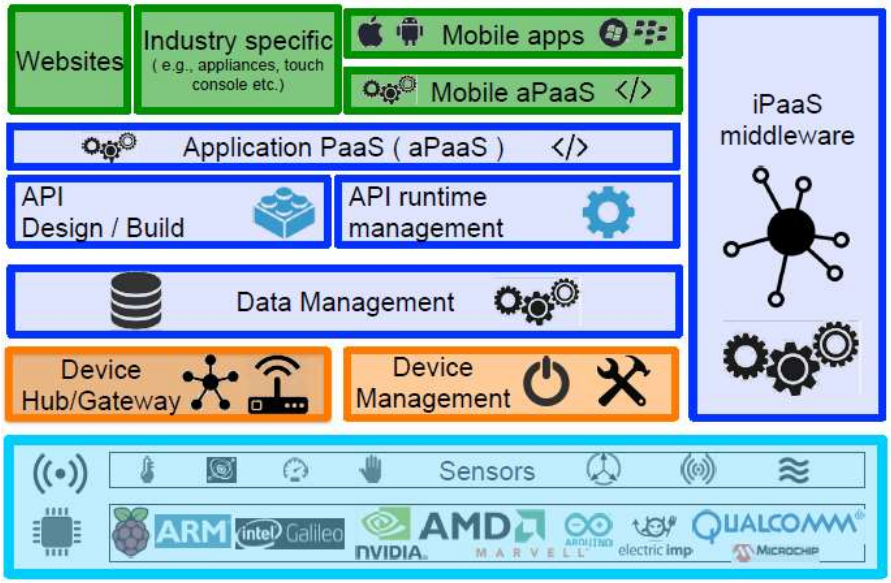


Рис. 2.4. Архітектура у вигляді сервісів.

Ще один приклад архітектури Інтернету Речей показаний на рис. 2.5. Як видно, усі наведені архітектури мають спільні риси: наявність трьох рівнів, подібні функції, наявність хмарних обчислень, використання Інтернету як інтеграційного рівня.

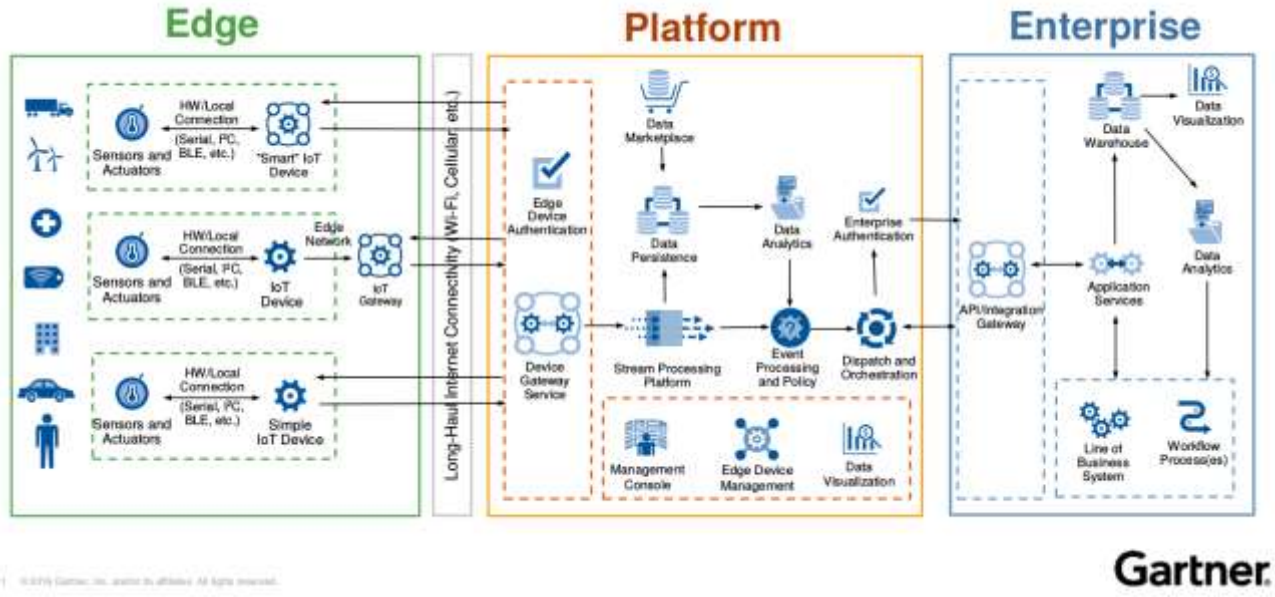


Рис. 2.5 Архітектура Інтернету речей

Датчики та живлення

Інтернет починається або закінчується однією подією: простий рух, зміна температури або, може бути, важіль замикає замок. На відміну від багатьох існуючих IT-пристроїв, Інтернет речей здебільшого пов'язаний з фізичною дією або подією. Він формує реакцію на якийсь фактор реального світу. Іноді при цьому один-єдиний датчик може згенерувати величезний обсяг даних, наприклад, акустичний датчик для профілактичного огляду обладнання. В інших випадках всього одного біта даних достатньо, щоб передати життєво важливі відомості про стан здоров'я пацієнта. Якою б не була ситуація, системи датчиків еволюціонували і, відповідно до закону Мура, зменшилися до субнанометрових розмірів і стали істотно дешевше. Саме до цього апелюють ті, хто прогнозує, що до Інтернету речей будуть підключені мільярди пристроїв, і саме тому ці прогнози виправдаються.

Тому, розглядаючи Інтернет Речей, необхідно розглядати мікроелектромеханічні системи, датчики і інші типи недорогих граничних пристроїв і їх електрофізичних властивостей. Також це стосується силових і енергетичних систем, необхідних для живлення цих граничних пристроїв. Не можна вважати, що граничні пристрої забезпечуються енергією за замовчуванням. Мільярди маленьких датчиків все одно потребують великої кількості енергії. З питанням живлення також пов’язані питання організації хмарних сервісів IoT.

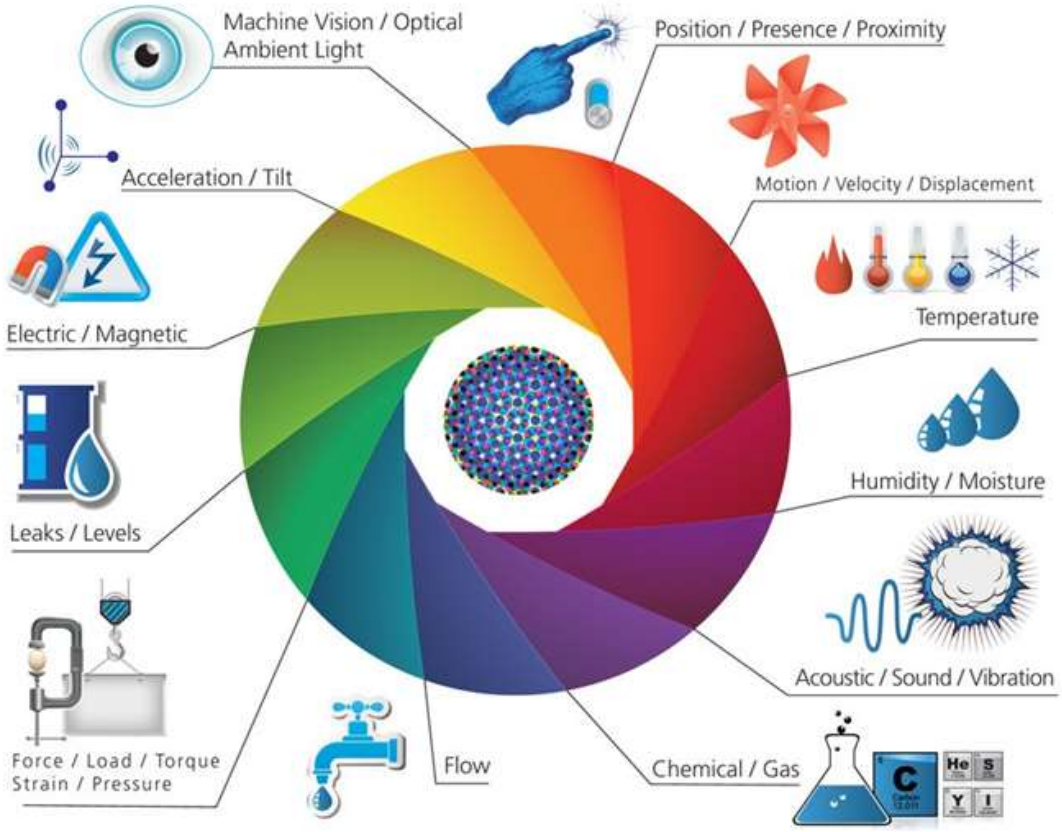


Рис. 2.6. Різновиди датчиків

Передача даних

Велика увага при розробці IoT приділяється встановленню з'єднання і роботі мереж. Інтернету речей не існувало б без надійних технологій передачі даних з найвіддаленіших і несприятливих областей в найбільші центри збору даних компаній *Google, Amazon, Microsoft* і *IBM*. Словосполучення «Інтернет речей» містить слово «Інтернет», тому необхідно вивчати питання, що стосуються мережних технологій, обміну даними та навіть теорії сигналів. Базова опора Інтернету речей - це не датчики і не програми, а можливість встановити з'єднання.

Передача даних і встановлення мережевого з'єднання базуються на базі систем зв'язку ближньої дії - персональних мереж (PAN), зазвичай побудованих без дотримання правил IP-протоколу. Це може бути як проводові так і бездротові мережі. До бездротових IoT-мереж/протоколів як правило відносяться протоколи *Bluetooth, mesh-мережі, Zigbee, Z-Wave*. Для IIoT це також *Wireless Hart* та *ISA100*. Це яскравий приклад різноманіття бездротових систем зв'язку IoT. Перелік дротових мереж ще більший, так як сюди входять усі можливі промислові мережі та протоколи.

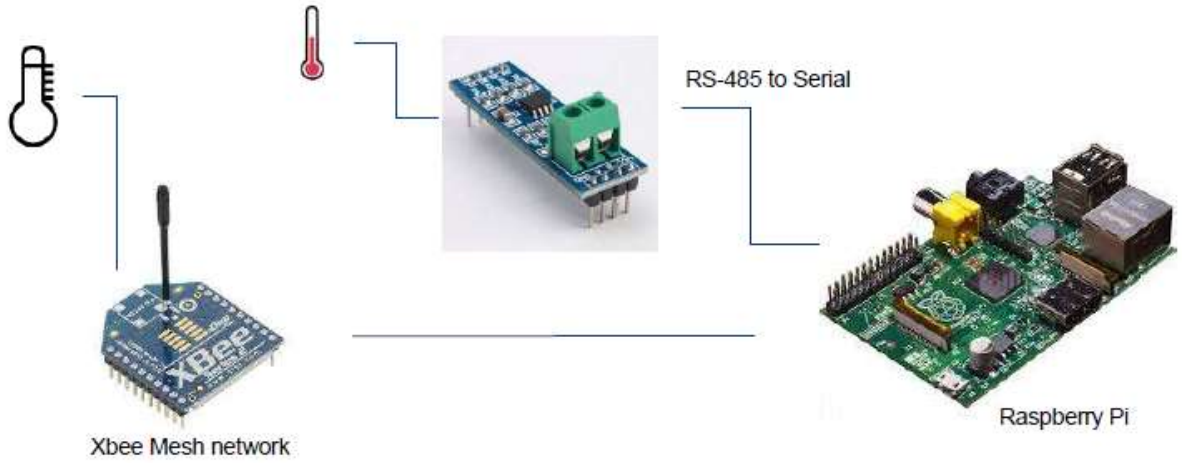


Рис. 2.7. Бездротові технології на основі протоколів Bluetooth, mesh-мережі, Zigbee, Z-Wave

Крім PAN використовуються бездротові локальні мережі та системи зв'язку на основі IP-протоколу, включаючи широкий діапазон Wi-Fi-мереж на основі стандартів IEEE 802.11, 6LoWPAN і технології Thread. Нерідко використовуються телекомунікації на основі стільникових стандартів (3G, 4G LTE) і нові стандарти, що забезпечують роботу Інтернету речей і міжмашинної взаємодії, такими як Cat-1 і Cat-NB, а також пропрієтарні протоколи LoRaWAN і Sigfox, що використовуються саме для IoT.

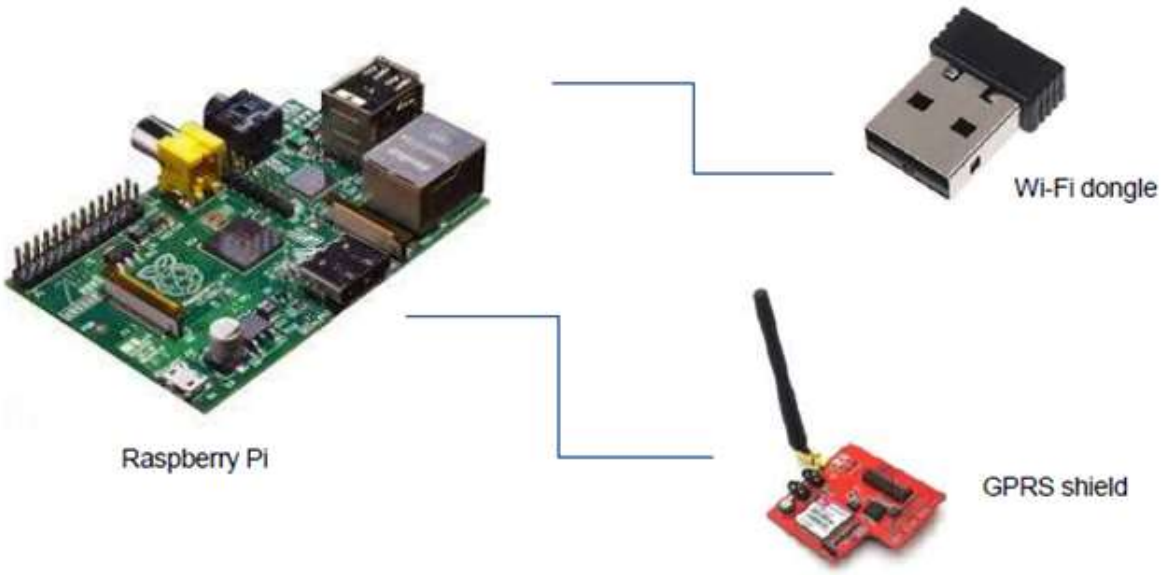


Рис. 2.8. Бездротові технології на основі IP-протоколу

Маршрутизація

Для передачі даних від датчиків в Інтернет-простір необхідні дві технології: маршрутизатор-шлюз і опорні інтернет-протоколи, що забезпечують ефективність обміну даними. Маршрутизатор особливо важливий в таких аспектах, як безпека, управління і напрям даних. Граничні маршрутизатори (Edge routers) керують і стежать за станом відповідних mesh-мереж, а також вирівнюють і підтримують якість даних. Також велике значення належить конфіденційності та безпеки даних. Маршрутизатор відіграє важливу роль в створенні віртуальних приватних мереж, віртуальних локальних мереж і програмно-визначених глобальних мереж. Вони в буквальному сенсі можуть містити тисячі вузлів, що обслуговуються єдиним граничним маршрутизатором, і в якійсь мірі маршрутизатор служить розширенням для хмари (edge device).

Рис. 2.9. Мережі та протоколи IoT

На цьому рівні використовується ряд протоколів, необхідних для обміну даними між вузлами, маршрутизаторами і хмарними сервісами в межах IoT-системи. Інтернет речей відкрив дорогу новим IoT-протоколам, які виходять на один рівень з традиційними протоколами HTTP і SNMP, які застосовуються вже кілька десятків років. Для передачі IoT-даних потрібні ефективні, енергозберігаючі протоколи з малою затримкою, здатні легко і безпечно відправляти дані в хмару і з нього. Зокрема тут використовуються такі протоколи, як всюдисущий MQTT, AMPQ і CoAP.

Туманні і граничні обчислення, аналітика і машинне навчання

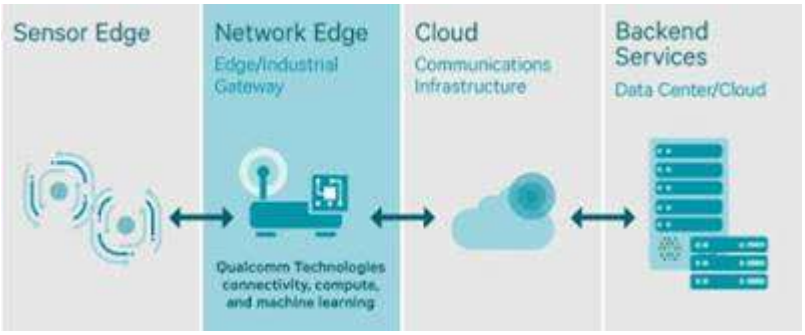


Рис. 2.10. Туманні та граничні обчислення

На цьому етапі необхідно вирішити, що робити з потоком даних, що надходять в хмарний сервіс з граничного вузла (Edge Device). Щоб навчитися правильно оцінювати, як система буде розвиватися і рости, необхідно розібратися у всіх тонкощах і складнощах архітектури хмарних систем, який вплив на IoT-систему робить запізнювання. Крім того, не все треба відправляти в хмару. Пересилання всіх IoT-даних обходиться значно дорожче, ніж їх обробка на кордоні мережі (граничні обчислення, Edge Computing) або включення граничного маршрутизатора в зону, яку обслуговує хмарний сервіс (туманні обчислення, Fog computing). Туманні обчислення також стандартизуються, зокрема є стандарт туманних обчислень, наприклад архітектура OpenFog.

Дані, які були отримані шляхом перетворення аналогового фізичного впливу в цифровий сигнал, можуть мати велику вагу. Саме тут в гру вступають засоби аналітики і процесори правил IoT-системи. Ступінь складності введення в дію IoT-системи залежить від того, яке рішення проектується. У деяких ситуаціях все досить просто: наприклад, коли на граничний маршрутизатор, який контролює кілька датчиків, потрібно встановити простий процесор правил, що відслідковує аномальні скачки температури. Інша ситуація - величезна кількість структурованих і неструктурованих даних в режимі реального часу передається в

хмарне озеро даних, що вимагає високої швидкості обробки (для прогнозної аналітики) і довгострокового прогнозування на базі високотехнологічних моделей машинного навчання, таких як рекурентна нейронна мережа в пакеті аналізу сигналів з кореляцією по часу. Тут є певні проблеми і складнощі аналітики, які вирішуються різними підходами та методами, наприклад складними обробниками подій, байесовськими мережами і формування нейронних мереж.

Загроза і безпека в Інтернеті речей

Багато IoT-систем не будуть обмежені безпечним простором будинку або офісу. Вони будуть розташовуватися в громадських місцях, в дуже віддалених областях, в рухомих транспортних засобах або навіть всередині людини. Інтернет речей - це величезна єдина мішень для будь-яких видів хакерських атак. Вже було виявлено нескінченна кількість направлених на IoT-пристрої навчальних атак, добре організованих зломів і навіть уразливостей в системі безпеки національного масштабу. Розробник IoT рішень повинен знати особливості таких вразливостей і способи їх усунення, стандартні заходи, спрямовані на захист Інтернету речей або будь-якого компонента мережі.

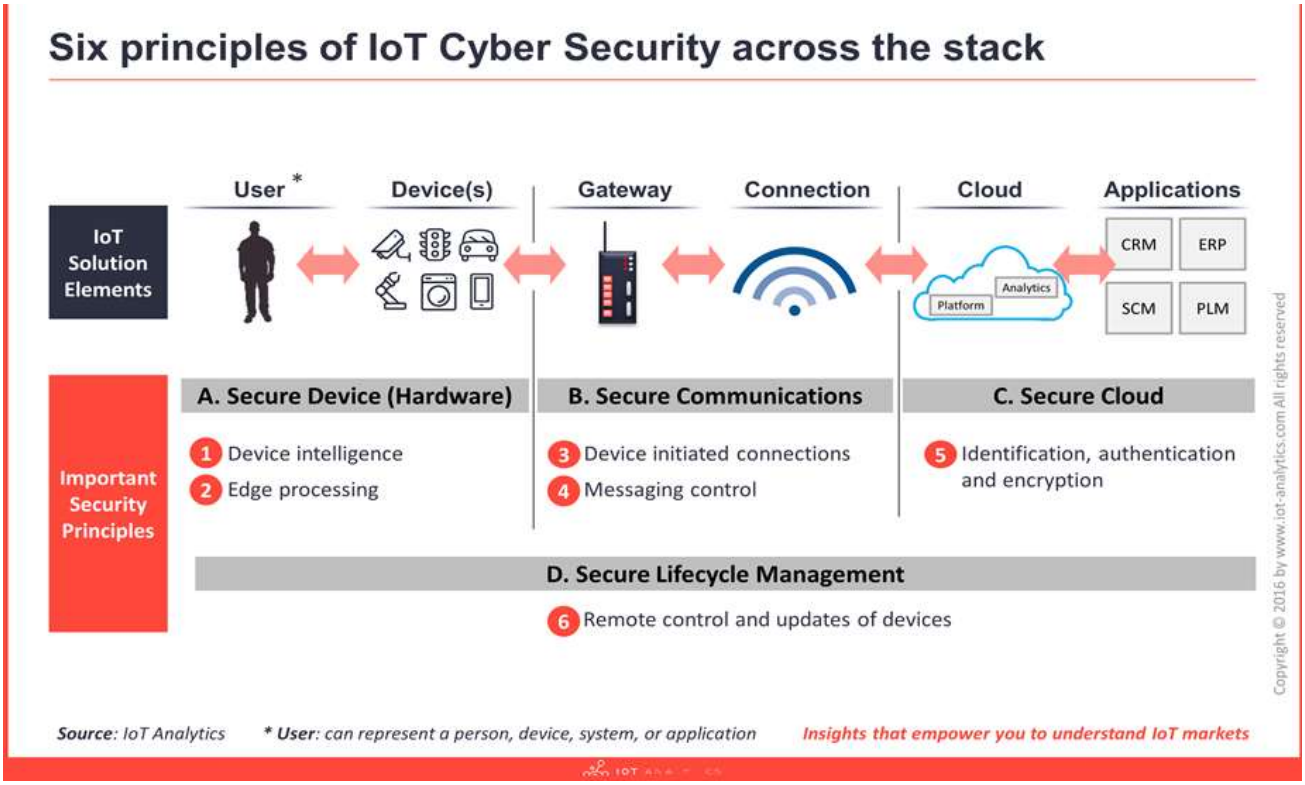


Рис. 2.11. Безпека в мережі IoT.

Контрольні питання до розділу

1. Історія Інтернету Речей.
2. Дайте визначення терміну «Промисловий Інтернет речей».
3. Для чого використовуються операційні технології (OT) в промисловому інтернеті речей?
4. Наведіть приклади застосування Промислового Інтернету Речей.
5. Які засоби, сервіси і технології відносяться до екосистеми Інтернету речей?
6. Наведіть та поясніть архітектуру Інтернету речей.
7. Представлення архітектури IoT у вигляді сервісів.
8. Назвіть особливості датчиків та живлення IoT.
9. Особливості передачі даних в IoT.

10. Особливості маршрутизації в IoT.
11. Туманні і граничні обчислення в IoT.
12. Безпека передачі даних в IoT.

Список рекомендованої літератури

1. Tripathy B. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. – Florida: CRC Press, 2017. – 334 c.
2. The 2nd Annual Internet of Things 2010 (англ.) [ЕлектроЕлектронний ресурс]. - Режим доступу: https://eu-ems.Com/summary.asp?event_id=55&page_id=342
3. Интернет вещей в научных исследованиях // електрон. текст. Дані URL: https://cyberleninka.ru/article/v/internet-veschey-v-nauchnyh-issledovaniyah (дата звернення: 01.06.2019)
4. АНАЛИЗ ТРАФИКА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ // електрон. текст. дані URL: https://cyberleninka.ru/article/v/analiz-trafika-ustroystv-interneta-veschey (дата звернення: 01.06.2019)
5. История появления технологии LoRa // електрон. текст. дані URL: *https://nekta.tech/technology/*

РОЗДІЛ 3. ЕТАЛОННА МОДЕЛЬ IoT

3.1. Стандарти сумісності IoT

Найближчим часом різнорідні «острівці» рішень, швидше за все, будуть випереджати в своєму розвитку розгортання IoT-рішень, заснованих на функціонально-сумісних стандартах. Так йдуть справи з будь-якою новою технологією на етапі її зародження.

Наприклад, *Sutaria and Govindachari* [1] відзначають, що дві характеристики мережевих IoT-пристроїв, що викликають найбільші проблеми, - це наявність пристроїв з низьким енергоспоживанням (розрахованих на роботу місяцями і роками без підзарядки) і частий обмін даними по мережах з втратою пакетів.

Нинішні стандартні протоколи Інтернету в цих умовах неоптимальні.
У більш широкому сенсі має місце дисбаланс між величезною кількістю пристроїв, що генерують дані з шаленою швидкістю в різних місцях, і використанням мережевих технологій і хмарних систем, які зберігають величезні обсяги даних в невеликій кількості локацій при відносно низькій швидкості оновлення даних.

Інтеграція цих двох класів систем для задоволення потреб користувачів вимагає певних можливостей від мережевих протоколів у всій архітектурі мережі і протоколів, від фізичного рівня до прикладного.

Над вирішенням цих питань працює кілька організацій і стандартизаційних форумів, прагнучі розширити або адаптувати протоколи Інтернету для пристроїв IoT. Основники організаціями є:

- *Міжнародний союз електрозв'язку (International Telecommunication Union, ITU):* 193 країни [2] і понад 700 членів по секторам і асоціаціям (науково-промислових підприємств, державних і приватних операторів зв'язку, радіомовних компаній, регіональних і міжнародних організацій).
- *Всесвітній форум IoT (IoT World Forum, IWF):* IBM, Intel, Cisco, Samsung.
- Національний інститут стандартів і технології Міністерства торгівлі США.
- *Консорціум індустріального Інтернету (Industrial Internet Consortium,IIC):* SAP, IBM, Intel, Fujitsu, General Electric, Oracle.

Для створення єдиної структури і класифікації необхідних функцій за їх місцем в стеку протоколів ряд цих груп також займається питанням формальної архітектури для IoT. У той час як існуючі стандарти та Інтернет зробили IoT можливим, в найближчому майбутньому навряд чи можлива поява стека нових стандартів, які доповнять або модифікують існуючі для сфери IoT.

Як і багато інших досягнень, що стали можливими завдяки Інтернету, IoT буде якийсь час стихійно розвиватися і проходити через процеси природного відбору, поки поступово не виявили життєздатні технології та механізми протоколів.

Але з урахуванням складності IoT має сенс створення архітектури, яка б специфікувала основні компоненти і їх взаємозв'язок. Архітектура IoT може надати такі переваги:

- дати адміністраторам мережі або IT-менеджеру корисний контрольний список для оцінки функціональності і повноти пропозицій від різних постачальників;
- служити орієнтиром для розробників в плані того, які функції потрібні в IoT і як вони взаємодіють;
- служити основою для стандартизації, стимулюючи сумісність і скорочення витрат.

3.2. Еталонна модель IoT від МСЕ-Т

Еталонна модель IoT від Міжнародного союзу електрозв'язку (МСЕ-Т) описана в Рекомендації Y.2060 [3]. На відміну від більшості інших еталонних моделей і архітектурних моделей, описаних в літературі, модель МСЕ-Т деталізує фактичні фізичні компоненти екосистеми IoT. Це корисно, тому що це зосереджує увагу на елементах екосистеми IoT, які повинні бути з'єднані, інтегровані, керовані і надані додаткам. Детальна специфікація екосистеми описує вимоги до можливостей IoT.

Один з важливих аспектів, який загострює модель, є той факт, що IoT на ділі не є мережею фізичних речей. Це скоріше мережа пристроїв, які з'єднано фізичними речами, разом з прикладними платформами - такими як комп'ютери, планшети і смартфони, які взаємодіють з цими пристроями. Тому огляд моделі MCE-T необхідно почати з визначення пристроїв:

- *Мережа зв'язку (Communication Network)* - інфраструктурна мережа, що з'єднує пристрої та додатки, така як мережа на основі стека протоколів IP або Інтернет.
- *Річ (Thing)* - предмет фізичного світу (фізичні речі) або інформаційного світу (віртуальні речі), який може бути ідентифікований та інтегрований в мережі зв'язку.
- *Пристрій (Device)* - елемент обладнання, який володіє обов'язковими можливостями зв'язку та додатковими можливостями вимірювання, спрацьовування, а також введення, зберігання і обробки даних.
- *Пристрій переносу даних (Data-carrying Device)* - пристрій переносу даних підключається до фізичної речі і непрямим чином з'єднує цю фізичну річ з мережами зв'язку. Прикладами можуть служити активні мітки RFID.
- *Пристрій збору даних (Data-capturing Device)* - під пристроєм збору даних розуміється пристрій, що зчитує / записуючий пристрій, що має можливість взаємодії з фізичними речами. Взаємодія може здійснюватися непрямим чином за допомогою пристроїв перенесення даних або безпосередньо за допомогою носіїв даних, підключених до фізичних речей.
- *Носій даних (Data Carrier)* - безбатарейний об'єкт перенесення даних, підключений до фізичної речі і має можливість надавати інформацію придатному для цього пристрою збору даних. Ця категорія включає штрих-коди і QR-коди, наклеєні на фізичні речі.
- *Сенсорний пристрій (Sensing Device)* - пристрій, який може виявляти або вимірювати інформацію, що відноситься до навколишнього середовища, і перетворювати її в цифрові електричні сигнали.
- *Виконавчий пристрій (Actuating Device)* - пристрій, який може перетворювати цифрові електричні сигнали, що надходять від інформаційних мереж, в дії.
- *Пристрій загального призначення (General Device)* – пристрій загального призначення володіє вбудованими можливостями обробки і зв'язку і може обмінюватися даними з мережами зв'язку з використанням дротових або бездротових технологій. Пристрої загального призначення включають обладнання та прилади, які стосуються різних галузей застосування IoT, наприклад, верстати, побутові електроприлади і смартфони.
- *Шлюз (Gateway)* - елемент IoT, що з'єднує пристрої з мережами зв'язку.

Він виконує необхідну трансляцію між протоколами, що використовуються в мережах зв'язку і в пристроях.

Унікальним аспектом IoT, в порівнянні з іншими мережевими системами, очевидно є наявність безлічі фізичних речей і пристроїв, відмінних від обчислювальних пристроїв і пристроїв обробки даних.

На рис.3.3, адаптованому з Рекомендації Y.2060, зображені типи пристроїв в моделі MCE-T. Модель розглядає IoT як мережу пристроїв, тісно пов'язаних з речами. Сенсорні і виконавчі пристрої взаємодіють з фізичними речами в навколишньому середовищі. Пристрої збору даних зчитують дані з фізичних речей або записують дані на фізичні речі шляхом взаємодії з пристроями перенесення даних або носіями даних, підключеними або пов'язаними з фізичним об'єктом тим чи іншим чином.

Ця модель показує відмінність між пристроями перенесення даних і носіями даних. Пристрій переносу даних є пристроєм в сенсі Рекомендації Y.2060. Як мінімум, пристрій завжди має можливості зв'язку і може мати інші електронні можливості. Прикладом пристрою перенесення даних є RFID-мітка. У той же час носій даних - це елемент, приєднаний до фізичної речі з метою ідентифікації або інформування.

В рекомендації Y.2060 відзначається, що технології, які використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження. Приклади кожної з них:

- *Радіочастотні*: радіочастотні ідентифікаційні (RFID) - бірки, або радіопозначки.
- *Оптичні*: штрих-коди і QR-коди можуть служити прикладами ідентифікаційних носіїв даних, які зчитуються оптично.
- *Інфрачервоні*: інфрачервоні мітки, що можна використовувати в Збройних Силах, лікарнях та інших середовищах, де потрібно відстежувати розташування і переміщення персоналу. Це можуть нашивки на військовій формі, що відбивають світло, і такі, що працюють від батарейок та випромінюють ідентифікуючу інформацію.

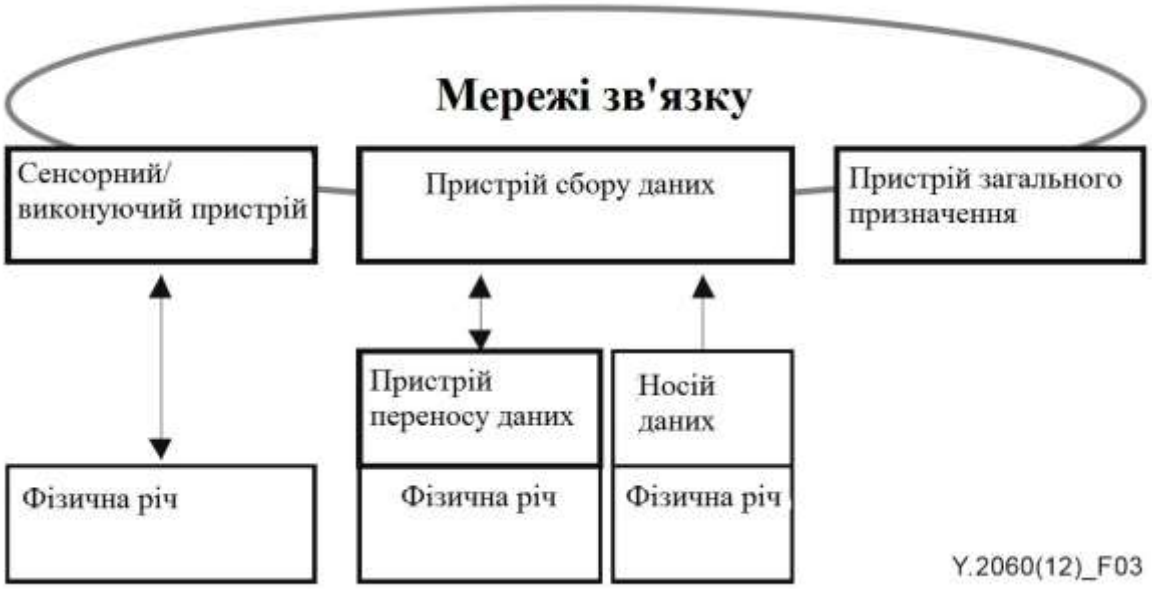


Рис. 3.1. Типи пристроїв та їх взаємозв’язок із фізичними речами

Останні можуть мати кнопку, при натисканні якої бейдж може використовуватись для проходу через автоматичні контрольні пункти, або ж бейджи, що автоматично повторюють сигнал для контролю за переміщеннями персоналу.

Пульти дистанційного керування, що використовуються в побуті або в інших середовищах для управління електронними пристроями, теж можна легко інтегрувати в IoT.

- *Гальванічне збудження*: прикладом можуть служити медичні імпланти, які використовують електропровідні властивості людського тіла [4]. В ході комунікації між імплантом і поверхнею гальванічна пара передає сигнали з імпланта на електроди, виведені на шкіру. Ця схема використовує дуже мало енергії, що дозволяє знизити розмір і складність імплантованого пристрою.

Останнім типом пристроїв з рисунку є пристрої *загального призначення*.

Вони володіють можливостями обробки даних і зв'язку, які можуть бути інтегровані в IoT. Хорошим прикладом є технологія «розумного будинку», яка може інтегрувати практично будь-який пристрій в будинку в мережу для централізованого або дистанційного керування.

В **Рекомендації Y.2060** наведено огляд елементів, задіяних в IoT. Розглядаються різні способи зв'язку з фізичними пристроями. Передбачається, що одна або кілька мереж підтримують зв'язок між пристроями.

В рекомендації особливу увагу приділено такому простою, пов'язаному з IoT: *шлюзу*. Як мінімум шлюз працює транслятором між протоколами. Шлюзи вирішують одну з

головних проблем при проектуванні IoT, а саме проблему сумісності, як між різними пристроями, так і між пристроями та Інтернетом або корпоративною мережею.

«Розумні» пристрої підтримують широкий спектр бездротових і дротових технологій передачі даних і мережевих протоколів. Крім того, можливості обробки даних у таких пристроїв, як правило, обмежені.

Рекомендація Y.2067 [5] закріплює вимоги до шлюзів IoT, які зазвичай розпадаються на три категорії:

- Шлюз підтримує різні технології доступу до пристроїв, дозволяючи пристроїв обмінюватися даними один з одним і з мережею Інтернет або корпоративною мережею, що містить додатки IoT. Такі схеми доступу можуть, наприклад, включати *ZigBee, Bluetooth* і *Wi-Fi*.
- Шлюз підтримує необхідні мережеві технології як для локальних, так і для глобальних мереж. Ці технології можуть включати в себе *Ethernet* і *Wi-Fi* на території організації, а також стільниковий зв'язок, *Ethernet, DSL* і кабельний доступ до Інтернету і глобальним корпоративним мережам.
- Шлюз підтримує взаємодію з додатками, управління мережею і функції безпеки.

Дві перших вимоги включають в себе трансляцію протоколів між різними мережевими технологіями і стеками протоколів.

Третя вимога зазвичай називається функцією IoT-агента. По суті, IoT-агент надає функціональність високого рівня від імені IoT-пристроїв, таку як організація або резюмування даних з декількох пристроїв для передачі в IoT-додатки, забезпечення протоколів і функцій безпеки і взаємодія з системами управління мережею.

Термін «мережа зв'язку» прямо не визначається в серії IoT-стандартів Y.206x. Мережа (або мережі) зв'язку підтримує зв'язок між пристроями і може безпосередньо підтримувати прикладні платформи. Вона може мати розміри невеликого IoT, такого як домашня мережа «розумних» пристроїв. У більш загальному сенсі мережу (або мережі) пристроїв з'єднується з корпоративними мережами або Інтернетом для зв'язку з системами додатків і серверами, на яких розташовані бази даних, пов'язані з IoT.

В рекомендації розглядаються також можливості зв'язку пристроїв між собою.

- *Перша можливість* - зв'язок між пристроями через шлюз. Наприклад, за допомогою шлюзу сенсорне або виконавчий пристрій з підтримкою *Bluetooth* може здійснювати зв'язок з пристроєм збору даних або пристроєм загального призначення, що використовують *Wi-Fi*.
- *Друга можливість* - зв'язок по мережі зв'язку без шлюзу. Наприклад, якщо всі пристрої в мережі «розумного будинку» підтримують *Bluetooth*, вони можуть управлятися з комп'ютера, планшета або смартфона з підтримкою *Bluetooth*.
- *Третя можливість* - прямий зв'язок пристроїв між собою за окремою локальної мережі, в той час як зв'язок із зовнішньою мережею (на малюнку не показана) здійснюється через шлюз LAN.

Кожна фізична річ в Інтернеті речей може бути представлена в інформаційному світі однією або декількома віртуальними речами, але при цьому віртуальна річ може існувати без відповідної фізичної речі. Фізичні речі зіставлені віртуальним речам, що зберігаються в БД і інших структурах даних. Додатки обробляють віртуальні речі і працюють з ними.

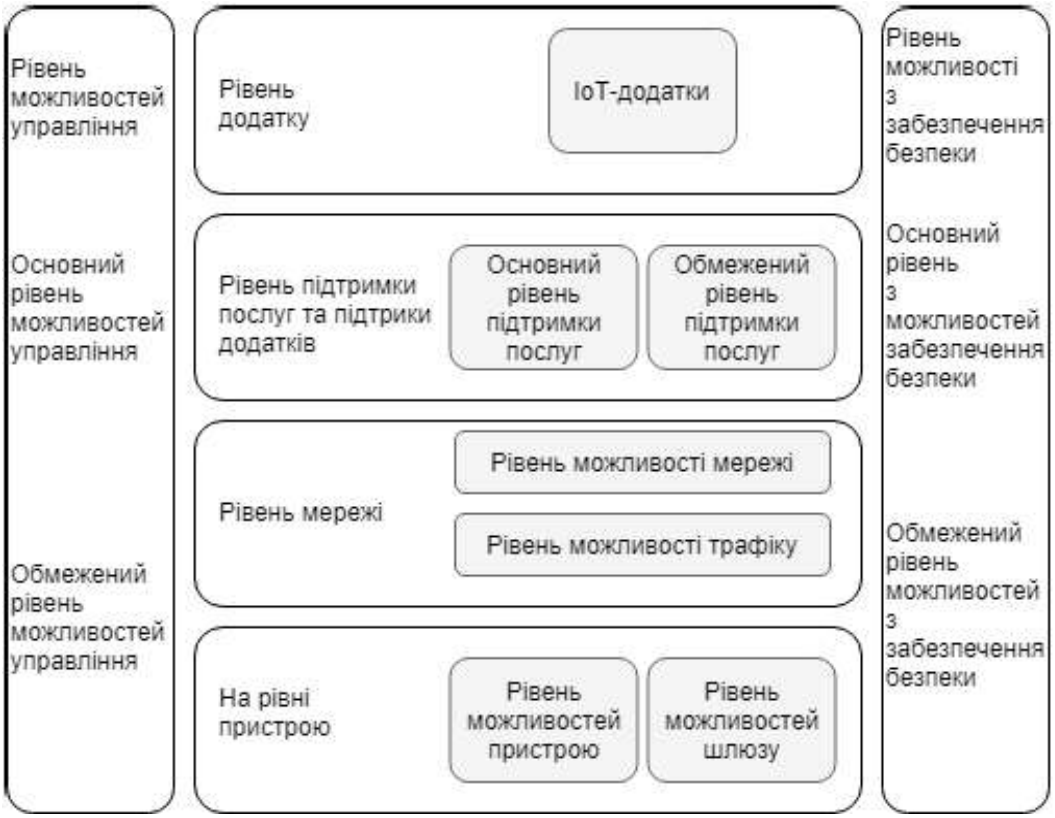


Рис. 3.2. Еталона модель IoT за рекомендацією Y.2060

Еталонна модель IoT від МСЕ-Т складається з чотирьох рівнів плюс можливості управління і безпеки, що діють між рівнями. До сих пір ми говорили про рівень пристрою. У термінах функціональності зв'язку рівень пристрою включає в себе, грубо кажучи, фізичний і канальний рівні OSI.

Рівень мережі виконує дві базові функції. Можливості мережі відносяться до взаємодії пристроїв і шлюзів. Транспортні можливості відносяться до транспорту інформації служб і додатків IoT, а також інформацією управління і контролю IoT.

Грубо кажучи, ці можливості відповідають мережевому і транспортному рівням OSI.

Рівень підтримки послуг і підтримки додатків надає можливості, які використовуються додатками. Багато різноманітних додатків можуть використовувати загальні можливості підтримки. До прикладів належать спільне опрацювання даних і управління БД. Спеціалізовані можливості підтримки – це конкретні можливості, які призначені для задоволення потреб конкретного підмножини додатків IoT.

Рівень додатку складається з усіх додатків, взаємодіючих з IoT-пристроями.

Рівень можливостей управління охоплює традиційні функції управління мережею, тобто управління несправностями, управління конфігурацією, управління обліком, управління показниками роботи і управління безпекою.

В Рекомендації Y.2060 як приклади загальних можливостей управління перераховані:

- *управління пристроями*: приклади включають виявлення пристроїв, автентифікацію, дистанційну активацію і дезактивацію пристроїв, конфігурацію, діагностику, оновлення прошивки і / або ПЗ, управління робочим статусом пристрою;
- *управління топологією локальної мережі*: прикладом є управління конфігурацією мережі;
- *управління трафіком і перевантаженнями*: наприклад, виявлення умов перевантаженості мережі і реалізація резервування ресурсів для термінових і / або життєво важливих потоків трафіку.

Спеціалізовані можливості управління тісно пов'язані з вимогами додатків, наприклад, вимогами з контролю лінії передачі електроенергії в «розумній» електромережі.

Рівень можливостей забезпечення безпеки включає загальні можливості забезпечення безпеки, які не залежать від додатків. В Рекомендації Y.2060 приклади загальних можливостей забезпечення безпеки включають:

- *На рівні програми*: авторизацію, автентифікацію, захист конфіденційності і цілісності даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист;
- *на рівні мережі*: авторизацію, автентифікацію, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;
- *на рівні пристрою*: автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами додатків, наприклад, вимогами безпеки мобільних платежів.

3.3. Еталонна модель від Всесвітнього форуму IoT

Всесвітній форум IoT **(IoT World Forum, IWF)** - щорічна подія, що спонсорується галуззю та об'єднує представників бізнесу, державних структур та вузівської науки з метою просування IoT на ринок.

Комітет з архітектури Всесвітнього форуму IoT, складений з лідерів індустрії, включаючи IBM, Intel та Cisco, в жовтні 2014 опублікував еталонну модель IoT. Ця модель є загальною структурою, покликаною допомогти галузі прискорити розгортання IoT.

Модель призначена для того, щоб стимулювати співпрацю та сприяти створенню повторюваних моделей впровадження.

Ця еталонна модель є корисним доповненням до моделі *MCE-T*. Документи *MCE-T* роблять упор на рівнях пристрою та шлюзу, описуючи верхні рівні лише в загальних рисах. І дійсно, в Рекомендації Y.2060 увесь опис рівня додатку вмістився в одну фразу. Найбільше уваги рекомендації серії Y.206x приділяють визначенню концепції для підтримки розробки стандартів взаємодії з пристроями IoT.

IWF стурбований більш масштабним питанням розробки додатків, проміжного програмного забезпечення і функцій підтримки для корпоративного Інтернету речей. Запропонована семирівнева модель зображена на рисунку 3.3.

Рис. 3.3. Еталонна модель від Всесвітнього форуму IoT

Документальний опис моделі IWF, опублікований Cisco [6], вказує, що розроблена модель відрізняється наступними характеристиками:

- *спрощує*: допомагає розбити складні системи на частини так, щоб кожна з цих частин стала більш зрозумілою;
- *прояснює*: надає додаткові відомості для точної ідентифікації рівнів IoT і вироблення загальної термінології;

- *ідентифікує*: ідентифікує аспекти, в яких ті чи інші типи обробки оптимізовані в різних частинах системи;
- *стандартизує*: є першим кроком до того, щоб постачальники могли створювати продукти IoT, здатні взаємодіяти один з одним;
- *організовує*: робить IoT реальним і доступним, а не просто абстрактною концепцією.

Рівень 1 утворюють фізичні пристрої та контролери, які можуть керувати кількома пристроями.

Рівень 1 моделі IWF приблизно відповідає рівню пристрою в моделі MCE-T . Як і в моделі MCE-T, елементи на цьому рівні – не фізичні речі як такі, а пристрої, які взаємодіють з фізичними речами, такі як сенсорні і виконавчі пристрої. Серед інших можливостей ці пристрої можуть вміти здійснювати аналого-цифрове і цифро-аналогове перетворення, генерацію даних, а також підтримувати дистанційний опитування і / або дистанційне керування.

Рівень 2 моделі IWF приблизно відповідає рівню мережі в моделі MCE-T. Основна відмінність в тому, що модель IWF відносить шлюзи до рівня 2, в той час як в моделі MCE-T вони відносяться до рівня 1. Оскільки шлюз є мережевим пристроєм і пристроєм зв'язку, віднесення його до рівня 2 має більше сенсу.

З логічної точки зору цей рівень реалізує зв'язок пристроїв між собою і між пристроями і низькорівневою обробкою на рівні 3. З фізичної точки зору цей рівень складається з мережевих пристроїв, таких як маршрутизатори, комутатори, шлюзи і брандмауери, що використовуються для створення локальних і глобальних мереж і підключення до Інтернету.

Цей рівень дозволяє пристроям здійснювати зв'язок один з одним і за допомогою більш високих логічних рівнів обмінюватися даними з прикладними платформами, такими як комп'ютери, пристрої дистанційного управління і смартфони.

У багатьох впроваджуваних системах IoT розподілена мережа датчиків може генерувати великі обсяги даних. Наприклад, офшорні нафтові родовища і нафтопереробні заводи можуть генерувати до терабайта даних щодня. Літак може генерувати кілька терабайт даних на годину. Замість того, щоб зберігати всі ці дані постійно (або хоча б довгий час) в централізованому сховищі, доступному для додатків IoT, часто більш доцільно виконувати якомога більшу частину обробки даних якомога ближче до датчиків. Тому завданням рівня периферійних обчислень (edge computing level) (**рівень 3**) є перетворення мережевих потоків даних в інформацію, придатну для зберігання і більш високорівневої обробки. Елементи обробки на цьому рівні можуть мати справу з великими обсягами даних і виконувати операції перетворення даних, в результаті яких зберігати доводиться вже набагато менший обсяг.

Опублікований Cisco документ по моделі IWF [7] містить такі приклади операцій на рівні периферійних обчислень:

- *аналіз*: аналіз даних по критеріях того, чи підлягають вони обробці на більш високому рівні;
- *форматування*: переформатування даних для однакової високорівневої обробки;
- *розархівування / декодування*: обробка криптографічних даних з додатковим контекстом (таким як походження);
- *дистиляція / скорочення*: скорочення і / або резюмування даних для того, щоб мінімізувати обсяг даних, трафік в мережі і в високорівневих системах обробки;
- *оцінка*: визначення того, чи становлять дані порогове значення або аварійний сигнал; цей процес повинен включати перенаправлення даних додатковим одержувачам.

Елементи обробки на цьому рівні відповідають пристроїв загального призначення в моделі MCE-T. Як правило, вони розгортаються фізично на краю мережі IoT, тобто поруч з сенсорами і іншими пристроями генерації даних.

Таким чином, частина базової обробки великих обсягів генеруються даних знімається з прикладних програм IoT, розташованих центрально.

Обробка на рівні периферійних обчислень іноді називається *туманними обчисленнями (Fog Computing).* Туманні обчислення і туманні служби, як очікується, стануть відмінною характеристикою IoT. Цей принцип проілюстрований на рис. 3.4.

Туманні обчислення представляють в сучасних мережевих технологіях тренд, протилежний хмарних обчислень. У хмарні обчислення великий обсяг централізованих ресурсів зберігання і обробки даних доступний розподіленим споживачам за допомогою хмарних мережевих структур для відносно невеликого числа користувачів.

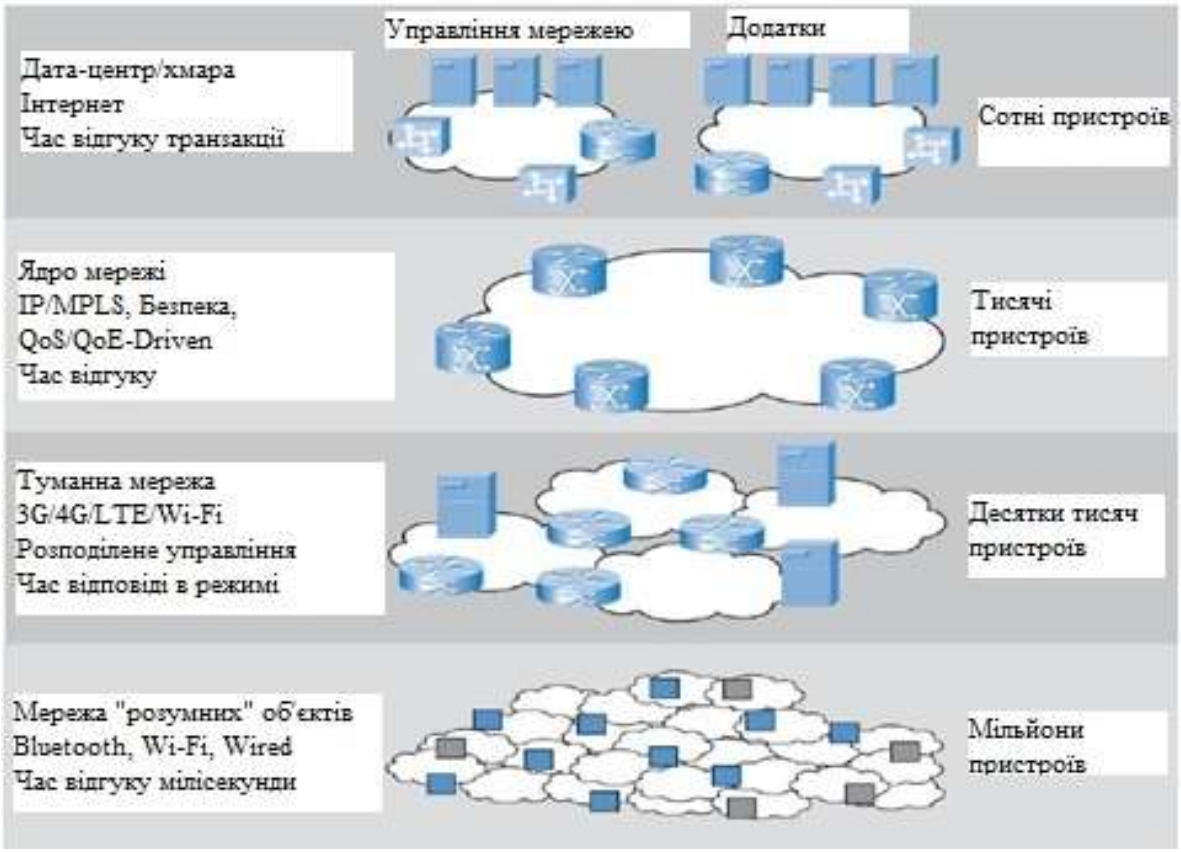


Рис. 3.4. Туманні обчислення

В туманних обчисленнях велике число окремих інтелектуальних об'єктів здійснюють зв'язок з туманними мережевими структурами, які здійснюють обчислення і зберігають ресурси поруч з периферійними пристроями в IoT.

Туманні обчислення вирішують проблеми, що виникли внаслідок діяльності тисяч або мільйонів «розумних» пристроїв, включаючи проблеми безпеки, конфіденційності, обмежених можливостей мережі і затримки. Термін «туманні обчислення» обраний тому, що туман стелиться по землі, в той час як хмари знаходяться високо в небі.

На рівні 4, рівні накопичення даних, дані, що надійшли з різних пристроїв, профільтровані і оброблені рівнем периферійних обчислень, поміщаються в сховище, де будуть доступні для більш високих рівнів. Цей рівень разюче відрізняється і від низькорівневих (туманних), і від високорівневих (хмарних) обчислень за особливостями конструкції, вимогам і методам обробки.

Таблиця 3.1. Порівняння хмарних та туманних обчислень

	Хмара	**Туман**
Розташування ресурсів, зберігання / обробки	Центр	Край
Затримка	Від низької до високої	Низька
Доступ	Фіксований або бездротовий	Головним чином безпровідний
Підтримка мобільності	Не застосовується	Так
Контроль	Централізований /ієрархічний (повний контроль)	Розподілений / ієрархічний (частковий контроль)
Доступ до служб	Через ядро	На краю / з портативного пристрою (смартфон і т.д.)
Доступність	99,99%	Висока нестабільність /високий рівень резервування
Число користувачів / пристроїв	Десятки і сотні мільйонів	Десятки мільярдів
Основний генератор контенту	Люди і пристрої	Пристрої / сенсори
Генерація контенту	У центральному розташуванні	Скрізь
Споживання контенту	На кінцевих пристроях	Скрізь
Віртуальна програмна інфраструктура	Центральні корпоративні сервери	Призначені для користувача пристрої

Дані, що проходять крізь мережу, називаються «даними в русі». Швидкість і організація даних в русі визначається пристроями, що генерують дані. Генерація даних відбувається по подіям, або періодично, або по виникненні якої-небудь події в середовищі. Для збору даних та їх обробки необхідно реагувати на їх появу в реальному часі. Навпаки, багатьом додаткам не потрібно обробляти дані зі швидкістю мережевої передачі. На практиці ні хмарна мережу, ні прикладні платформи не змогли б встигати за обсягами даних, що генеруються величезною кількістю IoT-пристроїв. Замість цього додатки мають справу з «даними в спокої», тобто даними в тому чи іншому легкодоступному сховище. Додатки можуть звертатися до даних у міру необхідності або поза режимом реального часу. Таким чином, високі рівні функціонують за принципом транзакцій, в той час як три нижніх рівні працюють по подіях.

Нижче перераховані названі в [8] операції, що виконуються на рівні накопичення даних:

- *перетворення «даних в русі» в «дані в спокої»;*
- *перетворення формату з мережевих пакетів в реляційні таблиці БД;*
- *перехід від обчислень щодо подій до обчислень за запитом;*
- *значне зниження обсягу даних за рахунок фільтрації і вибіркового зберігання.*

Ще один погляд на рівень накопичення даних полягає в тому, що він являє собою кордон між інформаційними технологіями (IT), під якими розуміється цілий спектр

технологій обробки інформації, включаючи ПЗ, обладнання, технології зв'язку і супутні служби, і операційними технологіями (*Operational Technology, OT*), що представляють собою обладнання і ПЗ, які виявляють або викликають зміни шляхом прямого моніторингу та / або контролю фізичних пристроїв, процесів і подій на підприємстві.

Рівень накопичення даних вбирає велику кількість даних і поміщає їх в сховище, практично не пристосовуючи до потреб конкретних програм або груп додатків. З рівня периферійних обчислень в сховище може надходити безліч різних видів даних в різних форматах і від різнорідних оброблювачів. **Рівень абстракції (рівень 5)** даних може агрегувати і форматувати такі дані способами, які роблять доступ додатків більш керованим і ефективним. У числі пов'язаних завдань можуть бути наступні:

- *Комбінування даних з різних джерел, включаючи вивірку кількох форматів даних.*
- *Виконання необхідних перетворень для забезпечення однакової семантики даних з різних джерел.*
- *Приміщення відформатованих даних у відповідну базу даних, наприклад, великі обсяги повторюваних даних поміщаються в систему великих даних, таку як Hadoop. Дані подій направляються в реляційну СУБД, що відрізняється більш швидким часом реакції і адекватним інтерфейсом для таких типів даних.*
- *Оповіщення додатків більш високого рівня про те, що дані заповнені або досягнутий певний рівень даних.*
- *Консолідація даних в одному місці (за допомогою ETL (extract, transform, load), ELT (extract, load, transform) або реплікації даних) або надання доступу до декількох джерел даних шляхом віртуалізації даних.*
- *Захист даних шляхом відповідної автентифікації і авторизації.*
- *Нормалізація / денормалізація і індексація даних для швидкого доступу додатків.*

Рівень 6 (рівень додатку) містить додатки будь-якого типу, що використовують дані IoT на вході або керуючі IoT-пристроями. Як правило, додатки взаємодіють з рівнем 5 і з даними в спокої, тому їм не обов'язково функціонувати на швидкостях мережі.

Слід передбачити спрощений режим роботи, який дозволить додаткам минути проміжні рівні і безпосередньо взаємодіяти з рівнем 3 або навіть рівнем 2. Модель IWF не визначає додатки по всій строгості, вважаючи цей аспект виходять за рамки дискусії про модель IWF.

Рівень взаємодії і процесу (рівень 7) з'явився в результаті визнання того, що IoT буде корисний лише тоді, коли з ним зможуть взаємодіяти люди. Цей рівень може включати кілька додатків і обмін даними і / або керуючої інформацією по Інтернету або корпоративної мережі.

IWF вважає еталонну модель IoT прийнятої в галузі базовою структурою, спрямованої на стандартизацію концепцій і термінології, пов'язаних з IoT.

Що ще більш важливо, модель IWF визначає необхідний функціонал і проблеми, які потрібно вирішити до того, як галузь зможе реалізувати цінність IoT.

Ця модель корисна як для постачальників, що розробляють функціональні елементи всередині моделі, так і для замовників, допомагаючи їм виробити свої вимоги і оцінювати пропозиції постачальників.

3.4. Модель NIST Special Publication 800-183

Публікація «Networks of Things» Національного інституту стандартів і технології Міністерства торгівлі США вийшла в розділі COMPUTER SECURITY в липні 2016 року [9]. Основними пунктами публікації є:

- Введено поняття «Network of« Things » - вид розподілених систем.
- IoT, мережі соц. медіа, мережі сенсорів, промисловий Інтернет розглядаються як види NoT.
- «Речами» може бути програмне забезпечення, «залізо», їх комбінація і людина.
- Виділено та описано характеристики п'яти ключових примітивів: сенсор, агрегатор (шлюз), канал зв'язку, зовнішня утиліта і тригер рішення.

- У модель також внесені шість елементів: середа, витрати, місце розташування, власник (оператор), Device_ID (для будь-якого прімітива), і момент часу (снепшот).

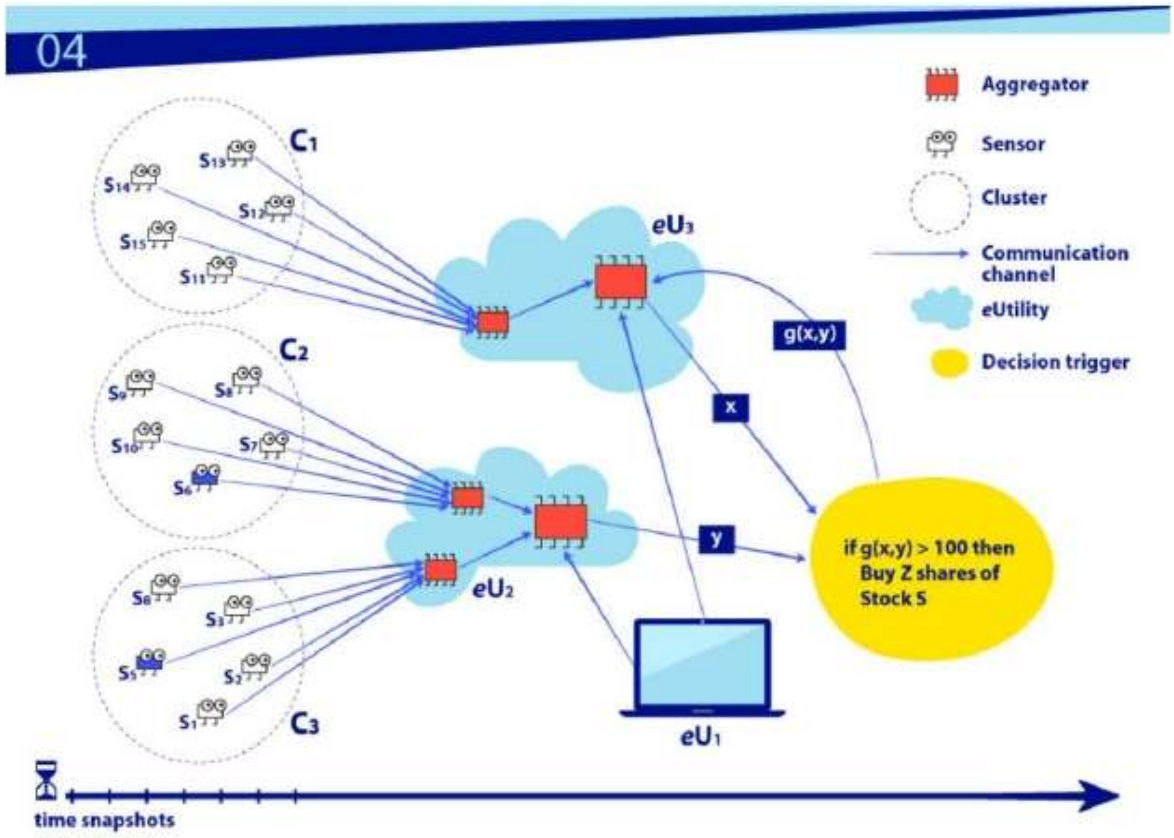


Рис. 3.5. Архітектура моделі за публікацією NIST Special Publication 800-183

Додаткові міркування:

- Система може бути відкритою, закритою або мати проміжний стан.
- Необхідність використання шаблонів проектування для побудови великих систем.
- Рівень довіри до системи в деякий момент часу - функція від реалізації примітивів з урахуванням основних елементів.
- Низька вірогідність виявлення помилок в системі під час тестування.
- Облік механізмів і особливостей впливу на зовнішнє середовище.

У публікації зачіпаються питання безпеки і надійності.

Як можна побачити з рисунку для шлюзів (агрегаторів) тут виділяється більша роль аніж у архітектурах міжнародного IoT форуму та Міжнародного союзу електрозв'язку. Агрегатор не просто виконує функцію «перепакування» з одного стеку протоколів у інший, а ще й агрегує, аналізує та зберігає дані.

3.5. Модель Industrial Internet of Things Reference Architecture

Консорціум промислового інтернету об'єднує понад 100 компаній. У січні 2017 року побачила версія 1.8 документа «The Industrial Internet of Things. Volume G1: Reference Architecture». Також були опубліковані INDUSTRIAL INTERNET SECURITY FRAMEWORK, і INDUSTRIAL INTERNET CONECTIVITY FRAMEWORK. Серед авторів архітектури представники SAP, IBM, Intel, Fujitsu, General Electric, Oracle.

В референсній архітектурі представлено три шаблони реалізації IIoT-системи.

Рівень краю збирає дані з кінцевих вузлів, використовуючи локальну мережу. Архітектурна характеристика цього рівня, включаючи широту розподілу, розташування, обсяг управління та характер локальних мереж, залежить від конкретних випадків використання.

Рівень платформи отримує, обробляє та пересилає команди управління з рівня підприємства на рівень краю. Він об'єднує процеси та аналізує потоки даних з краю та інших рівнів. Він забезпечує функції керування пристроями та активністю. Він також пропонує спеціальні послуги, не пов'язані з доменом, такі як запити даних та аналітика.

Рівень підприємства впроваджує доменні додатки, системи прийняття рішень та забезпечує інтерфейси для кінцевих користувачів, включаючи операторів. Рівень підприємства отримує потоки даних з краю та рівня платформи. Він також передає команди керування рівнями краю та рівнями платформи.

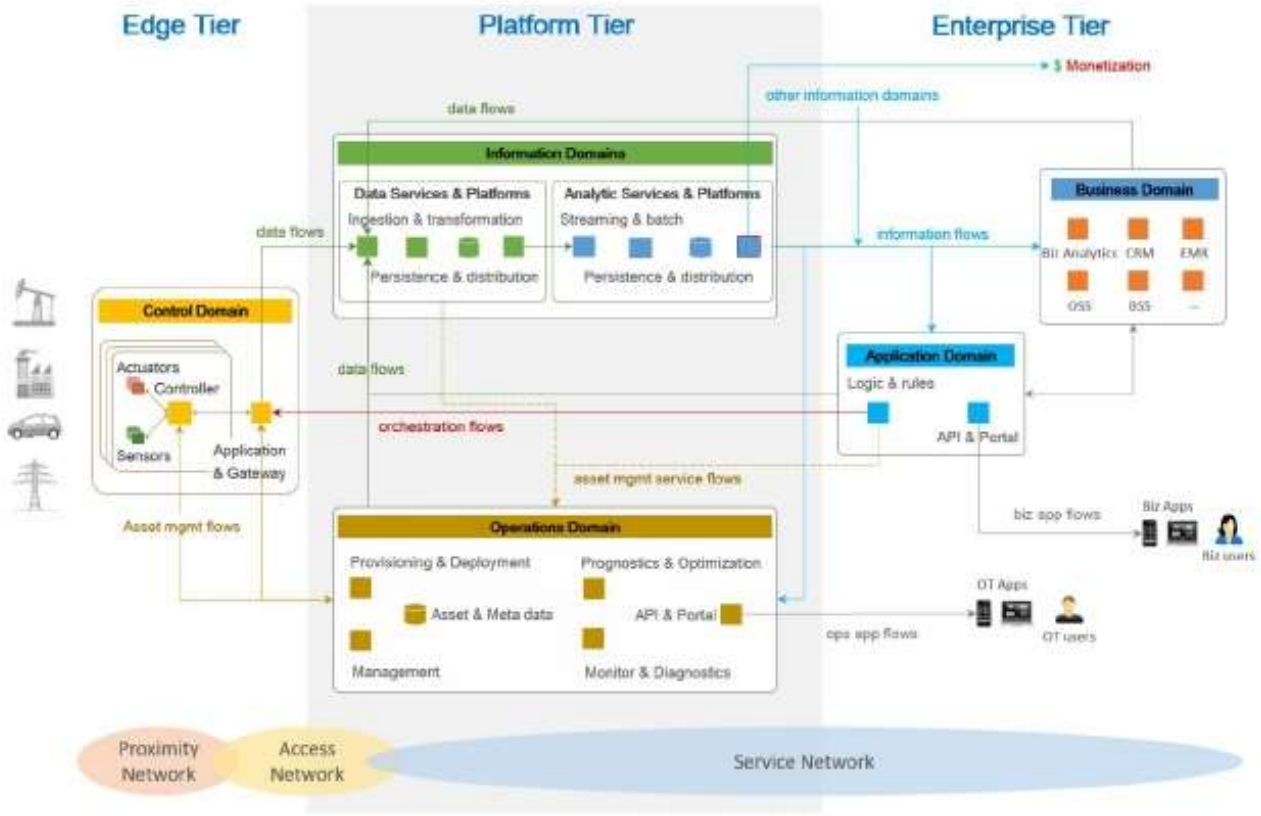


Рис. 3.6. Трирівневий шаблон моделі Industrial Internet of Things Reference Architecture

З'єднання та управління за допомогою шлюзів: шлюзовий зв'язок та схема архітектури керування складаються з локального рішення для підключення до краю системи IIoT з шлюзом, який переходить до широкосмугової мережі, як показано на рисунку (З'єднання та управління за допомогою шлюзів).

Шлюз виступає як кінцева точка для широкосмугової мережі при ізоляції локальної мережі краєвих вузлів.

Ця схема архітектури дозволяє локалізувати операції передачі та керування (край аналітики та обчислення). Його основна перевага полягає у зниженні складності систем IIoT, з тим щоб вони могли збільшуватись як у кількості керованих активів, так і в мережах. Однак він може не підходити для систем, де активи рухаються таким чином, що не дозволяє розташовувати стабільні кластери в межах локальної мережі [9].

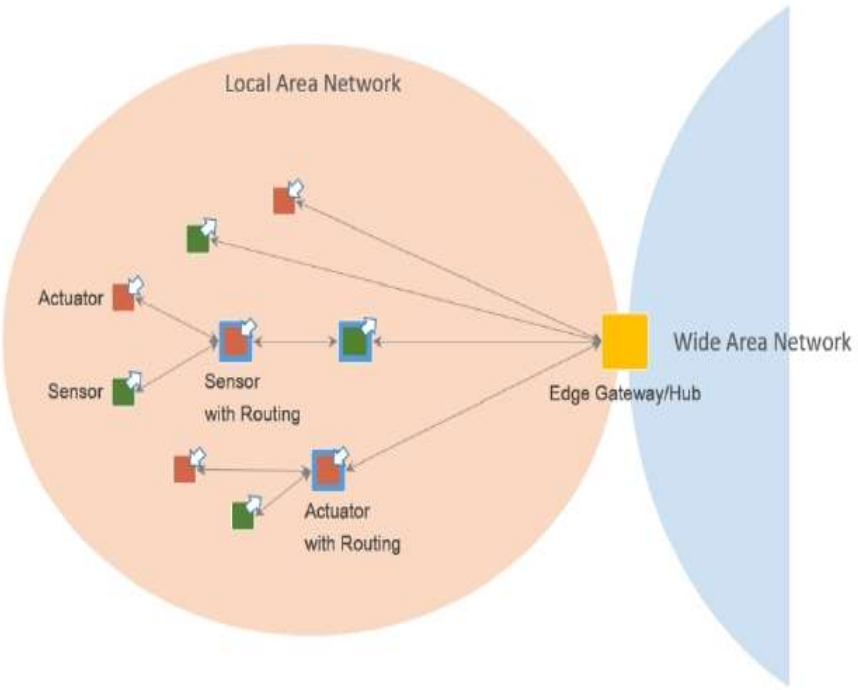


Рис. 3.7. З'єднання та управління за допомогою шлюзів

У топології *hub-and-spoke* граничний шлюз діє як концентратор для підключення кластера вузлів краю один до одного та до широкосмугової мережі. Він має прямий зв'язок з кожним об'єктом в кластері краю, що дозволяє приймати дані з кінцевих вузлів, а також керувати вузлами.

У мережевій сітці (або однорангової) топології краєвий шлюз також виступає як концентратор для підключення кластера вузлів краю до широкосмугової мережі. Проте в цій топології деякі верхні вузли мають можливість маршрутизації. Як результат, шляхи маршрутизації від вузла краю до іншого та до шлюзу змінюються і можуть змінюватися динамічно. Ця топологія використовується для забезпечення широкого покриття для програм з низькою потужністю та низькою швидкістю передачі даних на пристроях з обмеженим ресурсом, які географічно розподілені.

Багатошарова шина даних: багатошарова шина даних є загальною архітектурою в системах IIoT у кількох галузях промисловості (рис. 3.10. Шаблон з використанням багатошарової шини даних). Ця архітектура забезпечує низьку латентність, захищену однорангову передачу даних через логічні шари системи. Це найбільш корисно для систем, які повинні управляти прямими взаємодіями між додатками в областях, таких як контроль, локальний моніторинг та аналітика краю.

В даній архітектурі шлюз являється осередком зв'язку між речами та зовнішнім світом, він виступає в якості маршрутизатора та не має функцій зберігання даних, агрегації та аналітики.

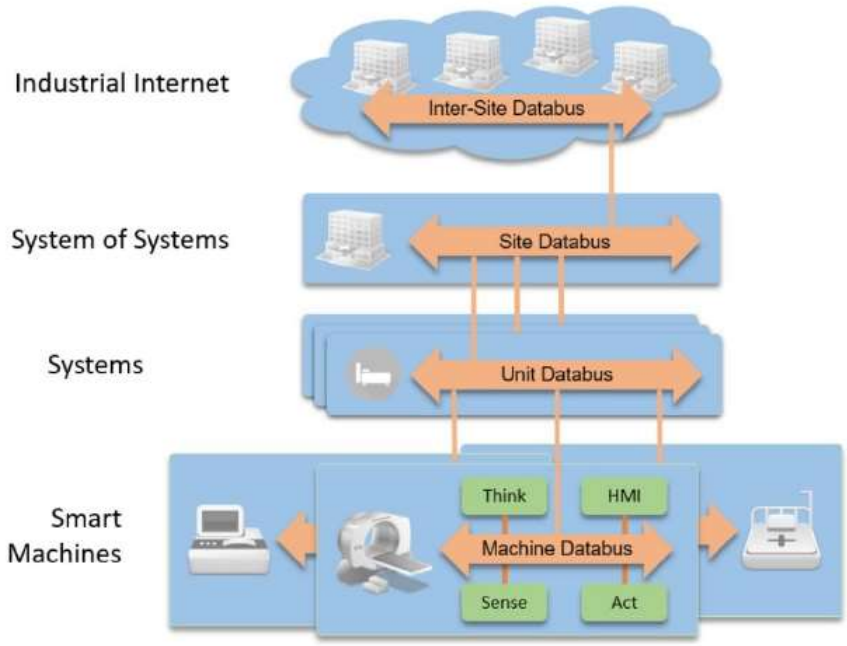


Рис. 3.8. Шаблон з використанням багатошарової шини даних

Контрольні питання до розділу

1. Які організації і стандартизаційні форуми працюють для розширення або адаптації протоколів Інтернету для пристроїв IoT?
2. Які переваги може надати архітектура IoT?
3. Наведіть приклади технологій, які використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження.
4. Дайте визначення поняттю «*Річ (Thing)*» еталонної моделі IoT від МСЕ-Т.
5. Дайте визначення поняттю «*Пристрій переносу даних (Data-carrying Device)*» еталонної моделі IoT від МСЕ-Т.
6. Дайте визначення поняттю «*Пристрій збору даних (Data-capturing Device)*» еталонної моделі IoT від МСЕ-Т.
7. Дайте визначення поняттю «*Носій даних (Data Carrier)*» еталонної моделі IoT від МСЕ-Т.
8. Дайте визначення поняттю «*Сенсорний пристрій (Sensing Device)*» еталонної моделі IoT від МСЕ-Т.
9. Дайте визначення поняттю «*Виконавчий пристрій (Actuating Device)*» еталонної моделі IoT від МСЕ-Т.
10. Дайте визначення поняттю «*Пристрій загального призначення (General Device)*» еталонної моделі IoT від МСЕ-Т.
11. Дайте визначення поняттю «*Шлюз (Gateway)*» еталонної моделі IoT від МСЕ-Т.
12. Еталонна модель IoT від МСЕ-Т. Особливості побудови.
13. Наведіть категорії вимоги до шлюзів еталонної моделі IoT від МСЕ-Т.
14. Які існують варіанти зв'язку пристроїв між собою в еталонній моделі IoT від МСЕ-Т.
15. Еталонна модель IoT від МСЕ-Т складається з декількох рівнів:
    a. *Мережевий рівень;*
    b. *Рівень мережі;*
    c. *Рівень остатку;*
    d. *Рівень додатку;*

e. *Рівень підтримки послуг і підтримки додатків;*
f. *Рівень якості обслуговування;*
g. *Рівень можливостей управління;*
h. *Рівень можливостей забезпечення безпеки.*

16. В Рекомендації Y.2060 як приклади загальних можливостей управління перераховані:
    a. *управління пристроями*:
    b. *управління топологією локальної мережі*;
    c. *управління топологією глобальної мережі*;
    d. *управління доступом до мережі;*
    e. *управління трафіком і перевантаженнями*;
    f. *управління сеансом встановлення зв'язку з пристроями*.

17. В Рекомендації Y.2060 приклади загальних можливостей забезпечення безпеки включають:
    a. *на рівні програми*: авторизацію, автентифікацію, захист конфіденційності і цілісності даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист;
    b. *на рівні мережі*: авторизацію, автентифікацію, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;
    c. *на рівні сервісів:* авторизацію, автентифікацію, конфіденційність даних про використання сервісу, управління сервісом;
    d. *на рівні пристрою*: автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.
18. Еталонна модель від Всесвітнього форуму IoT (IoT World Forum, IWF). Призначення. Особливості побудови.
19. Особливості роботи Рівня 1 еталонної моделі IWF.
20. Особливості роботи Рівня 2 еталонної моделі IWF.
21. Дайте визначення туманних обчислень. Особливості роботи Рівня 3 еталонної моделі IWF.
22. Особливості роботи Рівня 4 еталонної моделі IWF.
23. Особливості роботи Рівня 5 еталонної моделі IWF.
24. Особливості роботи Рівня 6 еталонної моделі IWF.
25. Особливості роботи Рівня 7 еталонної моделі IWF.
26. Проведіть порівняння туманних та хмарних обчислень.
27. Модель NIST Special Publication 800-183.
28. Які існують шаблони реалізації IIoT-системи в моделі *Industrial Internet of Things Reference Architecture.*
29. В референсній архітектурі моделі *Industrial Internet of Things Reference Architecture* представлено наступні шаблони реалізації IIoT-системи:
    a. *Рівень краю;*
    b. *Рівень доступу;*
    c. *Рівень платформи;*
    d. *Рівень шлюзу;*
    e. *Рівень підприємства.*
30. У топології *hub-and-spoke* моделі *Industrial Internet of Things Reference Architecture* граничний шлюз діє як:
    a. *Ретранслятор;*
    b. *Концентратор;*
    c. *Маршрутизатор;*
    d. *Комунікатор.*

Список рекомендованої літератури

1. Tripathy B. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. – Florida: CRC Press, 2017. – 334 с.
2. Sutaria, R., and Raghunath, G., “Making sense of interoperability: Protocols and Standardization initiatives in IoT,” International Conference on Recent Trends in Communication and Computer Networks – ComNet 2013, 2013.
3. Lake, D., Rayes, A., and Morrow, M., “The Internet of Things,” The Internet Protocol Journal, Volume 15, No. 3, September 2012.
4. ITU-T, “Overview of the Internet of Things,” Recommendation Y.2060, June 2012.
5. Ferguson, J., and Redish, A., “Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body,” Expert Review of Medical Devices, Volume 6, No. 4, 2011, http://www.expert-reviews.com.
6. ITU-T, “Common Requirements and Capabilities of a Gateway for Internet of Things Applications,” Recommendation Y.2067, June 2014.
7. Cisco Systems, “The Internet of Things Reference Model,” White Paper, 2014. http://www.iotwf.com/
8. Frahim, J., et al., “Securing the Internet of Things: A Proposed Framework,” Cisco White Paper, March 2015.
9. Модель NIST Special Publication 800-183 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
10. Модель Industrial Internet of Things Reference Architecture http://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf

РОЗДІЛ 4. IOT ПЛАТФОРМИ

4.1. Поняття IoT платформа

IoT-платформи об'єднують власне "речі" і "Інтернет". По суті - це ключовий інструмент розробки IoT-додатків і сервісів, що поєднує фізичні об'єкти і Мережу.

При цьому багато постачальників, які намагаються "тримати ніс за вітром", пропонують "IoT-платформи", які в корені відрізняються між собою. І в ряді випадків не є "платформою" в широкому сенсі слова, але абсолютно очевидно мають підстави себе такою вважати - є "річ", є якийсь ресурс в Інтернеті, який приймає / передає дані від / до "речі". І щось робить (намагається робити) з цими даними. Отже, претендувати на високе звання платформи цілком може. Притому, що чіткого і конкретного визначення IoT-платформи просто не існує.

На думку авторів "*IoT Analytics*", повноцінною IoT-платформою слід вважати таку платформу, яка дозволяє розробляти відповідні додатки / рішення (*IoT Application Enablement Platform*) [1].

А ось чотири типи платформ, які називають "IoT-платформами", проте вони не цілком підходять під класифікацію *IoT Analytics*:

- *Connectivity / M2M platforms*. Платформи в своїй роботі фокусуються на зв'язку розумних об'єктів через телекомунікаційні мережі, але рідко на обробці сигналів від датчиків (приклад такої платформи: *Sierra Wireless з продуктом AirVantage).*
- *IaaS backends.* Інфраструктура-як-сервіс-сервери, що надають хостінг-простір і обчислювальні потужності для додатків і сервісів, раніше оптимізували для десктопів і мобільних додатків, але зараз в фокус потрапив і IoT (приклад - *IBM Bluemix,* але не *IBM IoT Foundation*).
- *Hardware-specific software platforms.* Деякі компанії, що продають розумні гаджети, створюють власний програмний бекенд і міркують про нього, як про IoT-платформі. Але, так як ця платформа носить закритий для всіх інших характер, правомірність такого найменування сумнівна (наприклад - Google Nest).
- *Consumer / Enterprise software extensions.* Існуючі пакети корпоративного програмного забезпечення і операційні системи типу MS Windows 10 стають все більш відкритими для інтеграції IoT- пристроїв. В даний час ця область ще недостатньо розвинена, щоб називатися IoT-платформою, але майбутнє у неї дуже перспективне.

IoT Analytics виділили вісім компонентів повноцінної IoT-платформи:

- *Зв'язок і нормалізація (Connectivity & normalization):* зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями.
- *Управління пристроями (Device management):* забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень. Причому, не тільки ПО власне "речей", але і додатків, що працюють на пристрої або прикордонних шлюзах.
- *База даних (Database):* тут все досить зрозуміло і прозоро – сховище даних від "речей", що масштабується. Вимоги до цих даних, спроба навести порядок в обробці і перенесення даних з, наприклад, різних "платформ" або зовсім до інформаційних систем "третіх осіб".
- *Обробка та управління діями (Processing & action management):* дані, отримані від "речей" в кінцевому підсумку впливають на події в реальності. Отже "платформа" повинна вміти будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків.
- *Аналітика (Analytics):* дані від "речей" є цінними самі по собі. Тому існування комплексу засобів їх аналізу є обов'язковою вимогою до "платформи". Якщо сюди включити ще й кошти кластеризації даних і глибокого машинного навчання аж до прогнозуючої аналітики, то цінність "платформи" очевидно зростає.

- *Візуалізація (Visualization):* всю перераховану вище аналітику було б непогано показати таким чином, щоб людям було зрозуміло, приємно і красиво. Будувати графіки, моделі, просто візуалізувати те, що відбувається з "речами". Ну, і просто зручний інтерфейс [2].
- *Додаткові інструменти (Additional tools):* набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи. Бажано, щоб не дуже заглиблюватися в код і програмування.
- *Зовнішні інтерфейси (External interfaces):* інтеграція за допомогою платформи - одна з головних можливостей. Світ інтернет-розробки сьогодні не терпить замкнутих рішень. Завжди може знадобитися передача і обмін зі сторонніми системами. Тому справжня IoT- платформа повинна мати інтерфейси прикладного програмування (*API*), комплекти розробки програмного забезпечення (*SDK*) і шлюзи.

4.2. Платформа Linux Foundation

Організація *Linux Foundation* представила новий спільний проект *EdgeX Foundry*, націлений на розвиток відкритої платформи для спрощення створення рішень на базі IoT-пристроїв. Метою *EdgeX Foundry* є надання універсальної модульної платформи для забезпечення взаємодії між IoT-пристроями, додатками і сервісами, а також створення екосистеми з компаній-виробників, що випускають сумісні і взаємозамінні компоненти для Інтернету речей. Платформа не прив'язана до обладнання конкретних постачальників і операційним системам, і розвивається незалежної робочою групою, під егідою *Linux Foundation* [3].

Платформа дозволяє створювати шлюзи, які б поєднували наявні IoT- пристрої і збирають дані від різних датчиків. Крім організації взаємодії з пристроями, в цій платформі шлюз виконує завдання по первинній обробці, агрегування та аналізу інформації, виступаючи проміжною ланкою між мережею з IoT-пристроїв і локальних керуючим центром або хмарної інфраструктурою управління. На шлюзах також можуть виконуватися обробники, оформлені у вигляді мікросервісів. Взаємодія з *IoT* пристроями може бути організовано по дротову або бездротову мережу з використанням *TCP / IP-мереж* і специфічних (НЕ-IP) протоколів.

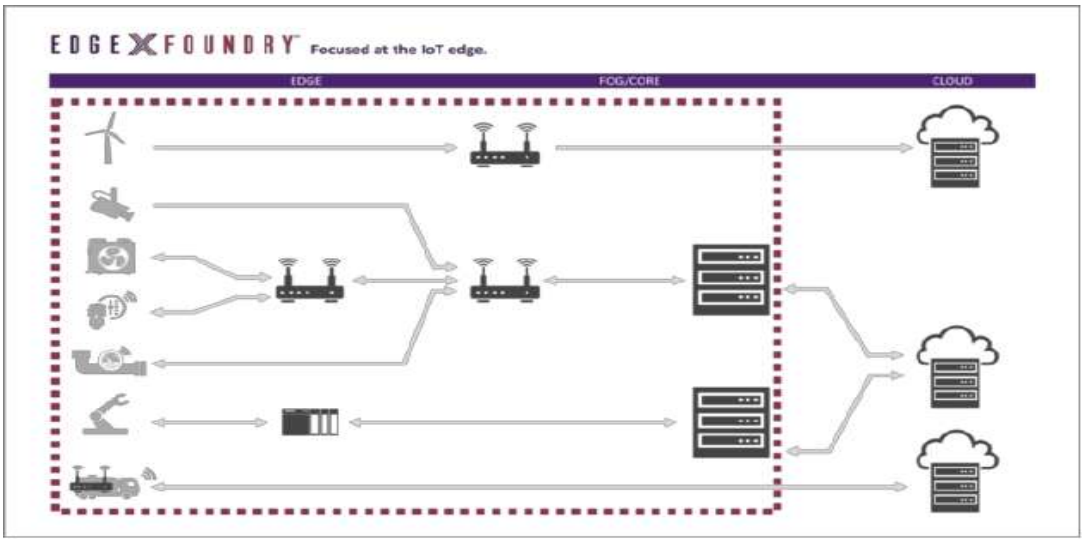


Рис. 4.1. Структура платформи Linux Foundation

Шлюзи різного призначення можуть об'єднуватися в ланцюжки, наприклад, шлюз першої ланки може вирішувати завдання з управління пристроями (system management) і забезпечення безпеки, а шлюз другої ланки (fog-сервер) зберігати дані, що надходять, виконувати аналітику і надавати сервіси (наступний слайд).

Система модульна, тому поділ функціональності на окремі вузли виконується в залежності від навантаження, в простих випадках достатньо одного шлюзу, а для великих IoT- мереж може бути розгорнутий цілий кластер [4].

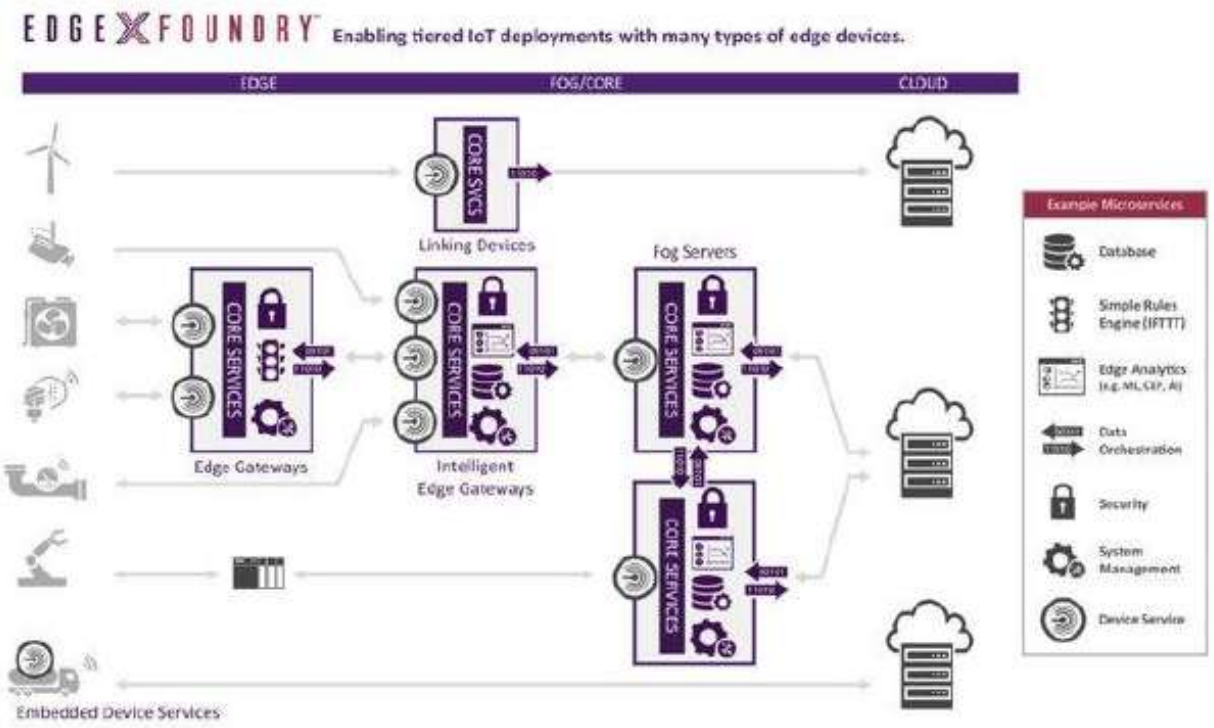


Рис. 4.2. Ланцюжки із шлюзів з різною функціональністю

В якості основи *EdgeX* виступає IoT-стек *Fuse*, який застосовується в шлюзах для IoT-пристроїв *Dell Edge Gateway*. Компанія *Dell* відкрила всі пов'язані з Fuse напрацювання під ліцензією *Apache 2.0* і передала права на проект під піклування *Linux Foundation*.

Консорціум *Linaro* увійшов в число учасників проекту і вважає, що *EdgeX* доповнює ініціативу *LITE (Linaro IoT and Embedded),* зосереджену на низькорівневих компонентах для IoT-пристроїв. Згадується також робота по інтеграції *EdgeX* з ОС реального часу *Zephyr*, що розвивається *Linux Foundation* для Інтернету речей.

Проект *EdgeX* налічує понад 125 тисяч рядків коду і включає в себе добірку готових мікросервісів для аналізу даних, забезпечення безпеки, управління і вирішення різних завдань. Платформа може бути встановлена на будь-яке обладнання, включаючи сервери на базі CPU x86 і ARM, що працюють під управлінням *Linux, Windows* або *MacOS*. Для розробки мікросервісів можуть використовуватися мови *Java, Javascript, Python, Go і C / C ++*. Для розробки драйверів для IoT-пристроїв і датчиків пропонується SDK [5].

Отже *EdgeX* не притримується рекомендацій, що зазначенні в моделях Всесвітнього форуму IoT та моделі від *MCE-T*. Ця платформа сильно розширює можливості шлюзу додаючи до можливості «перепакування» даних ще й функції туманних обчислень, таких як: первинної обробки даних та прийняття рішень в режимі реального часу (а не в часі транзакції при використанні хмарних сховищ), збереження, захист та аналіз даних.

Платформа має доволі широке поле застосування: безпека та спостереження, енерговиробництво, промисловість, розумний будинок, логістика. Для роботи с цією платформою найкраще підходять шлюзи від фірми *Dell*, адже вони використовують той самий стек *Fuse.*

4.3. Платформа AggreGate

AggreGate - це інтеграційна платформа для Інтернету речей, що пропонує швидке рішення п'яти головних завдань будь-якої IoT програми: отримання, зберігання, обробка, візуалізація даних та інтеграція з додатками рівня підприємства. На відміну від інших рішень, що надають базову інфраструктуру і комплекти розробника ПЗ для розробки вертикальних додатків, *AggreGate* пропонує не тільки інструменти візуальної розробки для побудови інтерфейсів кінцевих користувачів, а й ланцюжок обробки даних на сервері.

Незалежна від постачальника *M2M* платформа включає сотні драйверів пристроїв, що роблять можливим підключення будь-якого промислового або призначеного для користувача IoT пристрою. Крім застосування нормалізації даних на базі драйверів, *AggreGate* уможливлює отримання даних через зовнішні або вбудовані Агенти, конвертери протоколів пристроїв, що забезпечують буферизацію даних і підключення до серверів, оптимізовані для ненадійних стільникових і супутникових каналів з низькою пропускною здатністю [6].

AggreGate підлаштовує існуючі технології M2M, віддаленого моніторингу та обслуговування під новий світ *IoT*, що ґрунтується на відкритих стандартах, впровадженні хмарних додатків, засобах зберігання і обробки великих даних, багатому інтерфейсі користувача в браузері на базі HTML5 і інші тенденції. Це економить роки розробки і мільйонні інвестиції в розробку масштабованих і надійних рішень для Інтернету речей, інтегрованих в підприємство.

У той час як більшість вендорів IoT платформ пропонують інфраструктуру нижнього рівня для збору і зберігання даних, а також пропонують кінцевому користувачеві API і SDK для розробки додатків, IoT платформа *AggreGate* пропонує комплексне візуальне конфігурування, яке включає налаштування ланцюжків обробки даних, правил прийняття рішень, географічних карт, інструментальних панелей продуктивності, форм введення даних і навіть динамічних компонентів інтерфейсу без необхідності написання програмного коду.

Платформа AggreGate скорочує капітальні витрати і термін впровадження для виробників обладнання та системних інтеграторів, що створюють нові рішення для Інтернету речей. Вона являє собою міцну основу для підключення IoT пристроїв до додатків управління і веб-інтерфейсів кінцевого користувача [7].

Платформа гарантує високий показник повернення інвестицій для будь-яких IoT проектів, оскільки скорочує час простою системи і експлуатаційні витрати, підвищує ефективність і загальну задоволеність клієнтів.

Основними перевагами AggreGate є:

- *Широкі можливості підключення IoT пристроїв:* AggreGate підтримує великий набір комунікаційних протоколів, включаючи M2M / IoT, IT та протоколи автоматизації, а також такі загальні протоколи, як *SQL* і *SOAP*. Якщо операції запису і контролю підтримуються протоколом, *AggreGate* може їх використовувати.
- *Адаптована для M2M комунікацій:* Агенти встановлюють вихідні повідомлення з самим сервером. Це є ідеальним рішенням для стільникових і супутникових мереж, що не присвоюють білі статичні IP-адреси. Та ж технологія вирішує будь-які проблеми з брандмауерами і перетворенням мережевих адрес типових промислових мереж.
- *Єдина модель даних:* Єдина модель даних *AggreGate* надає загальний гнучкий підхід до конфігурації, контролю і моніторингу будь-яких пристроїв, джерел даних і системних об'єктів, незалежно від вендора, моделі, типу і цілі *Модульна, масштабована і надійна IoT архітектура:* Модульна архітектура хмарної IoT платформи AggreGate гарантує, що нові модулі зберігання, обробки і візуалізації даних можуть встановлюватися в ядро сервера як плагіни. Наприклад, додавання можливостей відстеження транспорту в існуючу M2M систему є справою звичайного встановлення пакета розширення.
- *Пакетна відкладена конфігурація пристроїв:* Не потрібно чекати, поки всі вони одночасно перейдуть у режим онлайн, достатньо внести зміни в конфігурацію і вони вступлять в силу в якомога більш стислі терміни.

- *Централізоване управління вбудованим ПО:* Централізоване оновлення вбудованого ПЗ та конфігурації вкрай важливо для будь-якої програми Інтернету речей. Ці оновлення можуть доставлятися пристроям користувача через центральний сервер за допомогою стандартних і приватних комунікаційних протоколів. Планування розподілу на нічні години не порушує роботу сервісів.
- *Дизайнер планів віддалених об'єктів:* Платформа для M2M додатків має вбудований візуальний редактор інтерфейсів. Це засіб побудови форм, графіків, звітів, таблиць, інтерфейсів і карт за допомогою миші. Не потрібно ніякого програмування навіть при побудові компонентів інтерфейсу з даними серверів / пристроїв.
- *Динамічні карти:* Відображають пристрої, групи, маршрути, геозони, з'єднання та інші об'єкти на географічних картах, що використовують будь-який ресурс, *наприклад Google Maps, Bing Maps, Open Street Map* та інші. Додайте до карт шари, елементи управління і вибору і візуально побудуйте будь операторський інтерфейс.
- *Зведені інструментальні панелі станів:* Візуалізують групи пристроїв і КПЕ (ключові показники ефективності) в масштабі системи на інструментальних панелях операторів верхнього рівня, що мають багаторівневу деталізовану навігацію по індивідуальних пристроях і сервісах. Звіти користувача запускаються за кілька кліків.
- *Безпечні зв'язки між пристроями:* Всі зв'язки між серверами і агентами можуть встановлюватися через безпечні SSL з'єднання і стискатися, щоб відповідати GPRS / 3G / LTE і супутниковим каналам. Агенти досить розумні, щоб при необхідності відправляти тільки важливі події замість необроблених значень метрик.
- *Зберігання великих даних в хмарі:* Незважаючи на те, що всі реляційні бази даних корпоративного рівня підтримуються як системи зберігання даних пристроїв, потоки подій зі світу Інтернету речей можуть направлятися в хмару великих даних. Інтегроване сховище типу NoSQL може працювати як всередині сервера, так і в якості окремого кластера зберігання, що складається з декількох вузлів.
- *Тривоги і обробка подій:* Гнучкі можливості керування пристроями, що включають фільтрацію, агрегування, маскування, кореляцію, підтвердження подій і аналіз першопричин. Настроюються тривоги, що підтримують різні типи тригерів, повідомлень (звукові, спливаючі повідомлення, e-mail, SMS і т.д.), ескалацію і коригувальні дії.
- *Графіки і тренди:* Підтримка графіків надає величезний список типів графіків, включаючи динамічно оновлюванні. Тисячі властивостей графіків, що налаштовуються.
  Підтримка ліній трендів, що автоматично розраховуються.
- *Докладні звіти:* Інструмент створення звітів з розширеними можливостями, автоматичне створення звітів на базі будь-яких даних. Вбудований редактор звітів, роздруківка та експорт звітів в різні формати.
- *Безкоштовний комплект розробника ПЗ:* можна використовувати API з відкритим вихідним кодом для Java, .NET, C / ++ і мобільних пристроїв з метою розширення можливостей рішення для Інтернету речей та інтегрувати IoT сервіси в будь-які інші корпоративні системи.
- *Гнучка модель безпеки:* З самого початку *AggreGate* розроблявся із застосуванням багатоклієнтського, розрахованого на багато користувачів підходу. Тонко налаштовуються права доступу і рольовий контроль доступу нерозривно вбудовані в усі аспекти системи.
- *Відмовостійка кластеризація:* Всі головні технології IoT покладаються на сервіси високої доступності, що забезпечуються багатовузловим ВІДМОВОСТІЙКИМ кластером. Два рівня кластерів гарантують захист сервера AggreGate і лежить в основі бази даних. Власна технологія кластеризації не залежить від стороннього ПЗ або підтримки кластеризації операційною системою.
- *Розподілена архітектура:* На відміну від багатьох M2M платформ, *AggreGate* масштабується до тисяч мікросерверів, що працюють на одноплатних комп'ютерах *Linux* на базі ARM, а також до мільйонів пристроїв в хмарі пристроїв. Унікальна

багаторівнева розподілена архітектура дозволяє встановити дійсно пірингові відносини між усіма вбудованими та звичайними серверами. Це гарантує необмежену масштабованість за допомогою балансування функціоналу системи між багатьма серверами, розділеними на кілька рівнів.

4.4. Платформа Everyware Cloud

Everyware Cloud (EC) від Eurotech є M2M / IoT-платформою, яка спрощує управління пристроями і збором даних шляхом підключення розподілених пристроїв через безпечні і надійні хмарні сервіси. Після того як пристрої будуть розгорнуті, *Everyware Cloud* дозволяє користувачам підключати пристрої, конфігурувати і управляти ними протягом всього життєвого циклу проекту.

Платформа *Everyware Cloud* може розгортатися як у публічній хмарі, так і в приватній. Для організації приватної хмари Eurotech пропонує спеціалізований *Everyware Server* - інтеграційну платформу M2M, розроблену для забезпечення додаткового рівня безпеки та конфіденційності за допомогою громадських хмарних технологій або без них, що охоплює всі можливості технології *Everyware Cloud*, виконану у вигляді надійного апаратного пристрою для забезпечення зручного і повного контролю в центрі обробки даних [8].

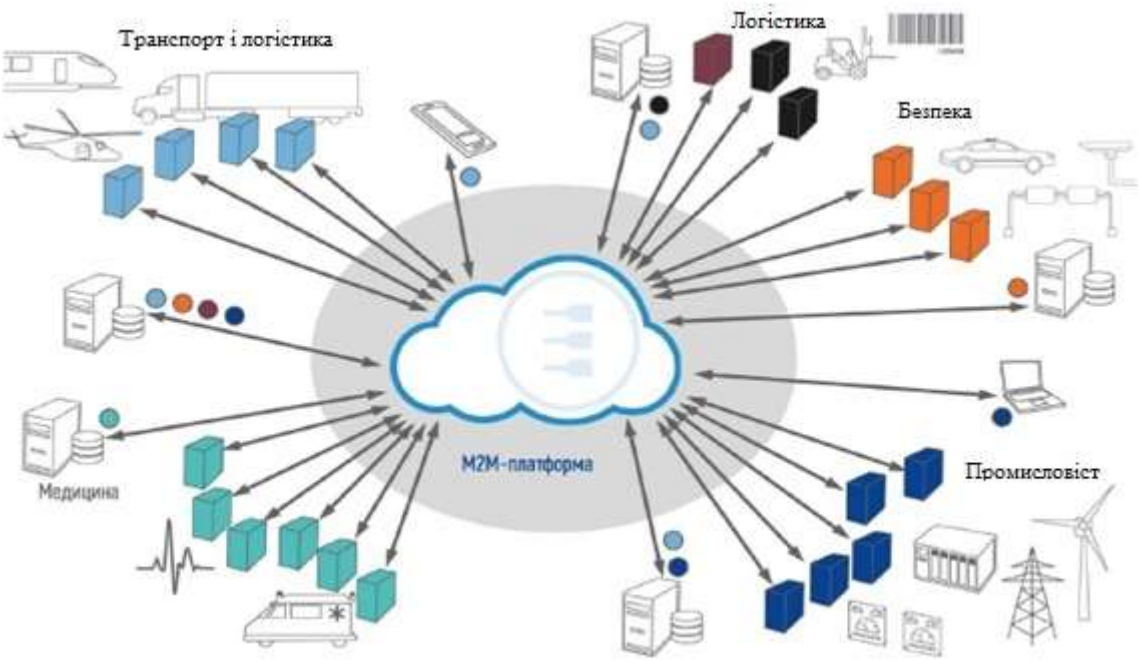


Рис. 4.3. Хмарна платформа Everyware Cloud

Everyware Server полегшує управління пристроями і даними при підключенні розподілених пристроїв до бізнес-додатків підприємства, з використанням безпечних і надійних протоколів зв'язку та обміну даними.

Everyware Cloud представляє собою програмну платформу, яка швидко з'єднує пристрої для створення і підтримки закінченого M2M-додатку. Вона забезпечує легкий шлях для підключення пристроїв до IT-систем і / або додатків.

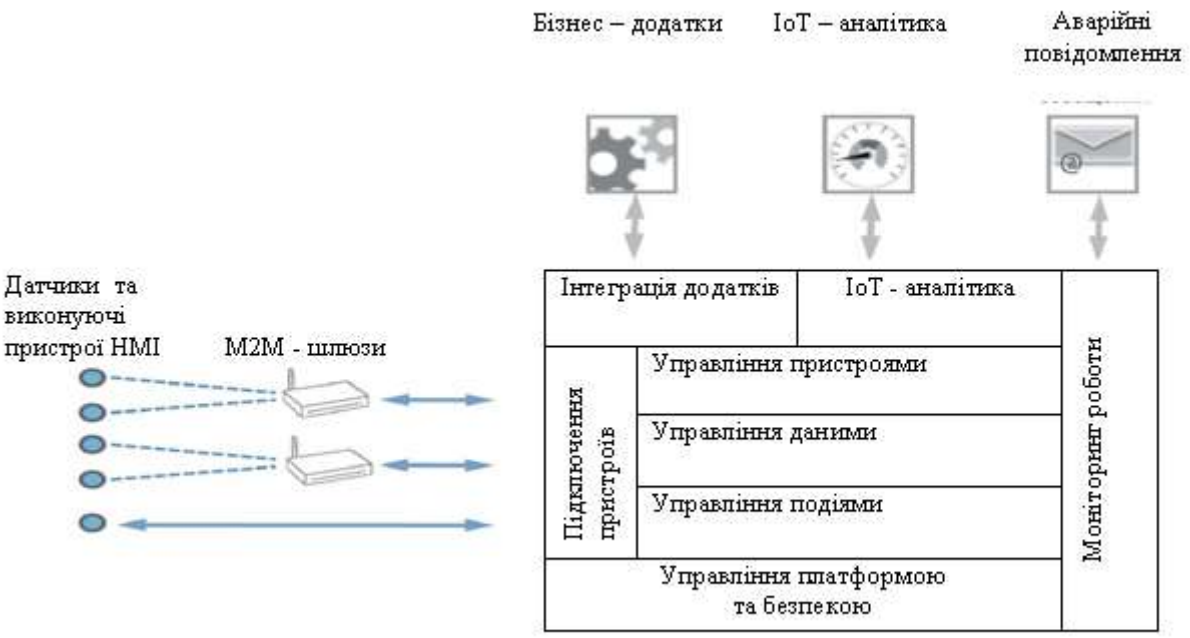


Рис. 4.4. Структура Everyware Cloud

Eurotech Everyware Device Cloud (EDC) - повністю закінчене рішення, яке містить спеціалізовані апаратні засоби, підключення і управління пристроями за допомогою *Eurotech Software Framework* і хмарні сервіси *Everyware Device Cloud Client* і *M2M* для обміну даними між польовими пристроями та бізнес-додатками підприємства [9].

IoT-платформа компанії Eurotech дає можливість спростити реалізацію складних проектів, дозволяючи отримати готове рішення швидше, ніж будь-коли раніше. Повна пропозиція включає:

- вбудовані комп'ютери і процесорні плати *Eurotech*, виконані на базі продуктивних процесорних платформ з низьким енергоспоживанням;
- операційну *систему Linux (Wind River, Yocto, Red Hat)* з повним набором інструментів для розробки і підтримки продуктів;
- програмний пакет *Everyware Software Framework (ESF)*, щоб спростити розробку додатків і підключення до мережі;
- хмарний клієнт *Everyware Device Cloud* для впровадження ефективних, надійних і захищених протоколів, що забезпечують дієвий зв'язок навіть в складних умовах;
- хмарний сервіс *Everyware Cloud* для миттєвого доступу до даних і управління пристроями через хмарні платформи.

Висновки

Отже IoT платформи об’єднують речі та Інтернет. Основними вимогами до IoT платформи за IoT Analytics є:

- Зв’язок і нормалізація,
- Управління пристроями,
- База даних,
- Обробка та управління діями,
- Аналітика,
- Візуалізація,
- Додаткові інструменти,
- Зовнішні інтерфейси.

Було розглянуто ряд платформ, як відкриті, так і комерційні проекти. Роль шлюзів варіюється від звичайних маршрутизаторів для перепакування даних для роботи в мережі Інтернет до міні серверів, що знаходяться на межі між речами та Інтернетом і виконують

функції агрегування та аналізу, реагують на певні події незалежно від хмари, тобто займаються туманними обчисленнями.

Контрольні питання до розділу

1. Особливості роботи платформи IoT *Connectivity / M2M platforms.*
2. Особливості роботи платформи IoT *IaaS backends.*
3. Особливості роботи платформи IoT *Hardware-specific software platforms.*
4. Особливості роботи платформи IoT *Consumer / Enterprise software extensions.*
5. Які компоненти повноцінної IoT-платформи виділяє *IoT Analytics.*
6. Компонента *«Зв'язок і нормалізація (Connectivity & normalization»)* повноцінної IoT-платформи за версією *IoT Analytics:*
   a) забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень;
   b) зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями;
   c) сховище даних від "речей", що масштабується;
   d) вміння будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків;
   e) інтеграція за допомогою платформи, передача і обмін зі сторонніми системами;
   f) набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи.
7. Компонента «*Управління пристроями (Device management)*» повноцінної IoT-платформи за версією *IoT Analytics:*
   a) забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень;
   b) зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями;
   c) сховище даних від "речей", що масштабується;
   d) вміння будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків;
   e) інтеграція за допомогою платформи, передача і обмін зі сторонніми системами;
   f) набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи.
8. Компонента *«База даних (Database)*» повноцінної IoT-платформи за версією *IoT Analytics:*
   a. забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень;
   b. зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями;
   c. сховище даних від "речей", що масштабується;
   d. вміння будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків;
   e. інтеграція за допомогою платформи, передача і обмін зі сторонніми системами;
   f. набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи.
9. Компонента *«Обробка та управління діями (Processing & action management)»* повноцінної IoT-платформи за версією *IoT Analytics:*
   a. забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень;

b. *зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями;*
c. *сховище даних від "речей", що масштабується;*
d. *вміння будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків;*
e. *інтеграція за допомогою платформи, передача і обмін зі сторонніми системами;*
f. *набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи.*

10. Компонента *«Додаткові інструменти (Additional tools)»* повноцінної IoT-платформи за версією *IoT Analytics:*
    a. *забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень;*
    b. *зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями;*
    c. *сховище даних від "речей", що масштабується;*
    d. *вміння будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків;*
    e. *інтеграція за допомогою платформи, передача і обмін зі сторонніми системами;*
    f. *набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи.*
11. Компонента *«Зовнішні інтерфейси (External interfaces)»* повноцінної IoT-платформи за версією *IoT Analytics:*
    a. *забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень;*
    b. *зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями;*
    c. *сховище даних від "речей", що масштабується;*
    d. *вміння будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків;*
    e. *інтеграція за допомогою платформи, передача і обмін зі сторонніми системами;*
    f. *набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи.*
12. Платформа Linux Foundation. Структура. Особливості.
13. Платформа AggreGate.
14. Основними перевагами AggreGate є:
    a. *Широкі можливості підключення IoT пристроїв.*
    b. *Адаптована для P2M комунікацій.*
    c. *Єдина модель даних.*
    d. *Модульна, масштабована і надійна IoT архітектура.*
    e. *Пакетна потокова конфігурація пристроїв.*
    f. *Децентралізоване управління вбудованим ПО.*
    g. *Зведені інструментальні панелі станів.*
    h. *Безпечні зв'язки між пристроями.*
    i. *Зберігання великих даних в хмарі.*
15. Основними перевагами AggreGate є:
    a) *Тривоги і обробка подій.*
    b) *Трафіки і бренди.*
    c) *Докладні звіти.*

d) Коштовний комплект розробника ПЗ.

e) Гнучка модель безпеки.

f) Відмовостійка кластеризація.

g) Розподілена архітектура.

16. Платформа Everyware Cloud. Структура. Особливості.
17. IoT-платформа компанії Eurotech дає можливість спростити реалізацію складних проектів, дозволяючи отримати повну пропозицію, що включає:

a) вбудовані комп'ютери і процесорні плати Eurotech, виконані на базі продуктивних процесорних платформ з високим енергоспоживанням;

b) операційну систему Linux (Wind River, Yocto, Red Hat) з повним набором інструментів для розробки і підтримки продуктів;

c) програмний пакет Everyware Software Framework (ESF), щоб спростити розробку додатків і підключення до мережі;

d) туманний клієнт Everyware Device Cloud для впровадження ефективних, надійних і захищених протоколів, що забезпечують дієвий зв'язок навіть в складних умовах;

e) хмарний сервіс Everyware Cloud для миттєвого доступу до даних і управління пристроями через хмарні платформи.

Список рекомендованої літератури

1. Tripathy B. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. – Florida: CRC Press, 2017. – 334 с.
2. Sutaria, R., and Raghunath, G., “Making sense of interoperability: Protocols and Standardization initiatives in IoT,” International Conference on Recent Trends in Communication and Computer Networks – ComNet 2013, 2013.
3. Lake, D., Rayes, A., and Morrow, M., “The Internet of Things,” The Internet Protocol Journal, Volume 15, No. 3, September 2012.
4. ITU-T, “Overview of the Internet of Things,” Recommendation Y.2060, June 2012.
5. Ferguson, J., and Redish, A., “Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body,” Expert Review of Medical Devices, Volume 6, No. 4, 2011, http://www.expert-reviews.com.
6. ITU-T, “Common Requirements and Capabilities of a Gateway for Internet of Things Applications,” Recommendation Y.2067, June 2014.
7. Linux Foundation розвиває EdgeX, нову платформу для Інтернету речей. (25 квітня 2017). Посилання https://www.opennet.ru/opennews/art.shtml?num=46446
8. Frahim, J., et al., “Securing the Internet of Things: A Proposed Framework,” Cisco White Paper, March 2015.
9. Хмарні технології в автоматизації.: комплексний підхід від Eurotech. Олексій П’ятницьких. (2016, Жовтень). Control Engineering, Росія. Посилання http://controleng.ru/wp-content/uploads/CE_IoT_Listalka.pdf

РОЗДІЛ 5. IoT ШЛЮЗИ

Узагальнюючи аналіз еталонних моделей IoT можна виділити перелік наведених нижче функцій шлюзів і характеристик шлюзів. Важливо підкреслити, що сьогодні переважна більшість виробників, особливо у старших моделях своїх шлюзів, забезпечують можливості як первинної обробки даних, до якої зазвичай відносять обробку подій і прийняття рішень в режимі реального часу, нормалізацію і фільтрацію даних для подальшої передачі на хмарний сервер, так і повноцінну аналітику зі зберіганням і візуалізацією даних.

Основними критеріями при виборі шлюзу для Інтернету речей можна назвати:

– **Підтримка периферійних/туманних обчислень**

В цьому випадку у якості критеріїв вибору слід звернути увагу на наступне:

- Підтримка шлюзом надійної спеціалізованої ОС (наприклад, від Wind River, Cisco, Microsoft).
- Наявність у фірми розробника шлюзу готових додатків для обробки даних, якість і можливості цих додатків, а також можливість підтримки їх даною моделлю шлюзу.
- Наявність у фірми розробника платформ для розробки замовником власного додатку зі зручними інтерфейси прикладного програмування (API) та комплектами розробки ПЗ.
- Можливості вибору ОС, мов та засобів програмування для реалізації власного додатка забезпечують адаптацію до потреб проекту.

Підтримуванні технології обміну даними

Підтримка необхідних технологій доступу до пристроїв для обміну даними між ними та з корпоративними або хмарними додатками IoT. Тут відображуються можливості збору даних з різних джерел, їх інтеграції, уніфікації представлення протоколів і форматів даних. В даному пункті слід звернути увагу на наступне:

– Максимальна кількість пристроїв, з якими може взаємодіяти шлюз:

- Перелік інтерфейсів з пристроями, в який можуть входити як сучасні протоколи проводових і безпроводових мереж (*Ethernet, Wi-Fi, Zigbee, 6LoWPAN, Bluetooth Low Energy* та ін.), так і успадковані протоколи (*BACNet, Modbus і CANbus* та ін.).
- Перелік інтерфейсів зовнішнім сервером додатків, в який можуть входити протоколи проводових і безпроводових мереж: *Ethernet, Wi-Fi*, протоколи стільникового зв'язку та ін.
- Підтримка *GPS* разом із стільниковим зв'язком забезпечить ефективну роботи з мобільними об’єктами з географічною прив'язкою, наприклад, транспортом.
- Наявність хорошого інтерфейсного профілю, заснованого на реалізації універсального само налаштування (*UPnP, Universal Plug and Play*), що визначає протокол для взаємодії з різними пристроями.

Функції маршрутизатора

Оскільки шлюз є вузлом стандартної *IP* мережі при взаємодії з сервером, то він зобов'язаний підтримувати мінімальні функції маршрутизатора.

У той же час ряд виробників (наприклад, *Cisco, Intel, Huawei*), позиціонують ряд моделей своїх шлюзів як повноцінні багато портові маршрутизатори. В цьому випадку можна виділити наступні можливості:

- Підтримка маршрутизації між декількома проводовими чи *Wi-Fi* локальними *IoT* мережами.
- Підтримка поширених функції *IP* маршрутизаторів – протоколів маршрутизації, *DHCP*, таблиць доступу, міжмережевих екранів і т.д.

Функції управління кінцевими пристроями мережею і додатками

- Управління пристроями включає можливості їх виявлення і автентифікації, конфігурацію, діагностику, оновлення прошивки і/або ПЗ, управління робочим статусом пристрою.

- Управління мережею включає можливості управління її моніторингом і конфігурацією, виявлення і керування перевантаженнями, керування трафіком, вимогами QoS.
- Управління додатками включає можливості керування їх встановленням і видаленням, виконанням оновлень, резервним копіюванням, від слідковуванням і усуненням несправностей.

Функції безпеки пристроїв, мережі і додатків

Як підкреслюється усіма без винятку авторами, наступні функції для IoT є життєво важливими.

- Захист на рівні ПЗ включає авторизацію, автентифікацію, конфіденційність і цілісність даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист.
- Захист на рівні мережі включає авторизацію, автентифікацію, конфіденційність даних, конфіденційність і цілісність даних сигналізації.
- Захист на рівні пристрою включає автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

Функції управління і безпеки всі крупні вендори забезпечують засобами власних платформ, власних ОС таких як *Wind River Linux, Windows 10 IoT, Cisco IOS*, додатковими апаратними засобами (*Dell, Cisco*), власними пакетами ПЗ, а також підтримкою стандартних рішень і сертифікованих рішень від сторонніх компаній.

У рамках подібної функціональності шлюзи можуть відрізнятися такими технічними характеристиками, серед яких можна виділити наступні:

- Обчислювальна потужність, об'ємами пам'яті і її типами, що важно врахувати при плануванні реалізації на шлюзі додатків.
- Форм фактор – компактність і форма конструктивного виконання, що важливо враховувати при плануванні місця розташування шлюзу.
- Умови експлуатації. Одні пристрої придатні лише для роботи у звичайних приміщеннях, інші - розраховані на роботу в широкому діапазоні температур, в умовах підвищеної вологості, запиленості.

Слід також звернути увагу на те, ринок послуг та пристроїв IoT зазвичай поділяють на два великі сегменти: *промисловий* і *споживчий* та сегмент, які відрізняються вимогами до ціни, надійності, безпеки, потужності, масштабованості. У цих рамках вендори можуть надавати як універсальні пристрої так і пристрої для конкретних вертикалей ринку в складі комплексних рішень.

Більшість виробників орієнтуються на промисловий ринок, хоча молодші моделі їх рішень, наприклад, Intel цілком підходять для простих економних рішень. А продукція таких компаній як Google чи Samsung в першу чергу орієнтована на споживчий ринок. Визначивши основні параметри, котрі повинен задовольняти шлюз можна провести огляд пропозицій від лідерів ринку IoT, а також від декількох компаній, що вийшли на ринок недавно. Перелік 15 перших вендорів з традиційного списку CRN/США «IoT 50» за 2017 рік можна знайти у [1].

5.1.Шлюзи компанії Eurotech

Компанія *Eurotech* в першу чергу відома своєю хмарної IoT платформою *Everyware*, яка покликана спростити адміністрування пристроїв і керування даними, забезпечуючи підключення розподілених пристроїв через захищені хмарні сервіси. Використовуючи цю платформу, замовники можуть відслідковувати, конфігурувати свої пристрої і керувати ними протягом всього життєвого циклу.

Практично всі шлюзи компанії *Eurotech* призначені для промислового застосування та експлуатації в жорстких умовах. Також компанія пропонує рішення, в тому числі шлюзи, для таких вертикалей ринку як транспорт і роздрібна торгівля.

Всі шлюзи мають досить великий набір інтерфейсів вводу/виводу і польових шин, а також необхідний набір проводових і безпроводових (бездротових) мережевих інтерфейсів

для організації надійного зв'язку: *Fast або Gigabit Ethernet*, стільниковий зв'язок, *Wi-Fi, Bluetooth, ZigBee.*

Для підключення шлюзів до локальних хмарних сервісів можна використовувати *Ethernet* або *Wi-Fi*, а до віддалених - технології стільникових мереж. Завдяки підтримці стільникового зв'язку з *GPS* більшу частину шлюзів можна використовувати для геолокації об'єктів, що переміщаються.

Широка лінійка шлюзів містить як компактні пристрої з низьким енергоспоживанням, так і високопродуктивні вбудовані ПК з широким функціональним набором.

Пристрої серій *ReliaGATE 10-20, ReliaGATE 10-11 і ReliaGATE 10-05* можуть служити малопотужним шлюзом для легких промислових застосувань. Їх основні функції - агрегування даних, одержуваних з польових пристроїв, перетворення повідомлень і протоколів, маршрутизація пакетів, організація двобічного зв'язку з хмарним сервером, де дані збираються, зберігаються і обробляються за допомогою бізнес-додатків [1].

Шлюзи серій *ReliaGATE 20-25, ReliaGATE 20-26, DynaGATE 15-10* пропонують додаткові можливості по обробці і зберіганню даних для надання послуг в автономному режимі, а при підключенні до хмарних додатків забезпечують контроль і управління в реальному часі. Вони часто застосовуються для виконання аналітичних функцій або завдань попередньої обробки, зокрема для передачі даних, що відповідають заданим параметрам.

Практично всі шлюзи, крім ReliaGATE 20-26, який використовує *Red Hat Linux*, поставляються з попередньо встановленою операційною системою *Yocto Linux*. Велика частина шлюзів забезпечується програмним забезпеченням *Everyware Software Framework (ESF)* на базі *Eclipse Kura і Java/OSGi*. Крім того, в якості шлюзів можуть виступати і процесорні плати в різних форм-факторах, на які також встановлюється спеціалізоване програмне рішення.

ESF - це промислова версія *Eclipse Kura* (версія з відкритим вихідним кодом) з додатковими можливостями з безпеки, діагностики, конфігурації і віддаленого доступу, повністю інтегрована в платформу *Everyware Cloud*. *ESF/Kura* дозволяє розробникам зосередити свою увагу на аналітиці та специфіці додатків і полегшити контроль і управління роботою шлюзу (змінювати параметри в реальному часі, оновлювати ПЗ, робити моніторинг пристрою, діагностику, забезпечувати безпеку і т. д.) [2].

5.2.Шлюзи компанії Intel

Шлюзи *Intel* для *IoT* дуже різноманітні і здатні задовольнити розробників проектів будь-якої складності. Їх оснащують процесорами *Quark, Atom, Core, Xeon.*

Шлюзи на базі *Intel Quark*, засновані на платі *Intel Galileo*, є гнучким, малопотужним і недорогим рішенням для організації нескладних обчислень іінтеграції пристроїв IoT. Процесори *Intel Atom* і *Intel Core* останніх поколінь забезпечують більш високу продуктивність, хорошу графіку і багату інтеграцію введення-виведення.

Сімейство *Intel Xeon* допомагає створювати шлюзи для інфраструктури з обчисленнями в пам'яті, аналізу в режимі реального часу, підвищеною оперативністю і безпекою. Шлюзи оснащують сховищами даних і оперативною пам'яттю, які відповідають вимогам процесора і призначень пристроїв.

Шлюзи технології *Intel IoT Gateway* випускаються більш ніж десятком фірм.

Вони забезпечуються засобами для створення власних додатків первинної обробки даних, збору даних з безлічі пристроїв, функціями перетворення протоколів і керування різними пристроями. Шлюзи *Intel* для IoT можуть підтримувати різні операційні системи, включаючи *Windows 10 IoT* і кілька мов програмування.

Більшість моделей поставляється з встановленою ОС Wind River Linux, в якій передбачений захист пристроїв від внутрішнього або зовнішнього несанкціонованого доступу. При цьому, в області захисту даних, тут є шифрування і безпечний обмін інформацією з зовнішніми системами.

У *Wind River Linux* в систему вбудовано керуюче ПО, яке дозволяє управляти не тільки локальними, але і віддаленими пристроями. Контролювати їх можна або вручну, або в

автоматичному режимі, ґрунтуючись на критеріях, заданих адміністраторами і програмістами. Крім того, підтримка платформ *Wind River Helix Device Cloud і Wind River Helix App Cloud,* дають великі можливості по управлінню пристроями, додатками і хмарними сервісами.

Шлюзи Intel володіють великими мережевими можливостями. Вони можуть підключатися відразу до двох локальних дротових мереж, одночасно працювати в декількох Wi-Fi-мережах, і, не переривaючи зв'язок, взаємодіяти зі спеціалізованими пристроями, використовуючи інші типи мереж.

Різноманітність підтримуваних мережевих інтерфейсів дозволяє рішенням для *IoT* створювати мережі на базі технологій *Bluetooth, ZigBee, 6LoWPAN* і ін., підключатися до хмарних сервісів, організовувати різні схеми управління. У список підтримуваних мережевих інтерфейсів входять і мобільні мережі: *GPRS, 2G, 3G. LTE* [3].

5.3. Шлюзи компанії Huawei

У компанії *Huawei* є цілий спектр продуктів, який формує середовище передачі, зберігання і обробки даних IoT за допомогою різних аналітичних систем.

Складовими платформи для зберігання і обробки великих даних є *Huawei FusionStorage* і *FusionInsight*.

Шлюзи серії *AR* від *Huawei* працюють як високопродуктивні маршрутизатори IoT, і особливо підходять для відеоспостереження, виробництва, транспортування, електропостачання та інших зовнішніх операцій. Лінійка дуже різноманітна и може задовольнити будь-які потреби як у плані обчислювальної здатності, так і у вимогах до різноманітних інтерфейсів підключення. Легкість зв'язку із речами та шлюзами забезпечується платформою *IoT Connection Management Platform.*

У лінійки в наявності є безліч типів інтерфейсів, які підходять до різноманітних терміналів. Шлюзи підтримують різні протоколи бездротового зв'язку: *Wi-Fi, ZigBee, Bluetooth* та *RF*. Також наявна підтримка сотового зв'язку у мережах *GSM, 3G* та *4G/LTE*, що разом із підтримкою *GPS* робить шлюз працездатним при перегонах транспорту. Маршрутизація трафіку може бути гнучко налаштована політикою маршрутизацій, статичними маршрутами та підтримкою динамічних протоколів *RIP, OSPF, IS-IS, BGP*. Підтримується перетворення різних галузевих протоколів та побудова єдиної мережевої платформи.

Більша частина шлюзів лінійки зроблена відповідно до вимог промисловості, тому витримує роботу у екстремальних умовах, таких яких велика кількість пилу в повітрі, вологість і т.д. Відтак шлюзи можуть працювати при температурах від -40 °С до +70 °С при відносній вологості від 5 до 95 %. При чому певним пристроям, наприклад AR550E, навіть не потрібен вбудований вентилятор для охолодження.

Шлюзи виконані відповідно до вимог стандарту IEEE 1613 і нормально функціонують навіть в умовах великих електромагнітних перешкод. Відповідність до стандартів віброзахисту надає право шлюзам компанії *Huawei* повноцінно працювати у сфері транспортування товарів.

У лінійці використанні високопродуктивні *ARM* процесори, що доповнюються великими об'ємами постійної пам'яті, в якості операційної системи використовується *Wind River LINUX*. Підтримка віртуалізації і можливість гнучкої масштабованої інтеграції додатків прискорюють розгортання послуг. Платформа надає управління повним життєвим циклом *ІКТ*-ресурсів: розгортання, моніторинг видалення додатків через *Agile Controller*.

Платформа від *Huawei* надає зручне та об'єднане управління терміналами, шлюзами, програмами та даними. Запуск розгортання можна запустити всього лиш відсканувавши серійний номер пристрою (*ESN*). Це дозволяє дуже швидко вводити пристрої у експлуатацію. Завдяки уніфікованій системі керування мережею (*NMS*), пристрої можна об'єднувати в певні групи та масово ними керувати. Є можливість встановлення ПЗ із *USB*-накопичувача та майже моментальний початок користування завдяки функції «*plug-and-play*».

Для керування через Ethernet та розширених операцій *Smart Grid*, найкраще підходять *AR2500 Agile Gateways*, тоді як *AR502 Gateways* ідеально підходять для роботи в умовах екстремальних температур, високої вологості та електромагнітних перешкод. Для мережевої інтеграції та обміну через віртуалізацію корисні шлюзи *AR3600* (з дизайном x86). Модель *AR510* є потужним шлюзом для мультимедійних і відеосервісів у різних приміщеннях та на відкритому повітрі (включаючи "зв'язані автомобілі").

Безпека підтримується міжмережевим екраном із поділом на зони та відстеженням стану, автентифікацією на основі 802.1X та автентифікацією по MAC-адресі та веб-автентифікація. Наявний захист ARP і захист від атак *ICMP*.

Додаткова безпека досягається завдяки відстеженню пакетів *DHCP* і відстеженню пакетів *DHCPv6 CPCAR*, чорному списку і відстеженню джерела атаки *PKI* і *KPM* [4].

5.4. Шлюзи компанії Cisco

Зокрема, компанія пропонує шлюзи, комутатори промислового класу і вбудовуються маршрутизатори для *IoT* з підтримкою платформи туманних обчислень *IOx*. *IOx* - це середа для додатків, яка допомагає мережевим пристроям, які її підтримують, контролювати і управляти пристроями IoT. Ця середа поєднує в собі найпопулярнішу відкриту *ОС Linux*, мережеву *ОС Cisco IOS* та потужні сервіси для швидкої та надійної інтеграції із сенсорами *IoT*, що дозволяє клієнтам створювати і запускати програми безпосередньо на промислових мережевих пристроях *Cisco*. Компанія *Cisco* створює та підтримує відкрите середовище для заохочення розробників переносити існуючі програми та створювати нові в різних галузях промисловості.

Компанія Cisco створює шлюзи для різноманітних вертикалей ринку: промисловість, енергозабезпечення, транспорт та логістика, розумні міста, навчання, охорона здоров'я та ін.

Також існує лінійка безпровідних шлюзів для мереж пристроїв *LoRaWAN*, що складається зі шлюзів *IXM-LPWA-800-16-K9* (підтримує частоти 863–870 МГц) та *IXM-LPWA-900-16-K9* (підтримує частоти 902–928 МГц). Цей тип зв'язку забезпечує M2M взаємодію на відстанях до 15 км при мінімальному енергоспоживанні, що забезпечує декілька років автономної роботи на одному акумуляторі AA. Вони підтримують до 16 каналів LoRa та захищені по стандарту *IP67.* Ці шлюзи вкрай зручні при використанні на рухомих об'єктах в автономному режимі роботи, а за рахунок волого- та пилозахищеності не потребують додаткових захисних коробів.

Широкий вибір маршрутизаторів у промисловому виконанні забезпечує функціональні можливості корпоративного класу, включаючи високоякісну передачу даних, можливості голосового та відео зв'язку зі стаціонарними і мобільними вузлами мережі через дротові та бездротові канали зв'язку.

Маршрутизатори *Cisco* надають доступну функціональність, що необхідна при створенні корпоративних рішень:

- динамічний багатоточковий *VPN (DMVPN);*
- аналіз якості обслуговування (*QoS*) для стільникового зв'язку;
- мульти-віртуальна переадресація маршрутів (*VRF*) для стільникового зв'язку;
- *Cisco IOx* для маршрутизаторів 809 і 829, що забезпечує виконання граничного додатків в мережах *IoT* Основною лінійкою IoT шлюзів від *Cisco* є *Cisco 800*, які позиціонуються як маршрутизатори промислової інтегральної мережі. На шлюзах Cisco встановлена операційна система *Cisco IOS*, що забезпечує просте управління, дає змогу створювати еластичні комунікації та підтримувати високий рівень безпеки.

Всі маршрутизатори серії 800 мають інтегроване *4G/LTE* бездротове з'єднання *WAN* та підтримують більш старі версії стільникового зв'язку. Дві зовнішні антени забезпечать максимально якісний зв'язок, а дві різні, одночасно активні, *SIM* карти допоможуть підтримувати зв'язок різних операторів в залежності від якості сигналу.

Маршрутизатор 829 також забезпечує високоякісні з'єднання бездротової локальної мережі *Wi-Fi*, підтримуючи 2.4ГГц та 5ГГц діапазони. Також у наявності вбудований 2x2

MIMO, що забезпечує швидкість з'єднання до 300 Мб/сек. Доступні й стандартні *Ethernet* порти, що підтримують також і *PoE/PoE+* з передачею потужності до 30 Вт.

Для забезпечення роботи в умовах виробництва шлюзи підтримують розширений діапазон температур від -40 º С до 60 º С. Дл я безперешкодної інтеграції із системами SCADA підтримуються протоколи DNP3, DNP3 IP та IEC від T101 до T104. Багатогалузева сертифікація шлюзів Cisco надає їм перевагу у корпоративних рішеннях, де велика увага приділяється надійності постачальника [5].

Стратегія *Cisco* в області *IoT* будується на шести стовпах технології: рішення з передачі даних в *IoT*-мережі, прикладна середу *IOx* і *fog*-додатки, а також *IT*- безпека, аналітика даних, засоби автоматизації та підтримка додатків. Саме *Cisco* ввів поняття туманних обчислень та Інтернету всього (*IoE, Internet of Everything*).

5.5.Шлюзи компанії NEXCOM

Серія *NEXCOM CPS* складається зі шлюзів *IoT*, готових до застосування, які легко встановлювати та налаштовувати. Заздалегідь встановлена за допомогою *NEXCOM Industrial IoT Studio* допоможе полегшити розробку додаткового ПЗ. У лінійки наявна широка підтримка різноманітних операційних систем. Відтак на шлюзи можуть бути встановленні *Windows 10 IoT, Ubuntu 14.04, FreeRTOS* та інші *Linux* системи.

Встановлені процесори *Intel Atom* надають достатню потужність для обробки даних на краю при цьому мають гарну енергоефективність. Для більш потужних обчислень можна обрати моделі із використанням повноцінних та більш енергоємних процесорів *Intel Celeron*. Вид жорсткого диску та його об'єм варіюється від 16 ГБ e-MMC до 128 ГБ SSD із підтримкою порту розширення SD карткою.

Серія CPS може витягувати та аналізувати дані PROFIBUS, PROFINET та Ethernet, надсилати попереджувальні повідомлення, зберігати дані в локальні та віддалені бази даних та виконувати інші функції обробки даних після декількох кліків мишею. Серія CPS також підтримує API хмарних інтерфейсів для підключення до хмарних серверів через бездротові 3G/Wi-Fi (додатковий модуль) та/або дротові локальні мережі. За допомогою серії CPS виробники можуть изначати потоки даних, завантажувати дані з кінцевих пристроїв у платформи хмарної служби, включаючи Microsoft Azure та IBM Bluemix.

Завдяки надійному дизайну, серія CPS може бути встановлена поряд з PLC, датчиками та пристроями вводу-виводу в жорстких середовищах. На зосередженість у сфері промисловості та транспорту вказує захист від вібрацій та ударів, а також можливість роботи в температурному діапазоні від -20°C до +65°C при високій вологості [5].

5.6.Шлюзи Edge Gateway компанії Dell

Компанія *Dell* просуває свої шлюзи серії *Edge Gateway* як економічне за витратами рішення підвищеної надійності, призначене для агрегації, передачі даних і організації їх аналізу безпосередньо на периметрі мережі. Компанія пропонує два модельних ряди - *Edge Gateway серія 5000* і *Edge Gateway серії 3000.*

Шлюзи серії 5000 передбачають модульне розширення, орієнтовані на стаціонарні системи, великі сенсорні мережі і більш серйозну аналітику в прикордонних сегментах *IoT* мережі. *Серія 3000* ідеально підходить як для фіксованих, так і мобільних варіантів використання, які потребують менших сенсорних мереж, менше місця, а також більш просту аналітику.

Шлюзи промислового класу *Edge Gateway* серії 5000 мають двоядерний процесор *Intel Atom E3800*, оперативну пам'ять ємністю від 2 Гбайт до 8 Гбайт, твердотільні накопичувачі ємністю 32 або 64 Гб і можуть працювати під управлінням різних ОС на вибір замовника *Ubuntu Snappy, Wind River Linux або Windows 10 IoT Enterprise*.

Віддалене управління може здійснюватися для платформи *WindRiver* за допомогою *Helix Device Cloud* або *Windows IoT Industry*, а для *Snappy Ubuntu - Dell Cloud Client Manager (CCM)* або *Dell Client Command Suite, Шлюзи серії 5000* є ідеальною платформою для засобів

інтеграції внутрішніх даних і аналітики від компанії *Dell*, також вони сумісні зі сторонніми рішеннями, в тому числі від сертифікованих незалежних постачальників ПЗ з числа партнерів компанії *Dell*. Захист мережевої периферії і датчиків забезпечується завдяки вбудованим засобам IT-безпеки *Dell*.

Шлюзи виконані в промисловому формфакторі, відрізняється надійністю і тривалим терміном служби. Вони також придатні для експлуатації в умовах підвищеної вологості, запиленості та здатні працювати в широкому діапазоні температур. Модель *Dell Edge Gateway 5100* можна експлуатувати при температурах від -30 ° С до + 70 ° С.

Універсальна підсистема вводу-виводу, яку легко розширити, дозволяє підключати, об'єднувати, передавати і відслідковувати дані з використанням практично будь-яких датчиків і мережевих протоколів від успадкованих протоколів (*BACNet, Modbus і CANbus*) до сучасних мереж (*Zigbee, 6LoWPAN і Z- Wave*). Мережеві можливості шлюзів підтримуються двома портами *Gigabit Ethernet* і модулями *802.11n Wi-Fi, Bluetooth Low Energy,* модулем зв'язку *3G* або *LTE*.

Серія 3000 включає три моделі, які призначені для використання в якості вбудованих рішень в сфері промислової автоматизації, енергетики, транспорту і в системах цифрових табло. Вони дозволяють безпечно передавати важливі дані про функціонування фізичного обладнання на периферії мережі в реальному часі.

Пристрої також розраховані на роботу в широкому діапазоні, стійкі до сильних ударів і вібрації. Всі три моделі включають в себе: процесор *Intel Atom*, оперативна пам'ять ємністю 2 Гбайт і сховище *eMMC* на 8 Гбайт (32 Гбайт в конфігурації з *WWAN*).

Вони оснащені інтерфейсами *Fast Ethernet* з функцією живлення PoE, портами USB 2.0. і 3.0, підтримкою стандартів підключення *Wi-Fi, Bluetooth LE*, стільникового зв'язку. Всі моделі мають вбудований модуль *GPS*, акселерометр і датчики атмосферного тиску для забезпечення ефективної мобільної роботи і управління ресурсами з географічною прив'язкою. У всіх моделях використовуються апаратні засоби захисту для забезпечення безпеки і конфіденційності даних.

Опціональне *ПЗ Dell Edge Device Manager (EDM)* допомагає з легкістю управляти віддаленими пристроями і гарантувати безпеку кожного з них.

Крім того, кожна модель шлюзів лінійки орієнтована на певну область застосування за рахунок додаткових можливостей. Модель 3001 орієнтована на застосування в сучасних виробничих середовищах, тр анспортних системах і периферійних мережах. Багатофункціональний порт *GPIO* (8-канальний) і програмовані послідовні порти (2 x RS-232, RS-422 або RS-485) дозволяють працювати з успадкованими системами, а також розширюють можливості підключення. Є можливість вибору ОС - *Ubuntu Core 16.0 і Microsoft Windows 10 IoT*. Модель 3002 орієнтована на застосування на транспорті і в логістиці.

Стійкість до перебоїв живлення, підтримка інтерфейсу *CANbus*, наявність вбудованих адаптерів *ZigBee* дозволяє організувати стабільний зв'язок з самими різними системами і датчиками на різних видах транспорту. Модель 3003 розроблена для установки в цифрових табло і терміналах роздрібної торгівлі. Вона має вихід *DisplayPort 1.1* для відеодисплеїв (2560 x 1600) і роз'єм лінійного входу/виходу 3,5 мм для високоякісної потокової передачі аудіо.

Всі моделі обслуговуються службою підтримки *Dell*. Наприклад, пакет послуг *Dell ProSupport* передбачає автоматизоване визначення проблем, цілодобовий доступ до інженерів служби підтримки і швидкої заміни компонентів для мінімізації простоїв; послуги розгортання *Dell Deployment*; програма *Dell IoT Solutions Partner Program* для управління рішеннями *IoT*; *Dell Financial Services* для оцінки вартості проекту (фінансових можливостей) [6].

5.7.Шлюзи Enterprise компанії Hewlett Packard

В області *IoT* компанія *HP* активно просуває рішення, що дозволяють перенести обробку даних з хмарних центрів обробки даних на периферію мережі (на кордон між OT і IT). Спеціалізовані *IoT* системи представлені в лінійці *HPE Edgeline*. Лінійка *HPE Edgeline Intelligent Gateway* призначена для збору, передачі даних і обробки подій, а лінійка *HPE Edgeline Converged IoT System* - для рівня первинного аналізу даних і потокової аналітики.

Шлюзи *HPE Edgeline Intelligent Gateway* є компактною і надійною апаратно-програмною платформою, що дозволяє об'єднати дані з вбудованих контролерів і цифрових датчиків і виконати обчислювальні функції початкового (GL10) і середнього (GL20) рівня для сучасних рішень *IoT*. Шлюзи призначені для роботи в промислових середовищах, наприклад на заводах, в розумних містах, на нафтових або газових об'єктах. Замовники можуть аналізувати потоки даних в реальному часі і приймати продумані рішення на основі достовірної інформації. Шлюзи відрізняються підвищеною міцністю і можливістю роботи в діапазоні температур від -20 ° C до + 60 ° C.

Конфігурація *HPE GL10 IoT* включає процесор *lntel Atom*, 4 Гбайт ОЗУ, твердотільний накопичувач 32 Гбайт, а *HPE GL20 IoT* - процесор lntel i5, 8 Гбайт ОЗУ, твердотільний накопичувач 64 Гбайт. Операційні системи – *Microsoft Windows IoT Core, Microsoft Windows Server, Canonical Ubuntu Snappy Core, CentOS*.

Обидва шлюзи мають широкий набір модулів вводу-виводу, в тому числі чотири порти живлення по мережі *Ethernet (PoE)* і модуль ЦАП/АЦП. Кілька слотів для плат mini-PCIe дозволяють користувачам самостійно підключати різні пристрої і забезпечують можливість розширення ресурсів відповідно до майбутніх потреб.

Шлюзи *GL10/GL20* мають можливість комунікацій по Wi-Fi, через мобільні стільникові мережі, мають по 2 порти *Gigabit Ethernet*.

Пристрої *HPE Edgeline Converged IoT System* представляються компанією *HPE* як перші в галузі конвергентні системи для промислового Інтернету речей.

Системи *Edgeline EL1000 і EL4000* можна представити як шлюзи 2-го рівня, які об'єднують дані з *HPE Edgeline Intelligent Gateway.*

Системи *HPE Edgeline* оптимізовані для високопродуктивного аналізу, інтерпретації, візуалізації даних і надання інформації в режимі реального часу на периферійних ділянках мережі. Вони об'єднують обчислювальні ресурси, сховища, засоби захоплення і контролю даних, операційне середовище рівня підприємства і надають розробникам платформу для доступу до структурованої і неструктурованої інформації, а також забезпечують автоматизацію роботи з цими даними.

Іншою важливою особливістю *HPE Edgeline* є унікальна інтеграція збору точних даних з вимірювальних систем і їх управління, заснована на базі відкритих PXI стандартів. Коли вони доповнюються автоматичним машинним навчанням, це відкриває нові можливості в моніторингу і управлінні, прогностичній аналітиці для виявлення можливих поломок, а також доповнену реальність для мінімального ручного обслуговування. *HPE Edgeline* приносить всі можливості управління віддаленими системами, які надає *Integrated Lights Out (iLO).*

HPE Edgeline повністю сумісні з такими популярними IoT системами безпеки як Aruba ClearPass для автоматизації автентифікації, запобігання загрозам злому і функцій відновлення систем в умовах підвищеного ризику поза ЦОДами. *Aruba Virtual Intranet Access (VIA)* дозволяє організувати безшовні *Virtual Private Network (VPN)* тунелі для безпечних з'єднань між вузлами на кордоні IT-мереж і корпоративною мережею.

Ці міцні і компактні системи працюють в розширеному діапазоні робочих температур від 0 ° C до + 55 ° C і здатні справлятися з підвищеним ударним та вібраційним навантаженням.

Важливою особливістю *HPE Edgeline* є безпрецедентні обчислювальні можливості. У EL1000 можна встановити один обчислювальний модуль (до 16 *ядер Xeon D або Xeon E3)* з двома відсіками для дисків *SATA SFF*, двома портами *Gigabit Ethernet* або *10 Gigabit Ethernet*. Широкі можливості підключення периферійних пристроїв забезпечуються за

допомогою двох слотів PCIe або *PXI/PXIe* разом з бездротовими модулями *Wi-Fi* або 3G. У *EL4000* можна розмістити 4 обчислювальних модуля, кожен з яких може отримати свій модуль розширення PCIe або PXIe і два *10G Ethernet* порти для прямого підключення до мережі.

Модель *Edgeline 4000* також надає можливість організувати відмовостійку розподілену систему зберігання даних, а також працювати з аналітичною платформою на базі *SQL HPE Vertica* для отримання, обробки і завантаження готових даних від мільйонів «розумних лічильників» в секунду, з затримками в наносекунди [7].

Висновки

Були виділенні основні критерії, що необхідно розглядати при виборі IoT шлюзів. Основники характеристиками, на які необхідно спиратись є:

- Підтримка перефирійних/туманних обчислень;
- Підтримуванні технології обміну даними;
- Функції маршрутизатора;
- Функції управління кінцевими пристроями мережею і додатками;
- Функції безпеки пристроїв, мережі і додатків.

Якщо декілька шлюзів задовольняють умовам описаним вище, то необхідно дивитись на такі характеристики, як: обчислювальна потужність, форм-фактор та умови, в яких шлюз можна використовувати.

Як можна побачити, лідери ринку *IoT Intel, Hewlett Packard, Cisco, Dell Technologies*, а також компанії, які на цьому ринку недавно *Huawei, NEXCOM, Monnit, Davra Networks* та ін., підтримують весь спектр перерахованих функцій. Всі з розглянутих виробників пропонують як універсальні шлюзи для використання у різних галузях промисловості, так і рішення для окремих вертикалей ринку.

Лінійки шлюзів, що пропонуються, включають як малопотужні енергоефективні моделі для легких економних проектів, наприклад, *NEXCOM*, молодші моделі *Dell* та *Intel*, так і промислові моделі, спрямовані на аналітику та зберігання великих об'ємів даних, самим яскравим представником яких є конвергентні системи *Hewlett Packard*.

Контрольні питання до розділу

1. Основними критеріями при виборі шлюзу для Інтернету речей можна назвати:
   a. Підтримка переферійних/хмарних обчислень.
   b. Підтримуванні технології обробки даних
   c. Функції маршрутизатора
   d. Функції управління кінцевими пристроями, мережею і додатками
   e. Функції безпеки пристроїв, мережі і додатків
2. У виипадку вибору критерія шлюза «Підтримка переферійних/туманних обчислень» на що слід звернути увагу?
3. У виипадку вибору критерія шлюза «Підтримуванні технології обміну даними» на що слід звернути увагу?
4. Які наступні можливості буде мати шлюз, який працює як багато портові маршрутизатори:
   a. Підтримка маршрутизації між декількома проводовими чи Wi-Fi локальними IoT мережами;
   b. Підтримка поширених функції IP маршрутизаторів – протоколів маршрутизації, DHCP, таблиць доступу, міжмережевих екранів;
   c. Підтримка комутації – вибір методу комутації, при проходженні даних від вхідного порта до вихідного.
5. У виипадку вибору критерія шлюза «Функції управління кінцевими пристроями мережею і додатками» на що слід звернути увагу?

6. У виипадку вибору критерія шлюза «Функції безпеки пристроїв, мережі і додатків» які функції для IoT є життєво важливими?
7. Які існують основні технічні характеристики шлюзів?
8. Шлюзи компанії Eurotech. Пристрої серій *ReliaGATE 10-20, ReliaGATE 10-11 і ReliaGATE 10-05.*
9. Шлюзи компанії Eurotech. Пристрої серій *ReliaGATE 20-25, ReliaGATE 20-26, DynaGATE 15-10.*
10. *Шлюзи компанії Intel на базі процесорів Quark, Atom, Core, Xeon.*
11. Шлюзи компанії Huawei.
12. Шлюзи компанії Cisco.
13. Яку доступну функціональність, що необхідна при створенні корпоративних рішень надають маршрутизатори *Cisco*:
   a. *динамічний багатоточковий VPN (DMVPN);*
   b. *аналіз якості обслуговування (QoS) для стільникового зв'язку;*
   c. *аналіз якості обслуговування (QoS) для проводового зв'язку;*
   d. *мульти-віртуальна переадресація маршрутів (VRF) для стільникового зв'язку;*
   e. *операційну систему Cisco Iox.*
14.Шлюзи компанії NEXCOM.
15. Шлюзи Edge Gateway компанії Dell.
16. Шлюзи Enterprise компанії Hewlett Packard.

Список рекомендованої літератури

1. Хмарні технології в автоматизації.: комплексний підхід від Eurotech. Олексій П'ятницьких. (2016, Жовтень). Control Engineering, Росія. http://controleng.ru/wp-content/uploads/CE_IoT_Listalka.pdf
2. Технологія Intel IoT Gateways. (2018). Офіційний сайт компанії Intel. https://software.intel.com/ru-ru/iot/hardware/gateways
3. Huawei AR Series Agile Gateways Brochures. (2017). Офіційний сайт компанії Huawei. http://www.huawei.com/minisite/iot/img/hw_ar_series_agile_gateways_brochure/en.pdf
4. Cisco IoT Networking. (2017). Офіційний сайт компанії Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/brochure-c02-734481.pdf
5. IoT Gateway. (2018). Офіційний сайт компанії NEXCOM. http://www.nexcom.com/Products/industrial-computing-solutions/iot-solutions/iot-gateway
6. Dell змінює економіку Інтернету речей з новими компактними шлюзами Edge Gateway. (1 березня 2017). Офіційний сайт компанії Dell. www.dell.com/learn/ua/ru/uacorp1/press-releases/dell-changing-economy-of-iot-with-new-compact-gateways-edge-gateway
7. Короткий огляд апаратних платформ, типових архітектурних рішень і послуг для корпоративних інформаційних систем. (2018, весна). Офіційний сайт компанії Hewlett Packard. https://h20195.www2.hpe.com/v2/GetPDF.aspx/c04771945.pdf

РОЗДІЛ 6. ПРОСТІ ТА ІНТЕЛЕКТУАЛЬНІ СЕНСОРИ

Увесь досвід розвитку людської цивілізації свідчить про те, що чим правильніше і краще люди розуміють світ, чим точніше, більше і глибше знають про нього, і чим у більшій згоді із законами природи діють, тим успішніше і краще облаштовують вони своє життя. У свою чергу, рівень, достовірність і глибина наших знань про світ багато в чому визначаються тим, за допомогою яких засобів сприймаємо ми цей світ, спостерігаємо за ним, стежимо за змінами, що відбуваються в нім, і явищами.

В період становлення людства наші пращури використали для цього тільки свої органи чуття, можливості яких обмежені. Але у міру розвитку технологій, техніки, науки люди стали все ширше застосовувати також і різноманітні технічні пристрої, які доповнюють або замінюють наші органи чуття.

Такі пристрої прийнято називати сенсорами (від латинських слів *sensus* - почуття і *sensorium* - орган чуття).

Можна сміливо стверджувати, що рівень розвитку цивілізації (разом з іншими найважливішими чинниками) характеризується рівнем розвитку сенсорів. Їх роль в забезпеченні нашої правильної орієнтації, в об'єктивнішому, точному і глибокому сприйнятті дійсності, в підвищенні якості і ефективності нашої діяльності важко переоцінити. Особливо це стосується біології, медицини, соціальної сфери, високотехнологічних галузей, де ми маємо справу з дуже складними об'єктами, оцінювати стан яких і процеси, в що них відбуваються, тільки "на око", за зовнішніми ознаками вже недостатньо.

Сенсори до того ж - це саме ті пристрої, в яких відбувається загадковий процес "народження інформації" і в яких фізико-хімічні зміни, що відбуваються в реальній дійсності, перетворюються на інформаційні сигнали, що служать основою для розумної поведінки, для формування і уточнення моделей цієї дійсності, наших уявлень про неї.

По великому рахунку, саме від сенсорів фактично і починається будь-яка розумна поведінка, всякий інтелект, уся інформатика.

Будь-яка розумна система, що виникла природним чином або створена іншою розумною системою, успішно функціонує і виживає у реальному світі лише тоді і доти, коли і доки вона отримує об'єктивну і якісну інформацію про нього.

Вражаюче швидке, можна сказати, "*революційне*", розвиток в останні десятиліття кібернетики, мікроелектронної і оптоелектронної елементної бази інформатики, так, власне, і самих прикладних галузей знань, зробило можливою побудову нового покоління "*розумних*" сенсорів. Такі сенсори стали називати "*інтелектуальними*" - від латинського слова *intellectualis*, яке окрім значення "розумовий" має також значення "*Розсудливий, міркуючий, розумний*".

Створення і усе більш широке застосування інтелектуальних сенсорів - це одна з ознак інформаційної стадії в розвитку суспільства.

Інтелектуальні сенсори - це вже не мрія, не окремі розрізнені досягнення сучасної техніки, що вони вже упевнено увійшли до нашого повсякденного життя. Їх розробка і виробництво сталі самостійною важливою інноваційною підгалуззю приладобудування. Поки цей факт не завжди усвідомлюють навіть фахівці - розробники окремих інтелектуальних сенсорів.

Різні автори по-різному трактують поняття "*сенсор*". У одних - це "чутливий прилад", майстерно створений людиною "пильний сторож", у інших - "аналізатор", що розпізнає, дізнається потрібний об'єкт ("аналіт"), у третіх - " датчик " якоїсь фізичної величини (температури, тиску, кута повороту), у четвертих - орган чуття тварини або рослини і так далі.

Сенсори - це "пристрої, які доповнюють або замінюють наші органи чуття". І усе це частково правильно. Дійсно, усі сенсори щось "відчувають" (наприклад, зміна температури, наявність магнітного поля, зміна кислотності розчину і тому подібне); за чимось "пильно спостерігають"; щось "розпізнають" (напр., відхилення від вертикалі, поява в повітрі надлишку вуглекислого газу, наявність у воді збудника холери ...); "вимірюють" яку-небудь

фізичну величину (напр., освітленість, прискорення, тиск ...). Усі вони, дійсно, замінюють або доповнюють наші органи чуття.

У понятті "датчик" акцент робиться на іншій важливій здатності сенсора - на тому, що він видає в зовнішній світ сигнали про те, що він "відчуває", "розпізнає", "вимірює". Щоб точніше визначити поняття "сенсор", потрібно відволіктися від деталей, від того, що саме "відчуває", "розпізнає", "вимірює" сенсор, з якою конкретною метою і як саме він це "робить", яким конкретно образом видає він сигнали в зовнішній світ.

Головне, загальне, що тоді залишається, - це те, що:

1. у сенсора є "об'єкт спостереження";
2. взаємодіючи з об'єктом спостереження, під його впливом сенсор міняє свій стан ("відчуває", "розпізнає", "вимірює") і якимсь чином видає сигнали про це ("сигналізує") "користувачеві".

Об'єктом спостереження є той матеріальний об'єкт, процес, та середовище, з якими взаємодіє сенсор, інформацію про які він "приставлений" збирати. Об'єктом спостереження може бути, зокрема, і усе середовище, що оточує сенсор.

Для *рівня (ватерпаса),* наприклад, об'єктом спостереження є плоска поверхня, на якій він встановлений; для радіоприймача об'єктом спостереження є те, що оточує його антену електромагнітне поле; для медичного градусника - тіло, що знаходиться в тепловому контакті з його кінцем, в якому знаходиться крапля ртуті.

"Користувачем", одержуючим, розуміючим і використовуючим сигнали від сенсора може бути людина, інша жива істота, автоматична система управління, регулювання або реєстрації, для яких сигнали від сенсора є "інформацією" про об’єкт спостереження. Таким чином, відволікаючись від частковостей, ми приходимо до наступного визначення поняття "сенсор".

Сенсор - це пристрій (прилад, орган, вузол), що перетворює фізичну (фізико-хімічне) зміну в об'єкті спостереження, його фізична дія в інформаційний сигнал для користувача.

Сенсор - ця сполучна ланка між реальним "фізичним" світом і світом інформаційних моделей, між матерією і інформацією.

Сенсори поставляють "користувачеві" найважливішу об'єктивну початкову інформацію, на основі якої тільки і можна передбачати події, розумно поводитися у світі, судити про те, наскільки створені і вживані користувачем інформаційні моделі адекватні реальним процесам і об'єктам, з якими він має справу.

6.1. Прості сенсори

Ще відносно нещодавно люди використали в основному прості сенсори, що дають тільки "сиру", первинну, необроблену інформацію про об'єкти і процеси, за якими ведеться спостереження.

Розшифровку, обробку цієї інформації, зіставлення її з іншими даними виконували самі люди, вони ж оцінювали її значущість і міру важливості.

Одними з перших простих сенсорів, напевно, були схили - для виявлення відхилень від вертикалі; згадані вже вище рівні - сенсори малих відхилень від горизонтального положення плоскої поверхні; флюгери, відстежуючі і показуючі напрям вітри; поплавці у вудках для лову риби; компаси - для точнішого орієнтування на місцевості і т. д.

Функціональна схема простого сенсора

Головними його складовими частинами є чутливий елемент і сигналізатор. Реагуючи на ту або іншу дію з боку об'єкту спостереження, чутливий елемент міняє свій стан, а сигналізатор видає про це якийсь зрозумілий користувачеві сигнал. Цей сигнал і є носієм інформації про об'єкт спостереження [1].

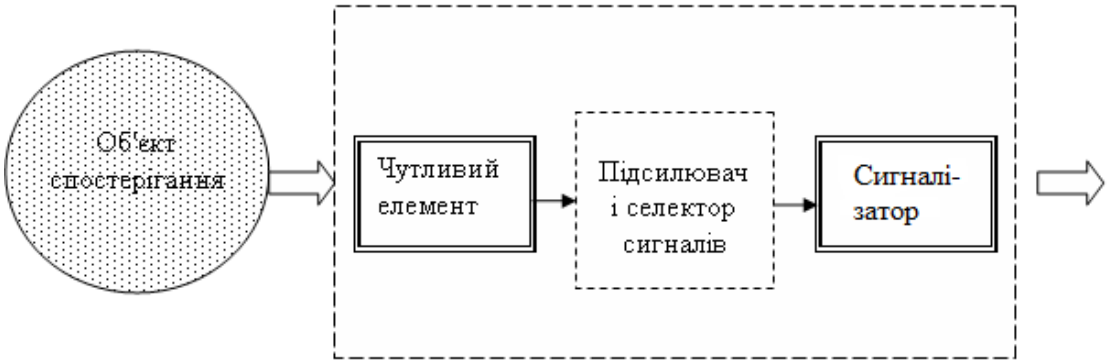


Рис.6.1.Функціональна схема простого сенсора

Якщо зміни в стані чутливого елементу дуже незначні і вихідні сигнали виходять дуже слабкими або "зашумлені" якимись сторонніми впливами, то в сенсорі використовують також вузли посилення і/або селектори корисних сигналів. Проте вони не є обов'язковою складовою частиною сенсора і тому зображені штриховою лінією.

Розглянемо декілька прикладів. У простому сенсорі магнітного поля - *в компасі* - чутливим елементом є намагнічена тонка стрілка (смужка із заліза або з іншого феромагнетика або з їх сплаву), встановлена і урівноважена на вертикальній осі, навколо якої вона може вільно обертатися. Магніт завжди прагне обернутися своїм північним полюсом у напрямі магнітних силових ліній. Роль сигналізатора спільно виконують тут вістря стрілки і шкала з кутовими діленнями, що полегшує відлік кута між напрямом магнітної стрілки і заданим напрямом (напр., напрямом руху).

Якщо магнітна стрілка досить довга, то в посиленні сигналів немає необхідності. А ось механічні вібрації, особливо під час руху, викликають значні коливання, "рискання" стрілки, що утрудняє відлік напряму. Для того, щоб зменшити "рискання", внутрішню порожнину компаса заповнюють рідиною з оптимально підібраною в'язкістю, яка, з одного боку, ефективно гасить швидкі хаотичні рискання стрілки, а з іншою, - не викликає значного запізнювання повороту стрілки при зміні напряму руху. Ця рідина і виконує в компасі роль селектора корисних сигналів або, якщо хочете, частотного фільтру, що "відрізує" коливання з частотами вище приблизно 1 Гц.

У звичних медичних *ртутних термометрах* - сенсорах температури тіла - роль чутливого елементу грає невелика крапля ртуті, залита всередину скляної колби. Будучи приведена в тепловий контакт з нашим тілом, вона нагрівається до його температури. Чим вище температура тіла, тим більше теплове розширення ртуті. Роль підсилювача сигналу грає приєднаний до колби скляний капіляр, в якому невеликі зміни об'єму краплі ртуті трансформуються в помітне подовження ртутного стовпчика. Останній разом з приставленою до капіляра температурною шкалою і виконують роль сигналізатора.

У *простому електрокардіографі* - сенсорі змін електричних потенціалів в різних точках на поверхні грудної клітки - чутливими елементами є електроди з присосками, змочені електролітом для забезпечення електричного контакту з тілом. Оскільки первинні сигнали від них - невеликі електричні потенціали - дуже слабкі, то обов'язково використовують електронні підсилювачі. Як правило, щоб заглушити електромагнітні завади, застосовують також електричний фільтр частот вище приблизно 10 Гц. Роль сигналізатора виконує те або інший пристрій для візуалізації електрокардіограми.

Тільки разом, тільки в сукупності і у взаємодії чутливий елемент і сигналізатор можуть служить сенсором. Вони є обов'язковими, невід'ємними функціональними вузлами сенсора. З розвитком техніки і зростанням вимог з боку прикладних областей (промисловості, наукових досліджень, медицини, технології) в сенсорах також почали виконувати спочатку просту, а з часом усе більш складну обробку інформації. Функціональна схема такого сенсора приведена нижче на рис. 6.2.

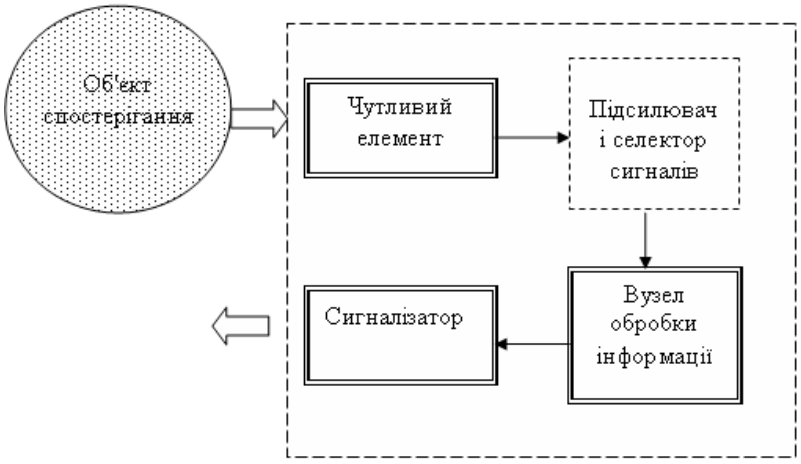


Рис. 6.2. Структура простого сенсора з обробкою інформації

Коли фахівцям з фізіології рослин стало необхідно визначати загальну кількість світла, що отримується рослинами за світловий день, був створений відповідний сенсор, в якому чутливим елементом є фотоприймач.

Під впливом зовнішнього освітлення він генерує фотострум, пропорційний світловому потоку, що падає.

Фотострум після посилення поступає в конденсатор, який і грає роль вузла обробки інформації, в даному випадку - роль інтегратора. Накопичений в нім за світловий день електричний заряд якраз і пропорційний кількості світла, отриманій рослинами ("світлосумі").

У *психрометрі* - сенсорі температури і відносної вологості повітря - роль вузла простої обробки інформації грає вбудована в нього *психрометрична* таблиця. У ній користувач, визначивши свідчення "сухого" і "вологого" термометрів, може знайти відповідне значення відносної вологості.

У деяких психрометрах є також таблиця залежності тиску або щільності насиченої водяної пари від температури. Тоді користувач дістає можливість, визначити не лише відносну, але і абсолютну вологість повітря.

На прикладі психрометра ми бачимо, що у сенсора можуть бути декілька чутливих елементів. В даному випадку в наявності 3 чутливі елементи: 2 колби з ртуттю, спиртом або іншою рідиною, що збільшує свій об'єм з підвищенням температури, і волога тканина, якою обмотана колба "вологого" термометра. Вона якраз і є чутливим елементом, що "відчуває" зміни вологості повітря.

У древньому пісочному годиннику - сенсорі часу - ніякої обробки інформації не було. А ось в механічному годиннику з'явилися зубчасті передачі, які і є в цьому сенсорі часу вузлом обробки інформації. Вони перераховують періоди коливань маятника в задані інтервали часу - хвилини і годинник.

На прикладі стрілочного механічного годинника ми бачимо, що сенсор може мати і декілька сигналізаторів. В даному випадку є 2 обов'язкові сигналізатори - хвилинна і годинна стрілки з циферблатом, і може бути навіть 3-ою - секундна стрілка.

6.2. Активні та пасивні сенсори

Досі розглядалися приклади простих сенсорів, які тільки реагують на вплив з боку об'єкту спостереження. Такі сенсори називають "пасивними".

На відміну від них "активні" сенсори самі якимсь спеціальним чином впливають на об'єкт спостереження (предмет або процес) і сприймають викликані цим зміни.

Одним з прикладів може бути тонометр - сенсор артеріального тиску крові. Вузлом дії на об'єкт є в нім манжета, яка накладається на плече або на передпліччі пацієнта і створює усебічний тиск на біотканину і кровоносні судини.

Задатчиком дії є надувна гумова "груша" або мініатюрний компресор. Чутливим елементом і одночасно підсилювачем сигналів служить стетоскоп, який приставляють до артерії, розташованої по напряму потоку крові за манжетою.

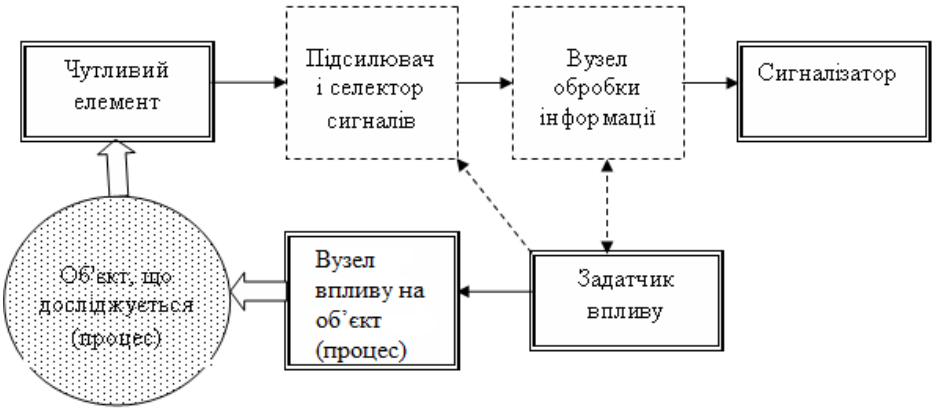


Рис. 6.3. Функціональна схема активних сенсорів

Поступово підбурюючи повітря і зменшуючи тим самим зовнішній тиск на артерії, лікар повинен уловити той момент, коли пульсація крові поновлюється. У цей момент тиск повітря в манжеті і її тиск ззовні на артерії приблизно дорівнюють систолічному артеріальному тиску крові усередині артерій.

При подальшому зниженні тиску в манжеті пульсові хвилі спочатку посилюються, а потім починають слабшати.

Коли тиск в манжеті порівнюється з артеріальним тиском діастоли і опускається нижче, то пульсові удари значно ослабляються.

Сигналізатором в цьому сенсорі є сполучений з манжетою манометр, на якому лікар прочитує значення систолічного (у момент відновлення пульсацій крові) і діастоли тиску (у момент значного послаблення пульсацій).

Вузла обробки інформації в простих тонометрах немає. Цю обробку виконує людина - лікар.

У тонометрі одночасно є присутніми і використовуються 2 чутливі елементи - мембрана, що приставляється до артерії, стетоскопа и манометр, що реагує на зміни тиску в манжеті. Одночасно використовуються і 2 сигналізатори - слухові виходи стетоскопа, які лікар вставляє у вуха, щоб прослуховувати биття пульсу, і стрільця манометра з відповідною шкалою.

Інший приклад "активного" сенсора наведемо знову з області фізіології рослин. Там свого часу з'явилася необхідність визначати об'ємний потік рідини крізь стебло або по гілках рослини і зміни цього потоку з часом. Вирішено це завдання була так. На стебло (гілку) в одному з місць встановлюють тонкий нагрівач, наприклад, вольфрамовий дріт, крізь який пропускається електричний струм. Нагріваючи гілку в місці свого розташування, нагрівач разом з нею нагріває і рідину, поточну по гілці, до фізіологічно допустимої температури, наприклад, до 39-40 С.

Нагрівач і є в даному випадку вузлом дії на об'єкт. Задатчиком дії служить регульоване джерело струму через нагрівач. Далі по ходу руху рідини уздовж стебла на відстані близько сантиметра встановлюють другий термочутливий елемент (термістор, термопару).

Сигнал від нього посилюють, фільтрують по частоті і подають в електронний вузол обробки інформації. Там визначається різниця температур гілки в місцях нагрівання і контролю.

Чим сильніше потік рідини, тим більше тепла переносить з собою рідина, і тим менше різниці температур.

Таким чином, по зміні різниці температур визначають зміни об'ємного потоку рідини усередині стебла (гілки).

6.3. Сенсорно-комп’ютерні системи

З появою в другій половині минулого століття електронних обчислювальних машин з'явилася і можливість виконувати досить складну обробку первинної інформації, що отримується від сенсора.

У зв'язку з цим інженери і учені почали створювати "розумні" сенсорно-комп'ютерні системи.

Сенсори тут грають роль зовнішніх "органів чуття" комп'ютера, поставляючи йому первинну інформацію.

Складну її обробку, підготовку до видачі отриманих результатів в найбільш зручній для користувача формі, її документування, систематизацію, упаковку і тривале зберігання виконує комп'ютер.

З появою в другій половині минулого століття електронних обчислювальних машин з'явилася і можливість виконувати досить складну обробку первинної інформації, що отримується від сенсора.

У зв'язку з цим інженери і учені почали створювати "розумні" сенсорно-комп'ютерні системи.

Сенсори тут грають роль зовнішніх "органів чуття" комп'ютера, поставляючи йому первинну інформацію.

Складну її обробку, підготовку до видачі отриманих результатів в найбільш зручній для користувача формі, її документування, систематизацію, упаковку і тривале зберігання виконує комп'ютер.

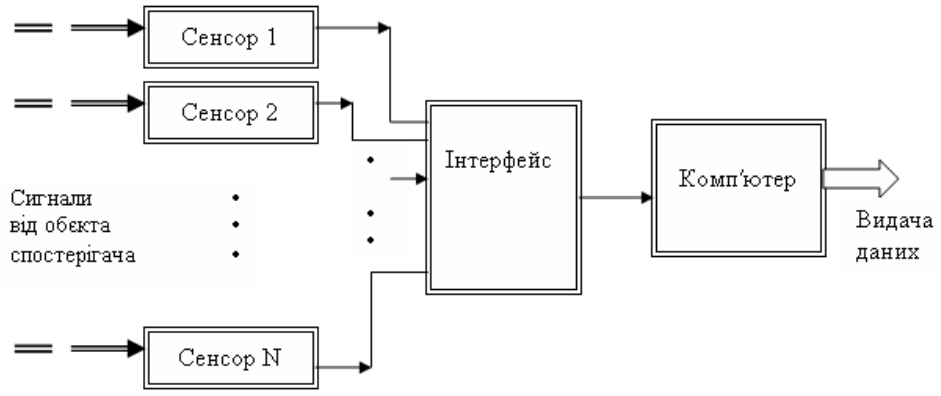


Рис. 6.4. Структура "пасивної" сенсорно-комп’ютерної системи

Наприклад, сучасні комп'ютеризовані електрокардіографи і електроенцефалографи.

У них від багатьох, встановлених в певних позиціях, електродів збираються, посилюються і обробляються слабкі змінні електричні сигнали, обумовлені роботою відповідно серця або головного мозку. А комп'ютер аналізує їх і видає в найбільш зручній формі лікарям [2].

У комп'ютерних електрокардіографах, наприклад, не лише обчислюються інтервали часу між "зубцями" кардіограми, що відповідають скороченням м'язів серця, і діапазон їх варіювання, середня частота пульсу і інші кількісні показники.

Шляхом зіставлення електрокардіограм, отриманих від різних точок грудної клітки, встановлюється орієнтація електричної осі серця, фіксуються екстрасистоли і інші порушення координації скорочень різних м'язів серця.

У комп'ютеризованій системі магнітокардіографії [3, 4] чутливими елементами є певним чином розташовані в просторі надпровідні квантові інтерферометри, які здатні з високою частотою і точністю сприймати мінімальні зміни магнітного потоку, пов'язані з роботою серця.

Окрім квантових інтерферометрів, використовують також до десятка чутливих електродів, які дозволяють паралельно знімати також електрокардіограму.

Інтерфейс складається з електронних схем посилення і попередньої аналогової обробки сигналів і з аналого-цифрових перетворювачів.

З виходу останніх інформація поступає в комп'ютер, який обробляє отримані дані відповідно до досить складних алгоритмів, видає результати аналізу на екран монітора у вигляді зрозумілих лікареві умовних зображень, цифрових і текстових даних і пропонує деякі діагностичні висновки.

Ще одним прикладом є пасивні комп'ютерні системи охорони і відеоспостереження.

Чутливими елементами в них служать відеокамери і датчики наближення, присутності, зміни обстановки.

Сигнали від датчиків і отримані зображення передаються в комп'ютер, де вони маркуються вказівкою місця виявлення і поточного часу.

Далі вони обробляються, зіставляються між собою і із стандартними сигналами, зафіксованими в пам'яті. У разі виявлення тривожних змін комп'ютер фіксує їх у своїй довготривалій пам'яті і виробляє сигнали привертання уваги службовців, а на монітори виводиться поліекранна інформація.

Тут до складу системи входять також засоби дії на досліджуваний об'єкт або процес. Цими засобами управляє комп'ютер, який може автоматично змінювати динаміку, інтенсивність і склад дій залежно від тих, що поступають від сенсорів даних.

Одним з прикладів такої системи є комп'ютерні томографи.

Об'єктом дослідження для них є головний мозок або інша частина людського тіла. Як вузли дії використовуються точкові джерела рентгенівського випромінювання, місце розташування яких можна міняти відносно досліджуваній частині тіла.

В якості сенсорів використовують детектори рентгенівського випромінювання, розташовані в одній площині у різних напрямах і під різними кутами.

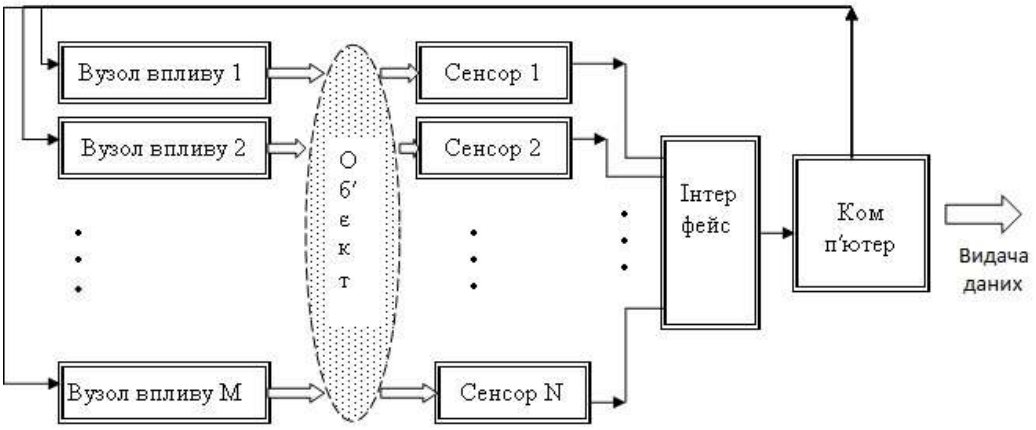


Рис. 6.5 Структура "активних" сенсорно-комп'ютерних систем

У сучасних томографах, які стали могутнім засобом діагностики захворювань, застосовують вже сотні таких детекторів одночасно. Високопродуктивний комп'ютер на основі великого масиву даних, отриманих багатьма детекторами під різними кутами, виконує складні обчислення, визначаючи за цими даними розподіл щільності живих тканин у відповідному перерізі тіла. Отримані зображення і вичислені показники видаються лікарям [5]. За допомогою комп'ютера лікар, який проводить дослідження, залежно від мети може змінювати режими роботи, переміщати вузли дії і масиви сенсорів відносно людського тіла, отримуючи зображення його внутрішньої структури також і в інших перерізах, і так далі. Таким чином ("переріз за перерізом") може бути отримана 3-мірна картина внутрішньої будови досліджуваного органу. Одним із засобів дії може бути також введення в організм людини контрастних речовин, що істотно підвищують контрастність зображень і дозволяють досліджувати також і динаміку фізіологічних процесів.

У магніторезонансній томографії засобами дії на досліджуваний орган людини є постійне однорідне магнітне поле, послідовності радіочастотних електромагнітних імпульсів

і додаткові слабкі градієнтні магнітні поля [6]. Магнітні моменти атомних ядер з некомпенсованим напівцілим спіном (^{1}H, ^{13}C, ^{13}Na, ^{13}P, …) орієнтуються уздовж постійного магнітного поля. А високочастотне електромагнітне поле збуджує їх прецесію навколо відповідного напряму. При виключенні електромагнітного поля прецесія ще деякий час триває. Збуджені ядра випромінюють при цьому електромагнітні сигнали характерної частоти.

Це називають "спіновою луною". Сенсорами є чутливі радіоприймачі, налаштовані на частоту ядерного магнітного резонансу, а селекторами - синхронні детектори відповідних імпульсних послідовностей. Амплітуда прийнятих сигналів пропорційна концентрації відповідних ядер в живих тканинах тіла.

Управління випромінюванням електромагнітних імпульсів і накладенням слабкого градієнтного магнітного поля, а також математичну обробку сукупності отримуваних сигналів виконує комп'ютер. На відміну від рентгенівської комп'ютерної томографії магніторезонансне дослідження не супроводжується шкідливим опроміненням організму, яке у великих дозах може бути небезпечним.

Застосування комп'ютерів надало користувачам не лише можливість отримувати значно збільшені об'єми набагато краще обробленої і достовірнішої інформації про досліджувані об'єкти. Воно підняло сенсорику на принципово більш високий рівень - на рівень діагностики. Старогрецьке слово " *diagnostikos* " означає "*здатний розпізнати*".

За відсутності комп'ютера інтерпретацію отримуваних від сенсорів даних, виведення з них здатні були виконувати тільки фахівці.

Фізики на основі отримуваних даних робили висновки про внутрішню структуру, функціонування, поточний стан і властивості досліджуваних фізичних об'єктів, інженери - про стан відповідних машин, технічних систем, про хід технологічних процесів.

Лікарі визначали стан внутрішніх органів людини, причини, суть захворювань, оцінювали хід лікування. У сенсорно-комп'ютерних системах значну частину складної розумової роботи, накопичення баз даних, цінного досвіду, необхідних для високоякісної діагностики, вдалося вже перекласти на комп'ютер.

6.4. Інтелектуальні сенсори

Зовсім нові можливості з'явилися в 80-х роках XX століття, коли почалося серійне виробництво мікропроцесорів і мікрокомп'ютерів, що уміщалися вже на одному кристалі кремнію ("чіпі"). Кожен з них - це маленький універсальний штучний електронний "мозок", який можна вбудувати в сенсор і виконувати в нім досить складну обробку первинної інформації. Тим самим склалися передумови для народження принципово нового класу сучасних "інтелектуальних" сенсорів.

Такі сенсори, як правило, є "активними", тобто не просто пасивно сприймають вплив, властивості, характеристики об'єкту спостереження, але і самі спеціальним чином впливають на об'єкт, сприймаючи і аналізуючи викликані цим зміни.

Для них не є проблемою врахувати нелінійність характеристик чутливих елементів, різні поправки і вплив сторонніх дій (напр., зміни температури). Якщо вимагається, вони самі автоматично можуть повторити виміри, усереднити результати, перерахувати в інші одиниці виміри і т. п.

Його "інтелект" зосереджений в мікрокомп'ютері МК (інші назви - мікропроцесор, мікроконтроллер, мікроконвертор).

МК не лише обробляє інформацію, але і організовує усю роботу сенсора і його інформаційний зв'язок із зовнішнім світом - з користувачем, із зовнішнім комп'ютером, з каналом зв'язку або з комп'ютерною мережею.

Мікрокомп'ютер за наявності відповідних закладених в його пам'ять мікропрограм може виконувати також самоконтроль, контроль усіх вузлів сенсора і видавати користувачеві попередження і діагностичні повідомлення. Користувач має можливість впливати на роботу сенсора через клавіатуру (Кл), зокрема, вибирати і змінювати режими роботи, задавати або змінювати якісь уставки і параметри і т. д.

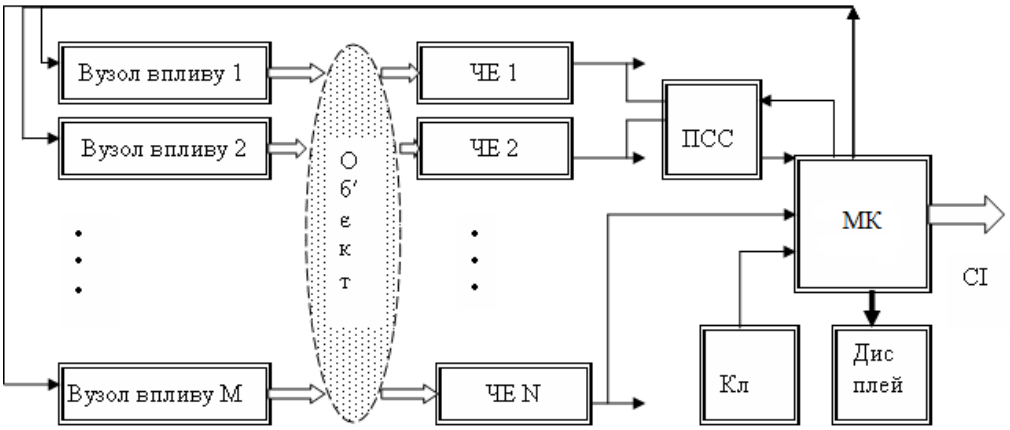


Рис. 6.6. Функціональна схема "інтелектуального" сенсора
ЧЕ - чутливі елементи; ПСС - підсилювачі-селектори сигналів; МК - мікрокомп'ютер;
Кл – клавіатура, СІ – стандартний інтерфейс.

Отримавши команду про початок роботи, мікрокомп'ютер в передбаченому програмою порядку включає вузли дії на об'єкт спостереження і починає відстежувати сигнали, що поступають від чутливих елементів (ЧЕ). Слабкі або "зашумлені" сигнали заздалегідь посилюються і виділяються в підсилювачі-селекторі сигналів (ПСС). Сигнали, що не вимагають посилення або селекції, можуть поступати безпосередньо в мікрокомп'ютер. Відстежуючи дані від чутливих елементів, мікрокомп'ютер може автоматично змінювати інтенсивність або характер дії на об'єкт спостереження, величину посилення або характер селекції сигналів у вузлі ПСС.

Відповідно до заданої мікропрограми мікрокомп'ютер обробляє сукупність сигналів, що поступають від чутливих елементів, а отримані результати перекодує в найбільш зручну для користувача форму і виводить на дисплей. Отримані результати можуть бути також помічені, розсортовані, "упаковані", занесені в довготривалу пам'ять мікрокомп'ютера і зберігатися в ній, а коли знадобиться, то через стандартний інтерфейс (СІ) передані в зовнішній комп'ютер або в комп'ютерну мережу. Завдяки цьому нові "інтелектуальні" сенсори органічно вписуються в новітні високопродуктивні технології промислового і сільськогосподарського виробництва, медичної практики, наукових досліджень.

У деяких інтелектуальних сенсорах клавіатуру і дисплей об'єднують у вигляді сенсорного екрану.

Наявність вбудованого мікрокомп'ютера надає "інтелектуальним" сенсорам небачену раніше гнучкість, можливість автоматичної адаптації до умов роботи, що змінюються. Стає можливою багатофункціональність, коли, міняючи яку-небудь насадку і переходячи в інший режим роботи, сенсор порівняно легко може виконувати зовсім іншу функцію. Наприклад, багато мобільних телефонів можуть служити і в якості записника, кишенькового комп'ютера, цифрового фотоапарата [7].

І, нарешті, інтелектуальний сенсор може бути здатний не лише збирати, обробляти і поставляти ті або інші дані про контрольований об'єкт, але і інтерпретувати їх, допомагаючи користувачеві в діагностиці і ухваленні рішення.

Можна сміливо стверджувати, що без інтелектуальних сенсорів не може функціонувати і справжній штучний інтелект. Адже глибока попередня обробка первинних даних вже в сенсорах - це передумова створення інформаційних моделей усе більш високого рівня.

Підводячи підсумок, поняття "Інтелектуальний сенсор" можна визначити таким чином.

Інтелектуальний сенсор - це сенсор, що має у своєму складі мікрокомп'ютер і завдяки цьому здатний виконувати досить складну обробку первинної інформації; враховувати все нелінійності і необхідні поправки; видавати дані в найбільш зручній для користувача формі; активно впливати на об'єкт спостереження, сприймаючи і аналізуючи викликані цим зміни; робити самоконтроль і самодіагностику; накопичувати і систематизувати дані; підтримувати інформаційний зв'язок із зовнішнім світом; змінювати

режими своєї роботи, адаптуючись до умов, що змінюються; переходити до виконання інших функцій і т. д.

Класифікація інтелектуальних сенсорів

Інтелектуальні сенсори можна класифікувати, як і прості сенсори, за призначенням, по класу точності або по швидкодії, по габаритах і масі, по діапазону допустимих умов застосування, по принципах їх дії і т. д.

За призначенням, наприклад, сенсори часто класифікують на призначені для застосування:

- в тих або інших галузях промисловості (у автомобілебудуванні, авіакосмічній, кораблебудівній, харчовій промисловості ...);
- в сільському господарстві (у тваринництві, рослинництві, при розведенні і лові риби);
- в різних видах техніки, медичних приладах, в наукових дослідженнях, в екології;
- в обслуговуванні населення;
- в спорті, у військовій справі;
- для контролю за якістю продуктів, води;
- для техніки безпеки і охорони об'єктів і т. д.

Сенсори, що використовуються як вимірювальні прилади, класифікують за призначенням залежно від того, які фізичні величини вони вимірюють. Їх прийнято називати " датчиками " (в'язкості, тиску, магнітного поля, потоку, сили, швидкості, температури, кута повороту, електричних величин і тому подібне).

По точності сенсори поділяють на стандартні класи точності, які прийняті в техніці вимірів. Іноді їх розділяють тільки якісно: на високоточні, середній точності і грубі, такі, що зазвичай називаються "індикаторами".

По габаритах і масі розрізняють великі стаціонарні сенсори (наприклад, радіотелескопи), переносні сенсори, портативні ("кишенькові") сенсори і мікросенсори.

По діапазону допустимих умов застосування розрізняють сенсори, придатні для використання,

- тільки в лабораторних умовах,
- в польових умовах або
- в особливих умовах (при дуже низьких або при дуже високих температурах, в морських умовах або під водою, в умовах підвищеної радіації, у вакуумі) і т. д.

Набагато складніше йде справа при спробах класифікації сенсорів за принципом дії. Адже сенсори можуть складатися з багатьох вузлів, кожен з яких може діяти по своїх принципах.

Вибираючи принцип класифікації сенсорів враховується те, що будь-який сенсор, і особливо інтелектуальний сенсор, - це, в першу чергу, інформаційний прилад, який спостерігає з деякого боку навколишній світ і добуває з нього корисну інформацію, необхідну для успішної діяльності всякої саморегулюючої життєздатної системи.

Інформаційна сторона сенсорів не менш важлива і потрібна, як і їх фізична, фізико-хімічна або біохімічна сторона. А за великим рахунком, вона навіть є головною, визначальною. Бо сенсори, власне кажучи, і існують для того, щоб добувати корисну інформацію.

Тому існує доцільність класифікації сенсорів саме за інформаційно-фізичною ознакою, зокрема, по фізичній природі первинних інформаційних сигналів, що виникають в них. Такий принцип класифікації доки є незвичним. Проте він є природним і зрозумілим, якщо розглядати сенсори як інформаційні прилади.

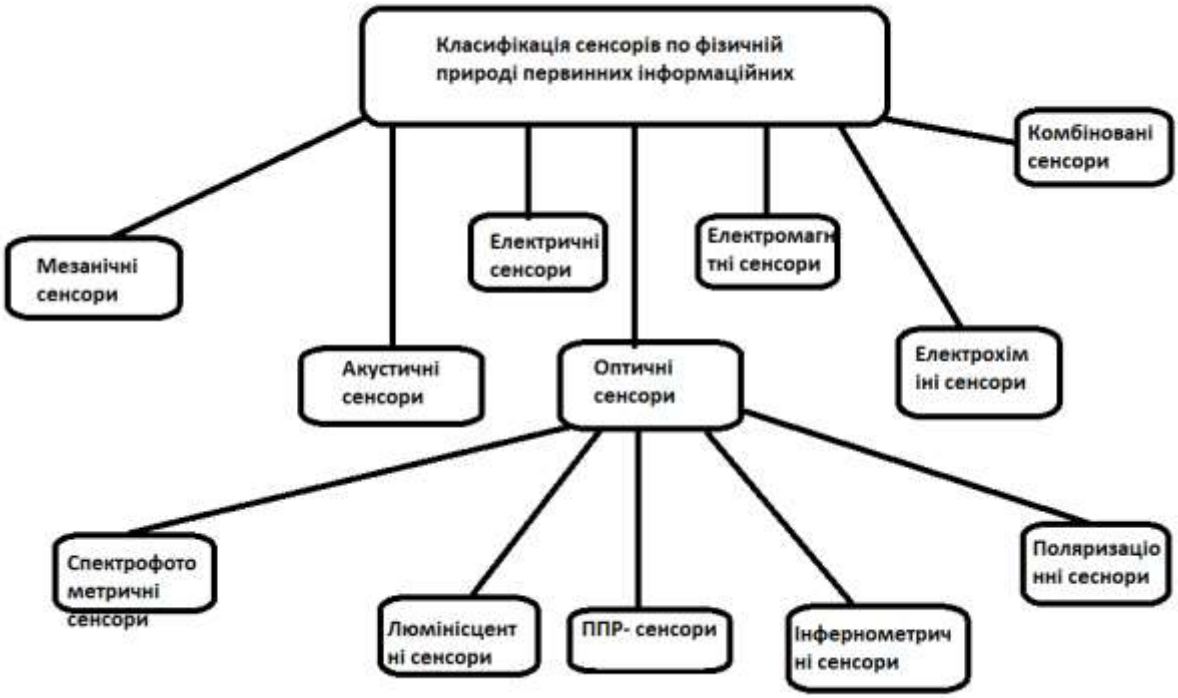


Рис. 6.7. Класифікація сенсорів по фізичній природі первинних інформаційних сигналів

До класу "комбінованих" відносяться сенсори, в яких формуються і використовуються одночасно декілька різних первинних інформаційних сигналів, що мають різну фізичну природу. Наприклад, в тонометрі первинні інформаційні сигнали, що поступають через стетоскоп у вуха лікаря, є акустичними. Але паралельно лікар дивиться на манометр і прочитує з нього величину тиску. Цей сигнал має вигляд механічного переміщення стрілки, тобто по фізичній природі є механічним.

Інший приклад - *магнітокардіографи.* У них первинними інформаційними сигналами є обумовлені роботою серця невеликі зміни магнітних потоків, що сприймаються надпровідними інтерферометрами, а також синхронні зміни електричних потенціалів на поверхні тіла.

Чутливим елементом *рівня (ватерпаса)* - сенсора малих відхилень від горизонтального положення плоскої поверхні - являється бульбашка повітря, плаваюча під прозорим віконцем на поверхні води. Під дією виштовхуючої сили (сили Архімеда) бульбашка завжди займає саме верхнє положення. І тому, якщо поверхня, на якій встановлений рівень, нахиляється по відношенню до горизонтальної площини, то бульбашка повітря переміщається. Сигналізатором є нанесена на віконце рівня шкала кутових нахилів, а первинним інформаційним сигналом - переміщення бульбашки повітря відносно шкали. Тому і цей сенсор ми відносимо до класу механічних.

Простий компас - сенсор для точного орієнтування на місцевості - зазвичай відносять до класу "магнітних" з тієї причини, що він реагує на магнітне поле Землі, і його стрілка встановлюється уздовж силових ліній цього поля. Проте первинним інформаційним сигналом в нім є поворот магнітної стрілки, тобто механічне кутове переміщення. Тому по нашій класифікації компас відноситься теж до класу механічних сенсорів.

До класу механічних слід віднести і *медичні ртутні термометри* - сенсори температури тіла. Адже первинним інформаційним сигналом в них є подовження ртутного стовпчика, тобто *механічне переміщення*.

Електрокардіографи, безумовно, відносяться до класу електричних сенсорів, оскільки первинними інформаційними сигналами в них є зміни електричних потенціалів в різних точках на поверхні грудної клітки. При подальшій візуалізації електрокардіограми за допомогою самописця або на екрані електронно-променевої трубки сигнали ці перетворюються на механічні відхилення пера самописця або електронного променя. Лікар

же сприймає їх очима у вигляді оптичних сигналів. Тобто, фізична природа сигналів потім може змінюватися. Але для класифікації важлива фізична природа саме первинних інформаційних сигналів.

У *тонометрах* - сенсорах для визначення артеріального тиску крові - первинним інформаційним сигналом є *акустичні коливання*, викликані пульсаціями тиску артеріальної крові. Тому тонометри можна віднести до класу *акустичних сенсорів*.

Проте, якщо враховувати те, що рівноправним первинним інформаційним сигналом є в них ще і механічне переміщення стрілки манометра, то тонометри слід віднести до класу комбінованих сенсорів - *акустомеханічних*.

Магніторезонансний томограф. Первинними інформаційними сигналами є в ньому електромагнітні сигнали характерних частот, викликані "спіновою луною", - що триває ще деякий час прецесією спінів ядер після виключення збудливого електромагнітного поля. Тому магніторезонансний томограф в такій класифікації відноситься до *електромагнітних сенсорів*.

6.5. Види механічних сенсорів

У механічних сенсорах первинні сигнали про стан досліджуваного об'єкту або процесу мають механічну природу.

Це можуть бути:

- зміна форми і/або розмірів тіл;
- зміна їх взаємного розташування, тобто механічне переміщення;
- зміна швидкості руху;
- виникнення прискорень;
- зміна амплітуди, фази або частоти механічних коливань і тому подібне.

Відповідно є сенс підрозділяти механічні сенсори з урахуванням фізичної природи чутливих елементів і первинних інформаційних сигналів, які в них виникають, на наступні види:

- деформаційні сенсори, первинними сигналами в яких є зміни форми, об'єму або розмірів чутливого елементу;
- сенсори лінійного переміщення, первинним сигналом в яких є переміщення центру маси тіла в просторі;
- сенсори кутового переміщення, первинними сигналами в яких є нахил тіла, поворот, обертання;
- акселерометри, в яких первинним сигналом є виникнення механічного прискорення;
- вібраційні сенсори, в яких первинним сигналом є зміна стану механічних коливань тіла або системи тіл;
- хроматографічні сенсори, первинні сигнали в яких з'являються внаслідок механічного переміщення молекул (рідини, газу) крізь пористе середовище.

На першому етапі технологічного розвитку людства переважна більшість сенсорів були механічними. Відхилення від вертикалі визначали за допомогою схилів, від горизонталі - за допомогою ватерпаса або просто налитої в чашу рідини, напрям вітру - по повороту флюгера або по направленню поширення диму з димарів і тому подібне.

Згідно систематизації схил і флюгер є сенсорами кутового, а ватерпас - сенсором лінійного переміщення. Навіть хід часу вимірювали механічними сенсорами: по спостережуваному руху сонця, місяця або зірок на небозводі, по переміщенню тіні на сонячному годиннику (усе це - сенсори кутового переміщення), по витіканню води або висипанню піску з посудини через вузький отвір (це - сенсори лінійного переміщення) і тому подібне.

Пізніше стали користуватися механічними маятниковими годинами. Термометри теж довго були тільки механічними, оскільки в них використовувалося явище теплового розширення тіл, і температуру визначали по механічному переміщенню стовпчика рідини у вузькому капілярі.

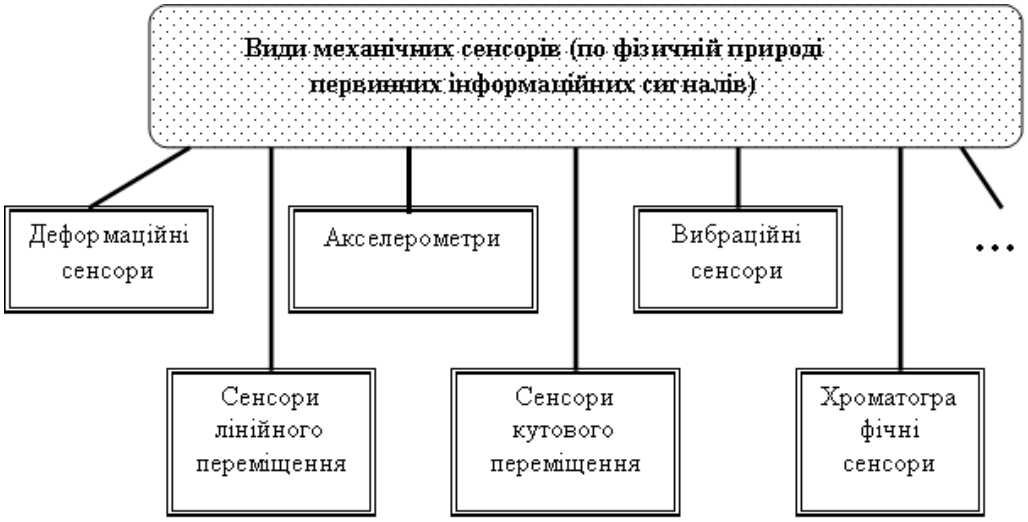


Рис. 6.8. Види механічних сенсорів

Механічним сенсором є, наприклад, і компас.

Останні два приклади наочно демонструють різницю між можливими підходами до класифікації сенсорів.

Якщо їх класифікувати *за призначенням* або *за вимірюваною фізичною величиною*, то звичайний ртутний або спиртовий термометри є температурними сенсорами, а компас - магнітним сенсором.

Якщо ж класифікувати *по фізичній природі первинних сигналів*, які виникають в сенсорі, то обидва названі види сенсорів є механічними: в термометрах первинним сигналом є подовження стовпчика рідини (сенсор лінійного переміщення), в компасі - механічний поворот магнітної стрілки (сенсор кутового переміщення).

6.6. Мікросистемні технології

Новий етап в розвитку механічних сенсорів почався в 90-х роках XX століття з розробкою і освоєнням ***мікросистемних технологій (МСТ).***

Мікросистемні технології - це технології групового виготовлення мікромеханічних деталей і пристроїв разом з електричними вузлами для їх живлення, управління і електронними мікросхемами для обробки інформації.

З цією метою були використані що існували і розвинені нові групові технологічні операції і процеси мікроелектроніки з інтеграцією знань і методів точної механіки і вимірювальної техніки.

Створені системи автоматизованого проектування мікроелектромеханічних інтегральних виробів і цілих систем на кристалі, які дозволяють істотно скоротити терміни розробки виробів, оптимізувати їх конструкцію і технологію виготовлення.

Назви групових технологічних операцій, які входять до складу МСТ :

- фотолітографія (варіанти - звичайна з використанням видимого світла, ультрафіолетова, рентгенівська, електронна і іонна літографії);
- відмивання, очищення;
- протравлення (хімічне, плазмохімічне, електрохімічне, іонне, анізотропне);
- напилення (вакуумне термічне, іонне, плазмове, магнітронне і тому подібне);
- намазування, пульверизація, наплавлення;
- епітаксія - гальванічне або хімічне осадження;
- окислення;
- легування (дифузія, іонна імплантація і тому подібне).

Мікросистемні "високі технології" розвивають нині вже сотні лабораторій, університетів, науково-дослідних інститутів і промислових фірм у всьому світі. Деякі з

опублікованих в Інтернеті прикладів розробок однієї з них - американської лабораторії *Sandia National Laboratories* (*http://mems.sandia.gov/scripts/images.asp*)

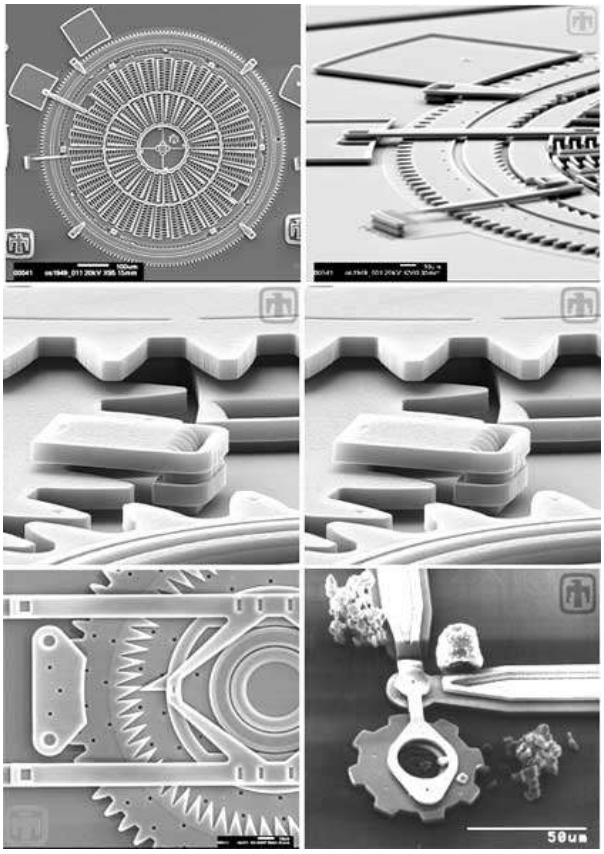


Рис. 6.9. Розробки американської лабораторії *Sandia National Laboratories*

Ліворуч згори - загальне зображення механізму храпового колеса діаметром усього лише 0,8 мм, виготовленого за допомогою МСТ.

Ліворуч внизу показаний увесь приводний механізм мікродвигуна із зубцями заввишки по 10 мкм, на інших фотознімках - різні деталі таких конструкцій при більшому збільшенні.

Справа внизу на тлі таких деталей для порівняння сфотографовані еритроцити і інші клітини крові людини. Відповідні технології називають "мікросистемними" тому, що вони дозволяють формувати на одній підкладці як мікроелектронні, так і оптичні, оптоелектронні, мікромеханічні, електрохімічні та ін. пристрою, створюючи досить складні системи, які прийнято називати *МЕМС* (мікроелектромеханічні системи, - *Microelektromechanical Systems)* [8].

У США, наприклад, за допомогою таких технологій створений прекрасно функціонуючий мініатюрний літак масою до 80 г (разом з паливом), призначений для проведення дистанційних відеоспостережень з висоти пташиного польоту.

Літак цей має розмах крил 15 см, розвиває швидкість до 70 км/год, несе на собі 2 відеокамери масою по 2 г кожна з електронікою, яка забезпечує радіопередачу відеозображень на відстань до 2 км. Тривалість автономного польоту, обумовлена запасом палива, може скласти до 30 хв.

Мікросистемні технології є "високою технологією", тобто складними, прецизійними, наукомісткими, вимагають для свого здійснення застосування дорогого високоточного устаткування, високочистого виробничого середовища, найвищої культури виробництва. Але завдяки тому, що тисячі або навіть мільйони компонентів виготовляють одночасно, в єдиному груповому технологічному процесі, - завдяки цьому вироби мають прийнятну вартість при дуже високих технічних характеристиках.

6.7. Деформаційні інтелектуальні сенсори

Найбільш відомими деформаційними чутливими елементами є деформаційні чутливі елементи для виміру температури, сили і тиску. У виробничих умовах для стеження за температурою з метою її регулювання перевагу зазвичай віддають біметалічним чутливим елементам. Вони є біметалічними смужками, які складаються з двох міцно сполучених між собою шарів металів з температурними коефіцієнтами лінійного розширення (ТКЛР), що істотно відрізняються.

При підвищенні температури один з металів подовжується більше, інший - менше. В результаті біметалічна смужка вигинається у бік металу з меншим ТКЛР.

З'являється первинний сенсорний сигнал - зміна вигину, що означає "зміну температури". Так в даному випадку "народжується" інформація.

Далі деформаційний сигнал можна використати різними способами.

У термостатах і автоматичних регуляторах температури з електронагрівачами вигинання біметалічної пластини використовують безпосередньо для автоматичного замикання або розмикання електричного ланцюга, через який електрична потужність подається в нагрівач. Досягши заданої температури величина вигину досягає такої міри, що електричний ланцюг нагрівача автоматично розмикається, і подальше нагрівання припиняється. Налаштування на потрібну температуру здійснюється регулюванням взаємного положення контактів. Коли температура знижується, то вигин біметалічної пластини зменшується, і контакт знову автоматично замикається. Виділення тепла в нагрівачі поновлюється, падіння температури припиняється, і вона знову починає підвищуватися. Біметалічна пластина виконує в даному випадку функції не лише чутливого елементу, але і *актуатора*.

Актуатор - це пристрій, який активно реагує на поданий сигнал, здійснюючи якусь дію.

У цьому прикладі біметалічна пластина-актуатор замикає або розмикає електричний ланцюг. Промислово випускаються відносно дешеві відрегульовані біметалічні термореле, які можуть пропускати і комутувати електричний струм силою до 16А, забезпечуючи точність регулювання температури 3-10 ^{0}С. Один з таких регуляторів - термореле ТК- 52 - показаний на рис. 6.10 а.

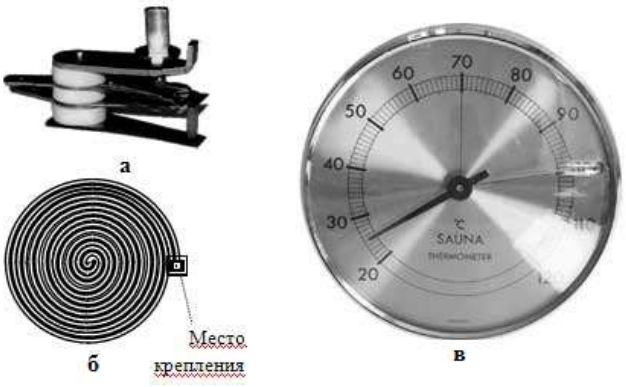


Рис. 6.10. Актуатор

а) Біметалічне термореле ТК- 52;
б) до пояснення принципу дії біметалічної спіралі;
в) зовнішній вигляд спірального біметалічного термометра "Сауна"

Вигинання біметалічної пластини можна використати не лише для комутації електричних ланцюгів, але і засобами точної механіки перетворити далі, наприклад, у відхилення стрілки на циферблаті з температурною шкалою. Щоб підвищити чутливість такого термометра і одночасно спростити і здешевити його конструкцію, застосовують біметалічні спіралі з великою кількістю витків (рис. 6.10 б). Така плоска спіраль з

підвищенням температури розкручується, а при зниженні - скручується значно більше, чим окрема смужка.

При вимірах тиску рідини або газу в якості чутливих елементів часто використовують механічні пристрої, які деформуються під дією тиску. Найбільш споживані з них - трубки Бурдона, сильфони і пружні мембрани - показані на рисунку. Принципи їх дії пояснюють рис. 6.10 (а, б, в).

Механічні деформаційні елементи, чутливі до тиску: *а* і *г* - трубка Бурдона; *б* і *д* - сільфон*; в* - мембрана (рис.6.11).

Рис. 6.11. Механічні деформаційні елементи, чутливі до тиску

Трубка Бурдона (рис. 6.11 *а*) - це порожня усередині пружна трубка з овальним або прямокутним (але тільки не круговим) перерізом, зігнута в кільце. Вільний кінець трубки герметично закритий, а інший кінець механічно закріплений і сполучений з об'ємом, в якому вимірюється тиск. Коли тиск усередині трубки перевищує зовнішній тиск, то воно розпинає трубку, вона починає розкручуватися - тим більше, чим більше вимірювана різниця тисків.

Цей принцип ще в 1848 р. винайшов французький вчений Э. Бурдон, на честь якого і названа трубка. Принцип цей використовується і у відомій дитячій іграшці - скрученій гумовій або паперовій "мові", яка при надуванні розкручується, значно подовжуючись. Рух вільного кінця трубки через відповідний механізм передається на стрілку (для оптичного прочитування) або на повзунок потенціометра або конденсатора змінної місткості (для перетворення на електричний сигнал). Одна з можливих конструкцій манометра показана на рис. Тут 1 - вільний кінець трубки Бурдону, 2 і 3 – передатний механізм, 4 - стрілка, 5 - шкала тисків.

Для розширення діапазону вимірюваних тисків і підвищення точності вимірів часто використовують не один виток трубки Бурдону, а 10-30 витків, згорнутих в спіраль. При цьому вдається перекрити діапазон тисків від 1 Па до 105 Па і забезпечити точність вимірювань від 4% до 0,1%.

Сільфон - це еластична гофрована трубка, усередині і ззовні якою створюються різні тиски: одно з них - вимірюване, інше - опорне. Чим більше перевищення тиску усередині над тиском ззовні сільфону, тим більше він розтягується. Завдяки гофрованим складкам деформація сільфону не призводить до втрати герметичності. До рухливого торця сільфону прикріплюють шток, який перетворює деформацію сільфону на лінійне переміщення. Сильфони частіше застосовують в сенсорах диференціального тиску. Іноді їх використовують також і як деформаційний чутливий елемент, що реагує на прикладену силу. Для цього в недорогих вагах і динамометрах сільфон герметично закривається з обох боків.

Для виміру ваги і сили часто використовують і інший деформаційний чутливий елемент - пружину. Пружини в якості чутливого елементу використовують зазвичай лише в межах лінійної пружної деформації, коли виконується відомий закон Гуку :

$$\Delta l = kFl ,$$

де k – коефіцієнт пружності, F – прикладена сила, l – *довжина* ненавантаженої *пружини*, Δl – величина розтягнення або стиснення *пружини*.

Мембрана - тонка пружна гнучка перегородка між двома об'ємами з різним тиском. Мембрана вигинається у бік об'єму з меншим тиском, причому її переміщення тим більше, чим більше різниці тисків. Діапазон вимірюваної різниці тисків залежить від коефіцієнта пружності мембрани. До місця найбільшого прогину кріплять шток, який перетворює деформаційний сигнал на лінійне переміщення і приводить в дію механізм відліку диференціального тиску [9].

Спектр деформаційних чутливих елементів не вичерпується лише контролем і виміром температури і тиску. Їх застосовують, наприклад, також для контролю і виміру крутильних моментів. В цьому випадку використовується пружна деформація кручення. В якості чутливого елементу часто використовують кварцеві волоски. (досліди П.Н. Лебедєва (Москва, 1900 р.) по виміру найменшого тиску світла. Винайдений ним сенсор складався з якнайлегших "крилець" 1, виготовлених з тонкої слюди і підвішених на тонкій нитці 2 з плавленого кварцу (рис. 6.12).

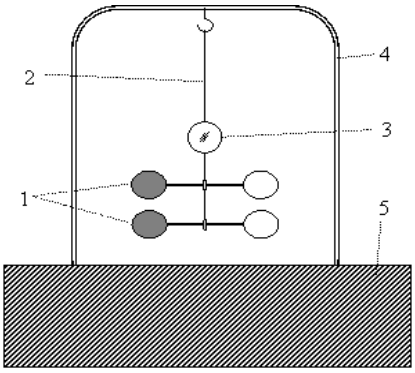


Рис. 6.12. Принцип дії сенсора світлового тиску П.Н. Лебедева

1 - "крильця"; 2 - кварцевий волосок; 3 - люстерко; 4 - скляний вакуумний ковпак; 5 - захищена від вібрацій станина

Одна із слюдяних пластинок була прозорою або дзеркальною, друга - зачорнена. Коли на крильця падало яскраве світло, його тиск на різні половинки крилець був різним. В результаті нитка закручувалася на кут, при якому виникаючий момент сили пружності точно компенсував момент, що крутить, створюється світловим тиском. Для виміру дуже малих крутильних деформацій на нитці зміцнювалося також легке люстерко 3. При його повороті відбитий світловий "зайчик" переміщався. І на досить великих відстанях від люстерка переміщення "зайчика" можна було точно вимірювати. Щоб виключити вплив рухів повітря, нитка 2 підвішувалася під скляним ковпаком 4, усередині якого створювався вакуум. А для виключення перешкод від вібрацій ковпак 4 встановлювався на важкій станині 5, добре захищеною від вібрацій.

Об'єктом спостереження в цьому сенсорі є світловий потік, що падає на крильця 1. Первинний сигнал деформації скручування нитки 2 посилюється за допомогою люстерка 3 і перетворюється на сигнал лінійного переміщення відбитого від нього світлового "зайчика". Величина переміщення прочитувалася фізиком-експериментатором. Тепер цю роботу може автоматично виконувати лінійка фотоприймачів.

На рис. 6.13. показаний принцип дії деформаційного чутливого елементу для контролю і виміру ще однієї величини - швидкості течії. У потоці рідини або газу 1 на кулясту мішень 2 діє сила, пропорційна квадрату швидкості потоку. Мішень кріпиться до гнучкої пружної "ніжки" 3, другий кінець якої прикріплений до нерухомої опори 5. Чим більше швидкості потоку, тим більше вигинається ніжка. Цей первинний сигнал деформації перетворюється на електричний сигнал за допомогою вбудованих в ніжку тензорезисторів 4. На один з тензорезисторів діє те, що стискає, а на іншій - розтягуюче зусилля. Електричні сигнали передаються назовні через провідники, пропущені усередині тіла "ніжки".

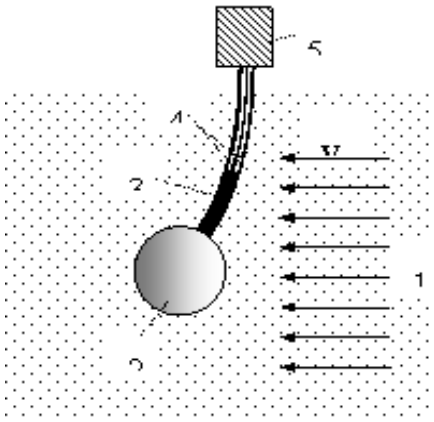


Рис. 6.13. Деформаційний елемент для контролю швидкості течії

Подібний принцип використали вже і наші предки, які "на око" оцінювали швидкість вітру за величиною вигину пружних стволів дерев. Чутливі елементи, що використовують пружну деформацію кручення або вигину, застосовують теж лише в межах їх пружної деформації, зазвичай навіть - в межах лінійної деформації, коли величина деформації пропорційна докладеному зусиллю.

При застосуванні мікросистемних технологій з усіх перелічених вище деформаційних елементів найпростіше реалізувати мембрани. Їм зазвичай і віддають перевагу. Безпосередньо у кремнієвій мембрані формують і кремнієві тензорезистори, які перетворять механічну деформацію в електричні сигнали. Поряд з мініатюрною мембраною в тому ж кристалі кремнію формують також і мікросхеми, потрібні для прочитування і електронної обробки сигналів.

Таким чином створюють, наприклад, мініатюрні датчики тиску повітря в автомобільних шинах (рис. 6.14 ліворуч). Їх розміщують усередині кожної шини біля її штуцера так, щоб вони не заважали експлуатації шин, їх обертанню, монтажу, демонтажу, балансуванню.

Інформація з сенсорів передається в центральний блок індикації і сигналізації (рис. 6.14 праворуч) безконтактним способом із застосуванням локального мікрохвильового радіозв'язку.

Рис. 6.14. Система контролю тиску і температури в шинах автомобілів

Ліворуч - мікроелектронний сенсор тиску і температури повітря в автомобільних шинах. Маса 32 р. Термін служби батареї 5 років. Праворуч - центральний блок індикації і сигналізації.

Кожен датчик має свій індивідуальний код, тому від кожного з них незалежно приймається своя інформація. Центральний блок з мікрокомп'ютером розміщується в кабіні водія і є інтелектуальною частиною сенсора. На його індикаторі показаний умовний вигляд автомобіля зверху з розташуванням усіх шин і відображаються виміряні значення температури і тиску в кожній шині. Необхідна періодичність і порядок перевірки, бажані одиниці виміру температури і тиску (градуси Цельсія або Фаренгейта, одиниці тиску) і критичні значення параметрів задає користувач. У разі виходу контрольованих параметрів за задані безпечні межі видається світлова і звукова сигналізація.

Наступним прикладом компактного портативного інтелектуального сенсора з деформаційними чутливими елементами, виготовленими із застосуванням МСТ, може бути і прецизійний цифровий манометр тиску DPI 740, показаний на рис. 6.15 і розрахований на застосування як в лабораторних, так і в польових умовах. З його допомогою можна вимірювати атмосферний тиск від 0,75 панів до 1,25 панів і абсолютний тиск будь-якого хімічно неагресивного газу в діапазонах від 3 кПа до 130 кПа, до 250 кПа і до 360 кПа.

Рис. 6.15. Прецизійний цифровий манометр тиску DPI 740

Наступний приклад - це портативні цифрові калібратори тиски РМ110. Вони призначені для перевірки і калібрування засобів виміру тиску (візуальних і записуючих манометрів, реле тиску і тому подібне). Для цього, окрім цифрового манометра, до складу калібратора входить також ручний насос з точним регулюванням тиску. Пневматичний ручний насос дозволяє створювати і регулювати тиск до 2 МПа, гідравлічний ручний насос - до 20 МПа. До складу сенсора входить також вимірник температури, який потрібний для точної термокомпенсації погрішностей виміру тиску. Калібратор здатний фіксувати не лише статичний тиск, але і короткочасні скачки тиску тривалістю від 50 мс. Є вбудована пам'ять і інтерфейс RS232.

Рис. 6.16. Портативні цифрові калібратори тиску РМ110L і РМ110Н.

Розмір цифрового манометра 98х92х33 мм, маса 0,5 кг Діапазон робочих температур від - 10 З до +50 С. Клас точності 0,05 %. Довготривала стабільність 0,01% за рік.

6.8. Принципи роботи глобальної системи орієнтування

Основою цієї системи, її "космічної складової", є сукупність 28 штучних супутників Землі, які обертаються навколо нашої планети на висоті близько 20 тис. км в семи різних площинах по 4 супутники на кожній. Період їх звернення складає приблизно 12 годин. Ці навігаційні супутники кілька разів в секунду передають радіосигнали з інформацією про свої точні координати і теперішній момент часу. Параметри орбіт розраховані так, що у будь-який момент часу з будь-якої точки на поверхні Землі видно від 5 до 12 супутників. Для роботи системи досить було б бачити 4 супутники і мати в цілому 24 супутники. Додаткові видимі супутники значно підвищують надійність роботи системи і точність визначення координат.

Сукупність навігаційних супутників GPS образно називають "сузір'ям, штучно створеною людиною". Система GPS була розроблена за замовленням Міністерства оборони США спочатку виключно для військових застосувань. В цілому на її створення витрачені близько 12 млрд. доларів США і декілька десятиліть часу. Перший супутник цієї системи був запущений в 1978 році. З 1989 року стали запускати навігаційні супутники нового покоління. І лише з середини 90-х років XX ст. система запрацювала в повну силу. Нині космічна складова системи GPS як і раніше підтримується Міністерством оборони США, хоча з 2000 р. вона відкрита і для цивільного використання.

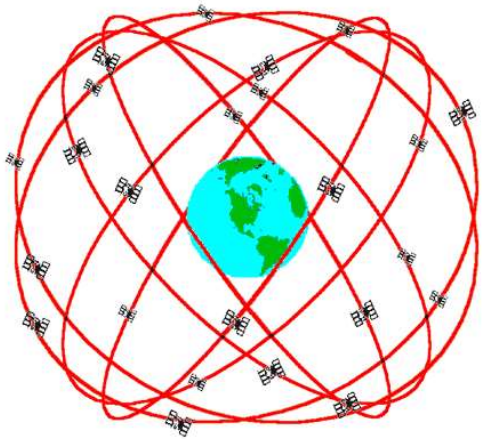


Рис. 6.17. Схема розташування орбіт штучних супутників Землі, які входять в систему GPS. Кожен розрахований на 10 років роботи.

На кожному навігаційному супутнику встановлений високоточний еталонний годинник (для надійності навіть по два годинника різних типів). За синхронізацією і точністю ходу усього годинника на супутниках GPS і за стабільністю їх орбіт невпинно стежить мережа контрольно-вимірювальних станцій, розташованих по усій земній кулі.

На кожному супутнику розміщені також комп'ютер, що розраховує його точні координати у момент посилки радіосигналу, і радіопередавач, працюючий в діапазоні частот вище за 1 ГГц. У нових моделях навігаційних супутників є також і двигун для точного коригування орбіти. Через досить короткі проміжки часу супутник передає в ефір в передбаченому форматі свій номер, свідчення свого годинника і свої поточні координати.

В якості системи відліку GPS узяті загальноприйняті географічна довгота і широта, висота над рівнем моря і так званий "час GPS" - час по еталонному годиннику [10].

Завдяки наявності такої системи супутників завдання точного визначення географічних координат об'єктів на земній кулі значно спростилося. Для цього досить мати при собі відповідний інтелектуальний сенсор - так званий " GPS- приймач " (чи " GPS- ресівер"). До його складу входять багатоканальний приймач радіосигналів від супутників GPS, мікропроцесор і точний власний годинник, який відлічує час GPS. Звичайно, щоб задовольнити вимоги мобільності, портативності і прийнятної вартості, години ці простіше і не так точні, як використовувані на супутниках. Тому їх невелика часова поправка

розглядається теж як одна з невідомих величин. Отримавши сигнали від 4-х супутників GPS, мікропроцесор визначає часи запізнювання кожного з сигналів, обчислює відповідну відстань до кожного супутника і вирішує систему з 4-х рівнянь алгебри з чотирма невідомими: три просторові координати GPS-приймача і часова поправка його годинника. Вичислені координати видаються користувачеві. Якщо приймаються сигнали більш ніж від 4-х супутників, то і число рівнянь виявляється більше за 4, що дозволяє значно зменшити погрішність обчислень, використовуючи алгоритми мінімізації середньоквадратичного відхилення. GPS-приймачі масового користування забезпечують погрішність визначення своїх географічних координат в межах 10-20 м, а високоточні GPS-приймачі для геодезичних вимірів - не більше декількох сантиметрів.

Сенсори GPS

Описані GPS-приймачі - це інтелектуальні сенсори, первинним сигналом для яких є просторове положення самого приймача в системі координат GPS.

Адже саме воно визначає часи запізнювання радіосигналів від навігаційних супутників. Т.е. по фізичній природі первинного сигналу GPS-приймачі є механічними сенсорами. А ось за принципом дії їх часто відносять до електромагнітних сенсорів.

Подальшим істотним їх розвитком є "GPS навігатори". Це спеціалізований навігаційний прилад, який забезпечує орієнтацію в незнайомій місцевості, допомагає планувати найкращі маршрути руху, вибирати орієнтири, запам'ятовує важливу для Вас інформацію про маршрут і т. д.

Разом з GPS приймачем, до його складу входять також кольоровий дисплей і пам'ять з картографічною інформацією. Можна виділити таких 3 групи GPS навігаторів: портативні (кишенькові), автомобільні і професійні.

Рис. 6.18. GPS навігатори

Ліворуч на рис.6.18 показаний приклад кишенькового GPS навігатора. Такі навігатори зазвичай мають невеликі габарити і масу, водонепроникний, стійкий проти ударів корпус і розраховані на туристів, рибалок, геологів, мандрівників, мисливців, грибників і інших масових користувачів. Кольоровий дисплей в таких навігаторах невеликий, але все таки достатній для виведення на нього GPS карти місцевості. Для зберігання картографічної інформації застосовують флэш-память з картографічною інформацією про потрібний Вам регіон, яку потрібно придбавати окремо. Якщо вона є, то GPS навігатор після автоматичного визначення своїх географічних координат виведе на екран дисплея карту ділянки місцевості, що оточує цей географічний пункт, в заданому Вами масштабі. На карті буде вказано місце Вашого перебування і найпримітніші орієнтири на місцевості, якщо такі є. За Вашою вказівкою GPS навігатор може запам'ятати і показати на карті увесь Ваш маршрут з відмітками часу, зафіксувати координати

Автомобільні GPS навігатори істотно більші, мають більший розмір екрану (рис.6.18 праворуч), розміщуються на панелі управління автомобілем. Їх картографічні можливості значно розширені: є багатий набір масштабів карти, вказується цінна для автомобілістів інформація про розміщення стоянок, автоінспекцій, станцій заправки пальним, обмежень швидкості і тому подібне.

Дисплей, як правило, сенсорний, є засоби голосових підказок. Діють програми прокладення альтернативних і розрахунку оптимальних маршрутів. Вимірюючи доплерівські зрушення частоти сигналів від супутників, автомобільний навігатор може вичислити напрям і швидкість руху автомобіля і вивести ці дані на дисплей, своєчасно сигналізувати водієві про небезпеку перевищення гранично допустимої швидкості.

Професійні GPS навігатори використовуються в авіації, на океанських, морських і річкових судах, локомотивах, автобусах, на великих вантажних автомобілях далекого дотримання. Окрім вказаних вже вище за функції, вони також підтримують постійний радіозв'язок зі своїми диспетчерськими пунктами, не завантажуючи екіпаж, збирають і автоматично передають диспетчерам інформацію від деяких важливих сенсорів. Завдяки цьому диспетчери мають оперативну і повну інформацію про стан усієї своєї транспортної мережі, можуть своєчасно реагувати на непередбачені ситуації, змінювати і оптимізувати маршрути, мінімізувати риски, порожні пробіги і тому подібне

GPS приймачі дозволили також по-новому вирішити завдання пересування сліпих людей. У складі портативного інтелектуального навігатора для сліпих, який розміщується в рюкзаку людини, GPS приймач обчислює поточні координати. На голові у сліпої людини в спеціальному шоломі розміщені мініатюрні електронний компас і гіроскоп, що визначають напрям повороту голови, 4 маленьких відеокамери і звуковий сигналізатор з передачею звуку на кістці черепа. Уші залишаються вільними, щоб зберегти важливу для орієнтації сліпих можливість добрі чути що відбувається навкруги. Сліпа людина голосом називає пункт призначення, що цікавить його. Мовна програма, налаштована на його голос і на множину з 30-40 можливих пунктів призначення, розшифровує це звукове повідомлення. Далі мікрокомп 'ютер навігатора планує маршрут і починає "вести" сліпого. Він вказує сліпому напрям руху за допомогою імітації звуку дзвінка, витікаючого нібито з того напряму, в якому слід рухатися.

Ще одним важливим застосуванням GPS приймачів стало створення так званих "*трекерів*" - інтелектуальних сенсорів для дистанційного визначення GPS координат людей або предметів, на яких вони встановлені. Сфера їх застосування - це підвищення безпеки і прискорення пошуку дітей, престарілих, хворих на амнезію і інших людей, що втрачають орієнтацію, а також тварин, викрадених автомобілів, цінних вантажів. Один з таких трекерів TR - 102 показаний на рис. У ньому застосовується високочутливий мініатюрний GPS приймач "*SiRF Star III*", який сприймає навіть слабкі відбиті сигнали від навігаційних супутників і здатний визначати GPS координати навіть при значному екрануванні прямих сигналів будівлями, горами і тому подібне. Трекер підтримує прямий мобільний радіотелефонний зв'язок з 10 заздалегідь запрограмованими телефонними номерами. Кожен з цих абонентів у будь-який час може зв'язатися з трекером, відправивши йому SMS запит. Кожен з цих абонентів у будь-який час може зв'язатися з трекером, відправивши йому SMS запит. І трекер в SMS повідомленні у відповідь передасть свої поточні координати [11].

Якщо у того, що просить є комп'ютер з картографічною програмою, то вона допоможе побачити на екрані монітора карту ділянки місцевості, в якій знаходиться відстежуваний об'єкт, і місце знаходження трекера. На трекерах, призначених для носіння людьми, є кнопка екстреного виклику (SOS), при натисненні на яку трекер відправляє на вказані в його пам'яті 3 телефонні номери сигнал тривоги і SMS сполучення з вказівкою своїх координат. Є також 3 кнопки швидкого з'єднання з цими номерами. У пам'ять трекера можна занести значення тимчасового інтервалу, після закінчення якого трекер відправлятиме SMS повідомлень своїх координат автоматично.

6.9. Сенсори лінійного та кутового переміщення

Сенсори лінійного переміщення

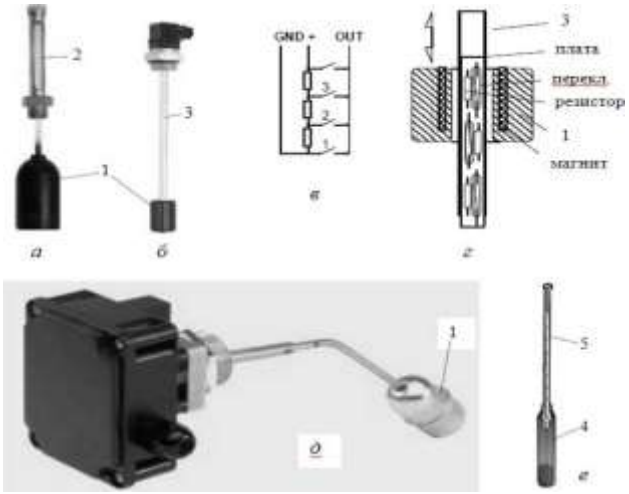


Рис. 6.19. Поплавцеві сенсори: *а* - з візуальним відображенням*; б* - з електричним прочитуванням*; у* - електрична схема*; г* - внутрішня конструкція*; д* - з механічним замиканням*; е* - ареометр

Невеликі постійні магніти розміщені в тілі поплавця. У кожен момент спрацьовує лише той перемикач, який розташовується усередині поплавця і тому схильний до дії магнітів. Опір електричного ланцюга прямо залежить від місця розташування поплавця і, отже, - від рівня рідини.

Ще одна конструкція поплавцевого сенсора показана на рис. 6.19 д. Тут поплавець жорстко прикріплений до одного кінця трубки, протилежний кінець якої закріплений на осі. При підвищенні рівня рідини і спливанні поплавця, трубка обертається навколо осі і при деякому рівні рідини замикає електричний контакт або перекриває отвір, через який тече рідина.

Для виміру щільності рідин часто застосовують ареометри. Ареометр складається з порожнистої скляної, металевої або пластмасової капсули 4 (рис. 6.19 е), до якої прикріплена тонка "шийка" з шкалою 5. Капсулу 4 заповнюють дробом з таким розрахунком, щоб капсула була повністю занурена в контрольовану рідину, але не тонула в ній, а плавала, і частина шийки з шкалою 5 виступала над поверхнею рідини.

Якщо ж щільність рідини зменшиться, то ареометр зануриться в неї глибше. Таким чином, глибина занурення ареометра в рідину однозначно залежить від її щільності. І вертикальне переміщення шийки ареометра відносно поверхні рідини є сигналом зміни щільності рідини. На цьому принципі побудовані і широко застосовуються:

- спиртоміри - ареометри для визначення об'ємного змісту спирту у воді або води в спирті;
- сахароміри - ареометри для визначення вмісту цукру в сиропі;
- солеміри - ареометри для визначення вмісту солі в розсолі;
- кислотоміри - ареометри для визначення змісту кислот в розчині;
- ареометри для визначення щільності молока, морської води, нафти і нафтопродуктів, електролітів і т. д.

Сенсори кутового переміщення

Серед сенсорів кутового переміщення виділяють 2 групи: *сенсори кута нахилу (крену) і сенсори кута повороту.*

Інклінометри

Сенсори кута нахилу називають ще " інклінометрами " (*від латинського incline - нахиляю*). Найчастіше йдеться про кутове відхилення від вертикалі або від горизонтальної площини. Вже найдревніші будівельники використали з цією метою схили, ватерпаси (рис. 6.20 *а, б, в*), пізніше - рівні (рис. 6.20 *в*).

На початку XX століття почали використати ртутні вимикачі, принцип дії яких показаний на рис.6.20 *г*. В герметично закритій капсулі вільно переміщається крапелька ртуті. У капсулу з діелектрика введені 2 металеві електроди. Коли капсула розташована вертикально, крапля ртуті знаходиться в центрі і електрично сполучає ці електроди. Якщо ж капсула і плата, на якій вона закріплена, нахиляються до горизонту на кут, який перевищує критичний, крапля ртуті під дією сили тяжіння зміщується, і електричний контакт розривається, сигналізуючи про небезпечний крен.

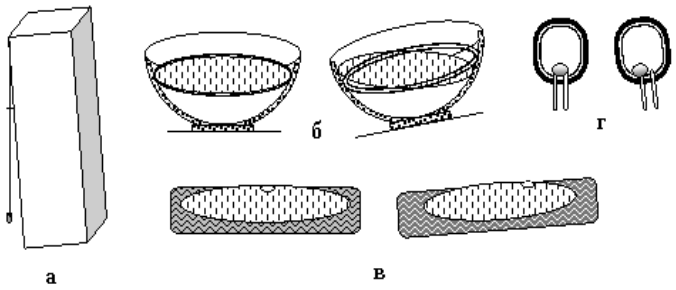


Рис. 6.20. Прості сенсори нахилу : *а* - схил; *б* - ватерпас; *в* - рівень; *г* - ртутний вимикач

За останні десятиліття створені і знайшли широке застосування точніші інклінометри з електричними вихідними сигналами. На рис. 6.21 показаний принцип дії електролітичних інклінометрів.

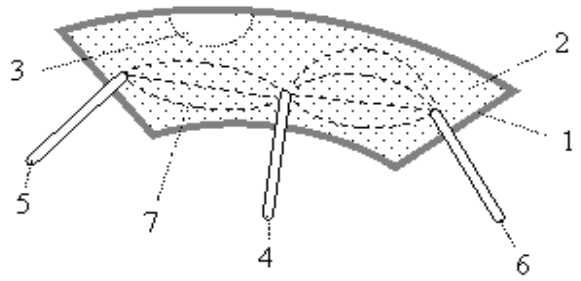


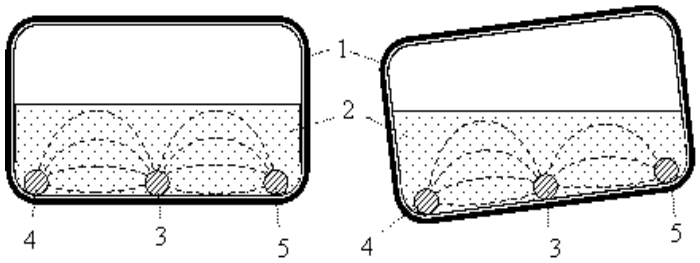
Рис. 6.21. Принцип дії електролітичного інклінометра

У дещо вигнутий герметичний корпус 1, наприклад, з кераміки або скла, залитий рідкий електроліт 2 так, щоб в нім залишилася повітряна бульбашка 3. У корпус введені три електроди: електрод 4 - в центрі, електроди 5 і 6 - на кінцях корпусу. Коли корпус знаходиться точно в горизонтальному положенні, а повітряна бульбашка - над центральним електродом, то електричні опори електроліту між електродами 5 і 4, 4 і 6 однакові.

Ці електричні опори включені в плечі мостової схеми, вихід якої сполучений з операційним підсилювачем. При рівності опорів міст збалансований, і сигнал на виході дорівнює нулю.

Якщо сенсор злегка нахиляється, то повітряна бульбашка зміщується убік. Електричний опір між електродами змінюється. Баланс мостової схеми порушується, і на її виході з'являється сигнал тієї або іншої полярності, величина якого пропорційна куту нахилу. Щоб виключити вплив поляризації електроліту, для балансування мостової схеми і для її живлення використовують змінний струм.

Інший варіант конструкції електролітичного інклінометра показаний на рис. 6.22. Електроди у вигляді тяганини розміщені тут паралельно осі, перпендикулярній до площини малюнка, навколо якої при нахилах обертається сенсор. Рідкий електроліт 2 заповнює корпус 1 лише частково. Коли нахилу немає, електричні опори між центральним електродом 3 і бічними електродами 4, 5 однакові. Ці опори включені в плечі мостової схеми змінного струму. Мостову схему балансують так, щоб напруга на виході дорівнювала нулю. При нахилах сенсора кількість електроліту з одного боку зростає, а з іншою зменшується. Відповідно змінюються і електричні опори. Сигнал на виході мостової схеми і після підсилювача стає тим більшим, чим більше кута нахилу. А його полярність вказує напрям нахилу [12].



Інша конструкція електролітичного інклінометра : 1 - герметичний корпус; 2 - рідкий електроліт; 3 - центральний електрод; 4, 5 - бічні електроди

Рис. 6.22. Конструкція електролітичного інклінометра

Висока точність, невеликі розміри, простота установки на об'єктах зумовили широкий діапазон їх застосування.

Це і контроль за вертикальним положенням висотних споруд, точне визначення напряму буріння нафтових, газових і інших бурових свердловин, визначення ухилу автомобільних доріг, залізничних колій, штреків в шахтах, крену кораблів, автомобілів, будівельних кранів і екскаваторів, вимір деформаційного прогину мостів, опорних балок і тому подібне.

Випускаються не лише прості, але і інтелектуальні інклінометри зі вбудованими мікропроцесорами, які виконують досить широкий набір функцій.

Це можуть бути одно- і двокоординатні інклінометри з цифровим інтерфейсом, з можливістю автоматичного управління запобіжними механізмами, з можливістю завдання користувачем критичних значень кутів нахилу, з видачею попереджувальних сигналів і т. п.

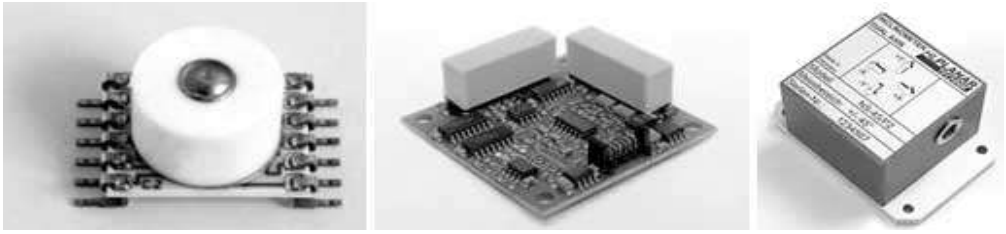


Рис. 6.23. Деякі зразки двокоординатних інтелектуальних інклінометрів фірми *HL* - Planartechnik Gmb

Деякі промислові зразки таких інклинометрів показани на рис. 6.23. Двохкоординатність досягається шляхом використання двох окремих одновісних інклінометрів, зорієнтованих у взаємно перпендикулярних напрямах.

Абсолютні енкодери

Сенсори кута повороту пройшли великий шлях вдосконалення. За багато століть розвитку техніки створені немало різних методів і пристроїв.

Спочатку це були виключно механічні пристрої. У них за допомогою механічних передач кут повороту або кількість виконаних оборотів перетворювалися і відображалися у

вигляді переміщення стрілки уздовж шкали з градусними діленнями або у вигляді числа, що формується в прозорому віконці системою коліщаток, на ободі яких нанесені цифри.

В середині XX століття популярнішими стали магнітні і електричні сенсори кута повороту або кількості оборотів.

Нині для виміру кутів повороту і кількості оборотів все частіше стали використовувати оптоелектронні енкодери. За принципом дії прийнято розрізняти так звані " абсолютні " і "інкрементні“ енкодери.

Абсолютні енкодери видають на свій вихід цифрові коди, які відповідають абсолютному значенню кута повороту відносно положення, прийнятого за нуль.

Принцип дії абсолютного энкодера, розрахованого на один оборот, пояснюється на рис. 6.24. На вал, закріплений на двох прецизійних підшипниках і кінематично сполучений з вузлом, обертання якого контролюється, насаджений кодовий диск.

На останньому виділені кілька кільцевих доріжок з прозорими і непрозорими ділянками. Навпроти доріжок з одного боку диска встановлені світлодіоди з циліндричною лінзою, а з іншого боку - лінійка фотодетекторів, по одному на кожну доріжку. Прозорий і непрозорий ділянки на доріжках підібрані так, щоб кожному кутовому положенню кодового диска відповідав свій унікальний двійковий код на виходах лінійки фотодетекторів.

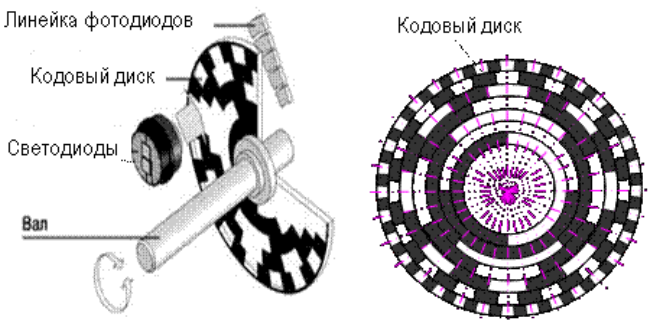


Рис. 6.24. Конструкція абсолютного енкодера

Один з можливих варіантів кодування диска показаний на рис. 6.24 справа. Сфокусований циліндричною лінзою в радіальну риску світло від світлодіодів проектується на кодовий диск. Світло вільно проходить крізь прозорі ділянки доріжок і, потрапивши на відповідні фотодетектори, викликає появу сигналу "1" на виходах відповідних підсилювачів. Крізь непрозорі ділянки доріжок світло не проходить, і на виходах відповідних підсилювачів формуються сигнали "0".

Загальне число можливих n-разрядных двійкових кодів складає 2n. При сучасному стані технології мікроелектроніки це виявляється зовсім недорого. І тому такі енкодери стали дуже популярними. Їх широко застосовують в антенних системах, в астрономії для визначення небесних координат зірок, в геодезичних приладах, в системах кругового спостереження і т. д.

Проте, є багато практичних завдань, коли окрім знання кутового положення в межах одного обороту потрібно реєструвати також кількість повних обертів і їх напрям. Т.е. потрібно визначати кути не в межах від 0◦ до 360◦, а в межах від -∞ до +∞. Для цього нині використовують багатооборотні енкодери, принцип дії яких показаний на рис. За допомогою зубчастих або інших механічних редукторів кут повороту зменшується в потрібну кількість разів, і кодові диски додаткових мір відлічують кількість оборотів в потрібних користувачам межах.

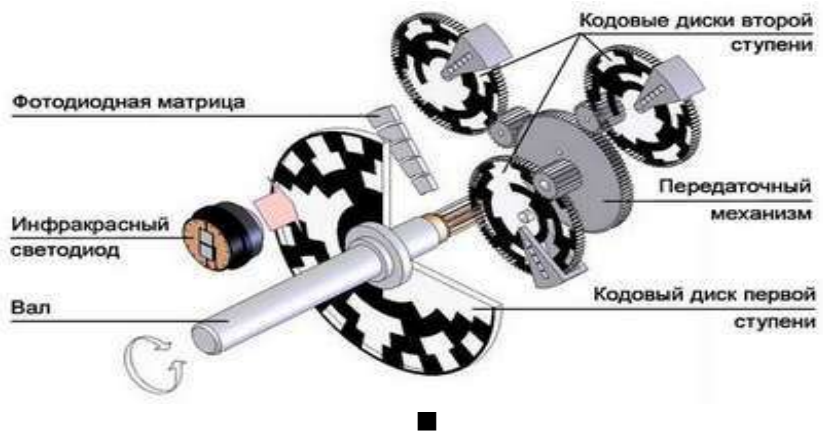


Рис. 6.25. Принцип дії багатооборотного абсолютного енкодера

У абсолютних енкодерах інформація про кутове положення валу зберігається навіть при відключенні живлення, оскільки фіксується фізично положенням кодових дисків. При використанні для кодування положення валу звичайного двійкового коду перехід до сусіднього положення може послужити причиною зміни декількох біт одночасно. Наприклад, при переході від 0111 до 1000 змінюються одночасно 4 біта. Тому поблизу позиції переходу із-за деякої несинхронної зміни розрядів можуть короткочасно видаватися невірні коди.

В інкрементних енкодерах використовують конструкцію, аналогічну показаній на рис.6.25, проте рахунковий диск має, як правило, лише одну доріжку, на якій прозорі і непрозорі ділянки чергуються. І відповідно замість лінійки фотодетекторів використовують лише 1 або 2 фотодетектори - залежно від того, можливе обертання диска лише в одному або в обох напрямах. На рис. 6.26 *а* показано взаємне розташування рахункового диска 1, блоку фотодетекторів 2 і світлового зонду 3 від світлодіода. Якщо диск 1 може обертатися лише в одному напрямі, то досить одного фотодетектора. На виході сенсора формуватиметься послідовність імпульсів з періодом, обернено пропорційним до швидкості обертання диска. Поява наступного імпульсу свідчить про поворот диска на кут 360▫ /*n*, де *n* - кількість пар непрозорих і прозорих ділянок на диску.

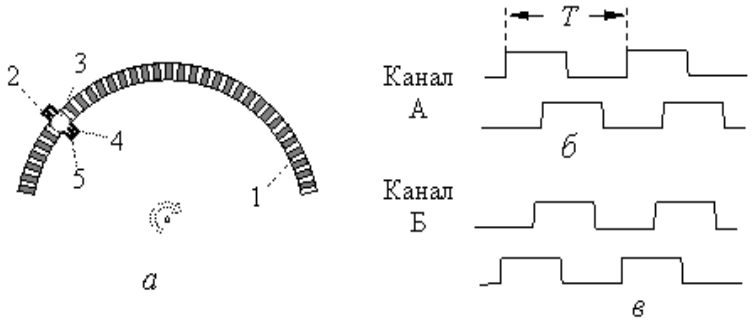


Рис. 6.26. Принцип дії інкрементного енкодера

Якщо диск може обертатися в обох напрямах, і інформація про це важлива, то блок 2 складається з двох фотодетекторів 4 і 5, розміщених уздовж доріжки на відстані менше, ніж ширина прозорої або непрозорої ділянки. Вихід сенсора в цьому випадку є двоканальним. На виході А формуються імпульси від фотодетектора 4, а на виході б - від фотодетектора 5. Якщо диск 1 обертається проти годинникової стрілки, то імпульси на виході А з'являються трохи раніше, ніж імпульси на виході б (рис.6.26 *б*). При обертанні диска за годинниковою стрілкою порядок появи імпульсів - зворотний (рис.6.26 *в*).

Іноді на рахунковому диску роблять додаткове прозоре віконце на сусідній доріжці (одно на усю доріжку) і ставлять ще один фотодетектор, сигнал від якого виводять на додатковий канал синхронізації. Цей канал використовують для фіксації початку відліку і для компенсації погрішностей, які можуть накопичуватися при великому числі оборотів.

Кутові енкодери нині все частіше застосовують спільно з інтелектуальними електронними модулями. Такі сенсори називають "інтелектуальними тахометрами“. На входи такого невеликого пристрою поступає від енкодера послідовність імпульсів, яку в реальному часі швидко обробляє мікропроцесор. Він підраховує загальне число імпульсів, що прийшли від інкрементного енкодера, починаючи від вказаного моменту часу. А знаючи кут повороту, який відповідає одному імпульсу, тахометр миттєво обчислює кутове положення контрольованого об'єкту у будь-який момент часу, може запам'ятовувати усю динаміку обертання із заданою дискретністю [13].

Отримуючи імпульси від двоканальних інкрементних енкодерів, інтелектуальний тахометр при обчисленні поточного кутового положення може враховувати і зміну напряму обертання. По тимчасових інтервалах між вступом імпульсів мікропроцесор може вичислити миттєву кутову швидкість. Він може також визначати середню кутову швидкість за певний інтервал часу, мінімальні і максимальні значення величин і тому подібне, - все, що треба користувачеві.

Роторні і турбінні сенсори

Ще одним прикладом сенсорів, в яких обертання є первинним механічним сигналом, служать роторні і турбінні вимірники об'ємного потоку рідини.

Чутливими елементами в них є лопаті колеса або міні-турбіни. У потоці рідини вони починають обертатися, і кут їх повороту, число оборотів прямо залежать від об'єму рідини, яка протікає через поперечний переріз труби, в якій вони встановлені.

Кут повороту, число оборотів перетворюються потім, як правило, в електричні сигнали за допомогою інтегрованих в конструкцію сенсора оптоелектронних, індуктивних, ємнісних або магніточутливих елементів.

Рис. 6.27. Промислові сенсори для виміру об'ємного потоку рідини
а - турбінний сенсор; б - роторний сенсор; в - сенсор разом з інтелектуальним лічильником "Omni-rr"

На рис. 6.27 вгорі справа показаний роторний сенсор з прозорою кришкою, - щоб був видний принцип його дії. Рідина, поточна крізь сенсор, передає частину свого механічного імпульсу лопатям, внаслідок чого колесо обертається. А вбудована оптоелектронна схема перетворює обертання на послідовність електричних сигналів.

"Інтелектуальну" частину подібних сенсорів випускають у вигляді автономних електронних модулів, які можуть бути розміщені безпосередньо біля сенсора (рис. 6.27 в). Залежно від конструктивного виконання і вживаних матеріалів такі сенсори придатні для виміру потоків води, нафтопродуктів, олій і інш. з температурою до 100 З в діапазоні від 0,025 л/хв до 100 л/хв з точністю від 1% до 5%.

6.10. Інтелектуальні акустичні сенсори

Фізичні основи роботи акустичних сенсорів

У акустичних сенсорах первинні інформаційні сигнали є акустичними. Це, наприклад, звуки живої мови, музика, спів птахів, сигнали ехолокації дельфінів або акустичні сигнали в ультразвуковій діагностиці, поверхневі акустичні хвилі і тому подібне.

Акустичні хвилі - це коливання тиску, що поширюються в повітрі (газах), рідини або в твердому середовищі. Відомо, що акустичні хвилі поширюються значно повільніше, ніж радіохвилі: в повітрі, наприклад, зі швидкістю близько 340 м/с, у воді - близько 1,5 км/з, в твердих тілах - 3-6 км/с. І це має свої позитивні сторони.

По частоті коливань акустичні хвилі підрозділяють на:

- інфразвуки (частота менше 16 Гц);
- звуки (діапазон частот від 16 Гц до 20 кГц), які сприймає людське вухо;
- ультразвуки (від 20 кГц до 1 ГГц);
- гіперзвуки (понад 1 ГГц, аж до 10^{13} Гц).

Інфразвуки у воді можуть поширюватися на сотні кілометрів. Сприймаючи їх, мешканці моря заздалегідь "чують" наближення шторму. Гіперзвуки і ультразвуки сильно розсіюються, поглинаються і тому затухають набагато швидше.

Ультразвукові хвилі по частоті зазвичай ділять на три діапазони:

- низькочастотний (16-100 кГц, довжина хвилі в повітрі 3-20 мм, у воді 15-90 мм);
- середніх частот (0,1-10 Мгц, довжина хвилі в повітрі 0,034-3,4 мм, у воді 0,15-15 мм);
- високочастотний (10-1000 Мгц, довжина хвилі в повітрі 0,34-34 мкм, у воді 1,5-150 мкм).

Акустичні хвилі природного походження, як правило, є складними, несуть з собою коливання різних частот. Їх частотний склад зазвичай характеризують частотно-амплітудним спектром - залежністю інтенсивності або амплітуди коливань від частоти.

Музичні звуки мають в основному дискретний спектр, інші - безперервний спектр. Звукові шуми мають дуже широкий безперервний спектр частот.

Інтенсивність акустичних, як і усіх інших видів хвиль характеризують середньою енергією, переносимою ними за одиницю часу через одиницю площі, перпендикулярної до напряму поширення, і вимірюють у Вт/м^2.

Специфічною характеристикою інтенсивності акустичних хвиль є амплітуда коливань тиску (Па). У області звуків, які чує людина, використовують і логарифмічну міру гучності звуку - так званий "рівень звукового тиску". Його виражають в децибелах (дБ) і обчислюють за формулою

$$N=20\ lg(p/p_0).$$

де p - амплітуда коливань тиску в паскалях, а p_0 - це так званий "поріг чутності", тобто мінімальна амплітуда звукових коливань, які здатне почути людське вухо.

Оскільки акустичні хвилі - це коливання тиску, то для сприйняття їх застосовують елементи, чутливі до швидких коливань зовнішнього тиску.

Як правило, це легкі мембрани або діафрагми, що перетворюють коливання тиску повітря, рідини або твердого тіла в механічні коливання, які, у свою чергу, перетворюються далі на електричні сигнали або в сигнали іншої природи.

Датчики, чутливі до звукових хвиль, що поширюються в повітрі або в газах, зазвичай називають мікрофонами; датчики, чутливі до акустичних хвиль, які поширюються у воді або

в рідинах, - гідрофонами; а датчики акустичних хвиль в твердих тілах, - стетоскопами. Лікарі, наприклад, вже багато століть застосовують механічні стетоскопи для прослуховування звуків усередині грудної клітки людини, скорочень серця, що виникають в результаті, проходження повітря по дихальних шляхах і т.д.

Основними параметрами акустичних датчиків є: частотний і динамічний діапазони, чутливість, диаграмма направленості і амплітудно-частотна характеристика (АЧХ).

Мікрофони

Перші мікрофони були резистивними. Для перетворення механічних коливань в електричний сигнал в них використали вугільний (графітовий) порошок, електричний опір якого зменшувався із зростанням тиску. Потім набір принципів роботи акустичних датчиків значно розширився. Нині використовуються: електростатичні (конденсаторні, ємнісні), волоконно-оптичні, п'єзоелектричні, п'єзорезистивні, електретні і інші типи таких датчиків.

Електретні мікрофони відрізняються тим, що для них не потрібне зовнішнє джерело напруги, оскільки джерелом електричного поля в них є электрет - матеріал з постійною (іноді говорять "замороженій") електричною поляризацією.

Промисловість випускає зараз багато типів високоякісних мікрофонів. Для прикладу на рис. 6.28 показані деякі мікрофони компанії Sanken.

Рис. 6.28. Мікрофони компанії Sanken

Ліворуч - конденсаторний мікрофон CS - 1 масою 100 г і завдовжки 180 мм Завдяки відповідній конструкції приймальної трубки (чутлива мембрана глибоко втоплена, а пластинчата м'яка бічна поверхня трубки глушить звукові коливання, що поступають збоку) цей мікрофон має вузьку діаграму спрямованості в діапазоні частот від 50 Гц до 100 кГц, майже плоску амплітудно-частотну характеристику, високу чутливість (- 30 дБ/Па). Він не спотворює звук, навіть якщо встановити його поряд з джерелом, відмінно працює аж до гучності звуку в 137 дБ. Його використовують у тому числі і для професійного звукозапису найвищої якості.

Нове "дихання" удосконаленню мікрофонів дало застосування мікросистемних технологій. Разом з чутливим до звуку датчиком з'явилася можливість сформувати в тому ж кристалі кремнію і усі електронні схеми, потрібні для посилення, селекції і обробки звукових сигналів. Це привело до зменшення на порядок розмірів, маси і вартості мікрофонів, що дуже важливо для усіх портативних пристроїв. Різко покращали чутливість і інші характеристики мікрофонів, зменшився вплив зовнішніх перешкод і шумів. "MEMS мікрофони", як їх стали називати, вже знайшли широке застосування в портативних відеокамерах, в мобільних телефонах, відеотелефонах.

Фирма Akustica Inc. почала промисловий випуск першою у світі акустичної системи на КМОП кристалі розміром 3,65х3х0,5 мм, виконуючій функції багатьох мікрофонів, електронних блоків і програмного забезпечення. Система перекриває частотний діапазон від 100 Гц до 10 кГц, має чутливість - 40 дБ, споживану потужність - лише 0,4 мВт.

Стетоскопи

У стетоскопах акустичні коливання зовнішньої грані твердого тіла перетворять у відповідні коливання тиску газу або рідини. Вони по звукопровідній трубці передаються на чутливий до акустичних коливань елемент. З метою підвищення чутливості площу контакту стетоскопа з твердим тілом збільшують, а стінки звукопровідної трубки поступово звужують, щоб сконцентрувати акустичні коливання тиску на невеликій площі і збільшити їх амплітуду. Звуження, як правило, робиться за експоненціальним законом.

Тривалий час чутливим елементом стетоскопа було тільки вухо людини. Промисловість продовжує випускати такі стетоскопи і зараз - вже не лише для медичних і ветеринарних, але і для технічних застосувань. Фірма *Draper,* наприклад, випускає стетоскоп D54503, призначений для виявлення (по змінах звукової "картини") дефектів в двигунах, підшипниках і в інших рухливих деталях працюючих машин (http://www.voltra.ru).

Зараз в стетоскопах застосовують вже і "штучне вухо". На рис. 6.29 ліворуч показаний медичний електронний стетоскоп *CADIscope* фірми CADITEC (Швейцарія), який сам через грудну клітку людини сприймає звуки роботи серця, посилює їх і відтворює у вигляді осцилограми на рідкокристалічному дисплеї разом з шкалою і відмітками часу. Таким чином можна виявити і наочно побачити ознаки навіть нечутних вухом хрипів в дихальних шляхах, сердечних аритмій і тахікардії.

Рис. 6.29. Стетоскопи

У разі потреби фонограму роботи дихальних шляхів і серця можна передати на комп'ютер і задокументувати. З комп'ютера її можна передати також на великі відстані через Інтернет і отримати термінову консультацію найдосвідченіших фахівців. На цей же дисплей можна вивести також синхронну електрокардіограму, отриману від електрокардіографа. Це робить електронний стетоскоп дуже цінним медичним інструментом для діагностики захворювань серця.

З використанням вищеописаних приймачів акустичних сигналів будують інтелектуальні акустичні сенсори, у тому числі такі, в яких за допомогою мікропроцесора виконується професійна обробка первинних сигналів і забезпечується зручний сервіс.

Диктофони

Одним з видів таких сенсорів є сучасні диктофони. Ще декілька десятиліть тому акустичні сигнали, які сприймалися мікрофоном, посилювалися і записувалися на магнітну стрічку в магнітофонах. Сучасні диктофони вже не мають рухливих вузлів, і тому їх можна застосовувати в дорозі, в умовах вібрацій, запиленої, в значно ширшому діапазоні температур довкілля. Наявність вбудованого мікропроцесора і програмного забезпечення дозволяє в реальному часі фільтрувати, обробляти, форматувати музику, живу мову і інші звукові послідовності в стандартні звукові файли, організовувати зручні для користувача каталоги цих файлів, інтерфейс із зовнішнім комп'ютером або мережею зв'язку.

Використовуючи флэш-память, можна записувати і зберігати дуже великі об'єми звукових файлів.

Цифровий диктофон SM розрахований на запис звуку на зовнішню флэш-память не лише зі вбудованого в нього мікрофону, але і з телефонної лінії. Запису у вигляді стандартних звукових файлів (в цілому до 1120 хвилин живої мови) можна прослуховувати за допомогою навушника, переносити на комп'ютер. В ході запису диктофон сам автоматично видаляє довгі паузи в мові, що дозволяє ефективно використати пам'ять. Маса цього диктофона тільки 17 г, габаритні розміри 51 х 42 х 11 мм. Літій-поліімерні акумулятори забезпечують 55 годин автономної роботи в режимі запису і до 2,5 місяців роботи в режимі очікування.

Портативний цифровий диктофон *Olympus VN* - 1100 легкий, зручний, має типовий дизайн, дружнє до користувача меню. Забезпечує можливість запису до 17 годин розмови. Записи автоматично датуються і можуть зберігати позначки користувача, легко переносяться в комп'ютер. Можуть відтворюватися, починаючи з будь-якого місця.

Портативні звукоаналізатори

Відколи людство зрозуміло позитивну роль мелодійних звуків і негативний вплив на наше здоров'я шумів і дратівливих надмірно гучних звуків, з'явилася і почала зростати потреба в їх акустичних вимірах. Потреба ця стала особливо актуальною, коли в технічно розвинених країнах світу були ухвалені закони, регулюючі допустимі рівні промислових і побутових шумів. Ще до недавнього часу для вимірів гучності звуку, часу реверберації звуків в приміщеннях, для виявлення і визначення резонансних частот і інших важливих акустичних характеристик приміщень використовувалася складна стаціонарна апаратура. Але зростаюча потреба у вимірах привела до створення відносно недорогих портативних вимірників гучності звуку і інших параметрів звукових коливань.

Портативний аналізатор звуку 2250 фірм *Bruel & Kjaer* є двоканальним. Схема його застосування показана на рис. 6.30 *б.* До входу приєднуються приймачі звуку зі вбудованим передпідсилювачем.

З'єднання може бути як безпосереднім, так і через спеціальний кабель завдовжки в десятки метрів. Аналізатор вийшов дуже зручним і різнобічним помічником для фахівців з акустики. Залежно від закладеного в його мікрокомп'ютер програмного забезпечення, він може використовуватися: як вимірника інтенсивності або гучності звуку; як реєстратор середнього рівня шуму на вулицях міста, в районах аеропортів, на промислових підприємствах в різних частотних діапазонах; для дослідження акустичних властивостей приміщень, концертних залів; для точного налаштування музичних інструментів, для контролю їх якості, пошуку шляхів їх поліпшення.

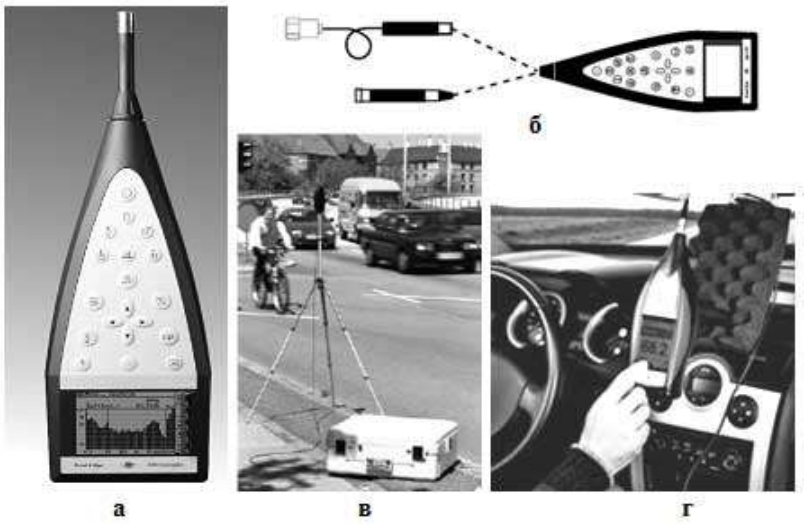


Рис. 6.30. Портативний аналізатор звуку сімейства 2250 фірми *Bruel & Kjaer*

Аналізатор може швидко розкласти звукові коливання в спектр, який виводить на свій рідкокристалічний дисплей. При цьому він може працювати як з тривалими, так і з короткочасними звуками, а також з механічними вібраціями, записуючи їх у свою пам'ять. З його допомогою можна по зміні характеру звуку оперативно виявити збої і порушення в роботі двигунів, машин, швидко знаходити причини неполадок.

На рис. 6.30 *в* показано застосування аналізатора звуку для оперативного контролю шумів на вулицях і площах міста, а на рис.6.30 *г* - для мобільних вимірів рівня шумів і створення шумової карти міста, околиць аеропорту, місцевості, що оточує занадто "шумні" підприємства. В цьому випадку мікрофони встановлюють на даху автомобіля, на якому об'їжджають контрольовану місцевість, фіксуючи в пам'яті приладу виміряні рівні шуму, що відповідає координати і час. Якщо в автомобілі є GSM навігатор, то результати вимірів рівня шуму автоматично прив'язуються до карти. Виміряний рівень шуму може автоматично порівнюватися з допустимим рівнем. При перевищенні рівня шуму подається сигнал, і мікропроцесор сам складає відповідний протокол.

Все більше власників мобільних телефонів починають користуватися так званою "*Bluetooth гарнітурою*". Ці невеликі легені акустичні сенсори кріплять до вуха з метою вивільнення рук від необхідності тримати мобільний телефон, яким можна тепер дистанційно користуватися на відстані до 10-20 м. З цією метою в гарнітуру вбудовуються мініатюрний мікрофон, схеми посилення сигналів від нього, *Bluetooth* радіоприймач-передавач, навушник і необхідні елементи управління. Деякі зразки з широкого вибору наявних на ринку гарнітур *Bluetooth* показані на рис. 6.31. Цілий ряд гарнітур підтримує сервіс видачі команд, що управляють, голосом, голосовий набір номера, а через деякі з них за допомогою голосу можна навіть управляти декількома домашніми пристроями, оснащеними інтерфейсом *Bluetooth*. Це може бути, наприклад, кондиціонер або обігрівач, радіоприймач або телевізор [14].

Рис. 6.31. Безпроводова гарнітура

Підслуховуючи пристрої

Серед інтелектуальних акустичних сенсорів є і прилади для непомітного прослуховування розмов. Відразу ж обумовимо, що це є законним лише за наявності дозволу суду або прокурора. Одним з видів таких сенсорів є спрямовані приймачі звуку (рис.6.32) з рупорною 1 або з параболічною антеною 2.

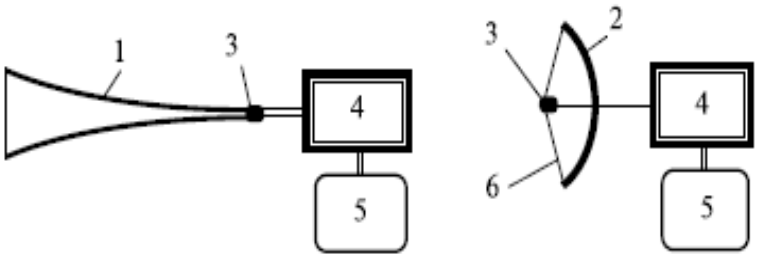


Рис. 6.32. Функціональна схема спрямованих приймачів звуку : ліворуч - з рупорною 1; справа - з параболічною антеною 2; 3 - мікрофон; 4 - електронний блок; 5 - навушники або гучномовець; 6 - розтяжки для кріплення мікрофону

Така антена не лише забезпечує гостру спрямованість і фільтрацію звуків, що приходять з інших напрямів, але і, збираючи звук з великої поверхні, концентрує його на малій площі мікрофону 3, чим забезпечує підвищення чутливості. У електронному блоці 4 робляться фільтрація, посилення і попередня обробка сигналів. Посилені звукові сигнали можна прослуховувати через навушники або гучномовець. Паралельно робиться запис розмови в пам'ять сенсора.

З параболічною антеною діаметром 0,4-1 м вдається досягти гостроти діаграми спрямованості і чутливості, достатніх для того, щоб за відсутності значного стороннього акустичного шуму почути і зафіксувати розмову, що ведеться на відстанях до 1200 м. У реальних умовах міста за наявності значного звукового фону ця дистанція скорочується до 100 м. Якщо розмова ведеться усередині приміщення або автомобіля за закритими вікнами, то для його прослуховування розроблені так звані «*лазерні мікрофони*».

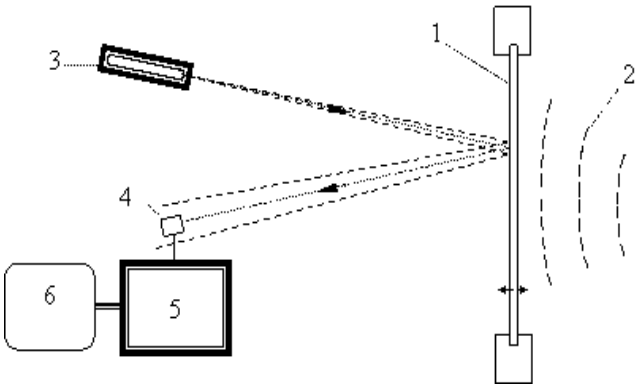


Рис. 6.33. Функціональна схема лазерного мікрофона

Звукові хвилі 2, досягаючи скла 1, викликають його вібрацію з відповідними звуковими частотами. Тут скляна пластина вікна грає роль мембрани - чутливого елементу сенсора, який перетворює звукові сигнали на механічні коливання. На значній відстані від скла (до 100-200 м) встановлюють лазер 3, невидимий (як правило, інфрачервоний) модульований промінь якого направляють на скло. На такій же приблизно відстані в межах конуса відбитого від скла лазерного променя розташовують приймальний пункт, до складу якого входять один або декілька фотоприймачів 4, електронний блок 5 і генератор звуку 6 (навушники або гучномовець). При вібраціях скла змінюється фаза світлових коливань, що потрапляють на фоточутливий елемент в точці прийому.

Сигнали від нього в електронному блоці посилюються, фільтруються, детектуються і записуються, а також можуть бути прослухані через навушники 6.

Можливо для прослуховування використовувати пристрої із застосуванням стетоскопа. Мініатюрний стетоскоп кріплять до стіни приміщення, що примикає до того, що охороняється, - до бетонної панелі стелі, пола або до стіни тієї ділянки системи вентиляції, яка підходить до приміщення, що прослуховується. Чутливість сучасних стетоскопів дозволяє прослуховувати розмову за бетонною стіною завтовшки до 1 м. Сигнал від стетоскопа передається на електронний блок, який його посилює, обробляє і через кабель посилає до передавача.

Раніше це були радіопередавачі на ультракоротких хвилях. Тепер частіше застосовують оптичні інфрачервоні передавачі з великою кутовою апертурою випромінювання. Це дозволяє встановити приймач у будь-якому зручному місці досить широкої зони, оскільки радіус прийому складає 500 м і більше. Передачу інфрачервоними променями виявити значно важче, ніж радіопередачу. Тим паче, що наявний в електронному блоці мікропроцесор дозволяє розбити розмову на фрагменти, стиснути соответствующу

Тонометри

Артеріальний тиск - це один з дуже важливих показників фізіологічного стану серцево-судинної системи людини. Тиск крові в артеріях змінюється в такт з роботою серця. Коли серце стискається і виштовхує кров в артерії, тиск в них короткочасно підвищується і досягає свого піку, який називають систолічним або "верхнім" тиском. У фазі максимального розслаблення сердечних м'язів тиск крові в артеріях найбільш низький, - його називають тиском діастоли або "нижнього".

Всесвітня організація охорони здоров'я затвердила норми, відповідно до яких нормальних (допустимими) для дорослої людини вважаються систолічний тиск від 100 до 140 мм рт. ст. і тиск діастоли від 60 до 90 мм рт. ст. Підвищений артеріальний тиск прискорює зношування, старіння кровоносних судин, невиправдано збільшує інтенсивність роботи серця і навантаження на нього, підвищує ризик інсультів, інфарктів. Знижений артеріальний тиск викликає у людини апатію, млявість, зниження життєвого тонусу. Тому як з гіпертензією, так і з гіпотензією потрібно боротися за допомогою здорового способу життя, ліків або засобів народної медицини. Але для правильного лікування потрібно контролювати артеріальний тиск. Для цього і потрібні тонометри - прилади для виміру артеріального тиску.

У XVIII- XX повіках використовувалися ручні тонометри, сучасний варіант яких показаний на рис. 6.34. Такий тонометр складається з манжети 1, гумової груші 2, сполучних гумових трубок 3, механічного манометра 4, фонендоскопа 5 і вентиля 6 для випуску повітря.

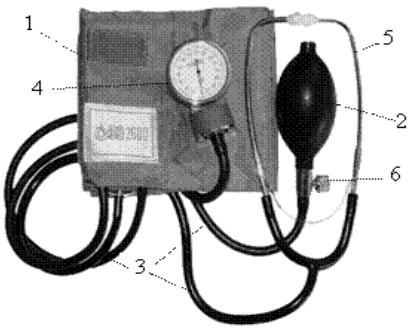


Рис. 6.34. Ручний тонометр

Перед виміром манжету 1 накладають на плече пацієнта так, щоб її гумовий мішечок охопив увесь обвід руки, і застібають. Навушники фонендоскопа 5 вставляють у вухо (лікаря, медсестри або самого пацієнта, якщо він вимірює тиск сам собі), а слуховий елемент фонендоскопа (стетоскоп) вставляють під край манжети у згину ліктя над артерією. Закривають клапан 6 і за допомогою гумової "груші" 2 через сполучну трубку 3 нагнітають в манжету повітря до тих пір, поки в навушниках фонендоскопа не зникне звук пульсації крові в артерії.

Таким чином, звук пульсації крові в артерії і є тут тим первинним інформаційним сигналом, який дозволяє вимірювати артеріальний тиск крові. Тому тонометри і відносимо ми до класу акустичних сенсорів. Тонометри є активними сенсорами тому, що вони активно впливають на кровоносні артерії, чинячи на них зовнішній тиск, що міняється. Т.е. манжета служить в тонометрі вузлом активного впливу на контрольований об'єкт (кровоносні артерії). А фонендоскоп служить акустичним чутливим елементом, що дозволяє спостерігати реакцію об'єкту на відповідну дію.

Нині усе більш споживаними стають інтелектуальні електронні (цифрові) тонометри. Їх розділяють на 2 групи: *напівавтоматичні і автоматичні*. У *напівавтоматичних* тонометрах ручною залишається тільки операція нагнітання повітря в манжету (за допомогою гумової груші), а в деяких - ще і операція поступового зниження тиску в манжеті (за допомогою ручного вентиля).

Дві з багатьох марок напівавтоматичних тонометрів показані на рис. 6.35. Такі тонометри складаються з манжети, гумової "груші", електронного блоку і сполучних трубок.

До складу електронного блоку входить мікрофон, підсилювач і селектор звукових сигналів, датчик тиску в манжеті, автоматично керований повітряний клапан, звуковий сигналізатор, мікрокомп'ютер, рідкокристалічний індикатор і кнопки управління приладом.

Рис. 6.35. Напівавтоматичні тонометри

Як тільки з мікрофону поступає перший звуковий тон, який свідчить про початок пульсації крові в артерії за манжетою, мікропроцесор фіксує значення систолічного тиску. А в мить, коли інтенсивність звукових тонів різко зменшується, фіксує тиск діастоли. Крім того, мікропроцесор в ході виміру тиску обчислює і інтервали часу між послідовними ударами серця, підраховує середню частоту пульсу і варіації тривалості інтервалів між ударами. Після фіксації тиску діастоли, сам мікропроцесор відкриває клапан. Повітря виходить з манжети, і тиск в ній швидко падає до нуля. Вимір закінчується, а комп'ютер виводить на екран дисплея знайдені значення верхнього і нижнього артеріального тиску, частоту пульсу і попередження у разі помилок або виявлення істотної сердечної аритмії.

У деяких тонометрах усі ці значення разом з датою і часом виміру фіксуються в енергонезалежній пам'яті приладу, де можуть зберігатися дані 30-100 вимірів. В цьому випадку мікропроцесор може обчислювати і виводити значення середнього артеріального тиску і частоти пульсу за останній період, кількість випадків аритмії, і тому подібне. Деякі напівавтоматичні тонометри мають також кольорову шкалу артеріального тиску, на якій у вигляді стовпчиків відображаються виміряні рівні тиску і червоним кольором виділяються небезпечні зони.

Деякі марки *автоматичних тонометрів* показані на рис. 6.36. У їх комплектацію вже не входить гумова груша, оскільки процес нагнітання повітря в цих тонометрах теж автоматизований. Для цього в електронному блоці є мініатюрний керований електронасос. Користувачеві залишається лише правильно накласти манжету на плече і натиснути кнопку. Увесь подальший процес виміру відбувається автоматично. Якщо в процесі виміру з'являються якісь перешкоди (перебої сердечного ритму, ворушіння руки, кашель, сторонній гучний звук і тому подібне), то вбудований в прилад мікропроцесор сам запускає процес виміру повторно.

Рис. 6.36. Автоматичні тонометри

Повністю автоматичний режим дає також можливість підвищити точність виміру Запам'ятавши артеріальний тиск цього користувача, мікропроцесор при наступних вимірах сам регулює рівень нагнітання повітря так, щоб він лише на необхідну величину перевищував систолічний тиск цього пацієнта, і забезпечує тим самим комфортніші умови виміру. Деякі з автоматичних тонометрів мають також інтерфейс до зовнішнього комп'ютера, виводять на свій дисплей поточну дату і час. Вони можуть бути запрограмовані на різні сервісні дії. Наприклад, нагадувати звуковим сигналом і значками на дисплеї про необхідність прийому ліків або чергового виміру тиску.

Гідролокатори

Ще активнішими акустичними сенсорами є ехолокатори, які самі генерують акустичні хвилі для того, щоб зібрати потрібну інформацію про контрольовані об'єкти. У цьому вони подібні до радіолокаторів, але зондування довкілля ведеться не радіохвилями, а акустичними хвилями. Оскільки акустичні хвилі поширюються значно повільніше, ніж радіохвилі, той час запізнювання відбитих сигналів значно більше, що істотно спрощує обробку сигналів при зондуванні на невеликі відстані.

Перевагу в ехолокації зазвичай віддають ультразвуковим (далі УЗ) хвилям, оскільки вони:

- мають меншу довжину хвилі і тому більш високу роздільну здатність;
- при тій же амплітуді коливань тиску мають значно більш високу інтенсивність (яка пропорційна квадрату частоти);
- не сприймаються людським вухом, тому не створюють для нас небажаний звуковий фон.

УЗ хвилі середніх і високих частот досить сильно поглинаються і швидко затухають в повітрі і газах. Тому для ехолокації в повітрі застосовують переважно низькочастотні УЗ хвилі.

Ехолокацію у водній і взагалі в рідкому середовищі прийнято називати гідролокацією. Перші гідролокаційні прилади вимірювали тільки глибину водойми, тобто відстань від акустичної антени до дна моря (океану, річки, озера). Саме такі прилади спочатку і називали ехолотами. Якщо судно з ехолотом переміщалося, то на основі таких вимірів будувався профіль дна відносно поверхні води уздовж траєкторії переміщення судна.

Нині поняття "ехолот" значно розширилося. Ехолотами називають усі сенсори, які діють за принципом сприйняття звуків, відбитих від розташованих віддалік предметів, тобто за принципом луни (від грецького "луна" - відбитий звук, відгомін, відгук). У гідролокації назви " гідролокатор " і " ехолокатор ", "ехолот", "сонар" (абревіатура від англійської назви "*SOund NAvigation and Ranging*", приблизний переклад - звукова навігація і вимір відстаней) стали практично синонімами.

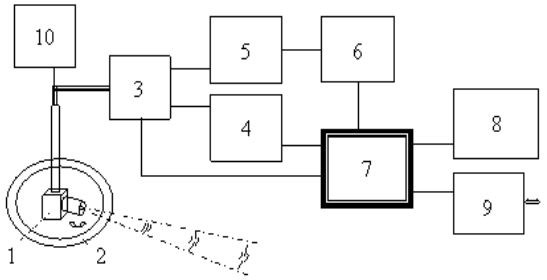


Рис. 6.37. Принцип роботи гідролокатора

Акустична антена 1, герметично захищена оболонкою 2, зробленою з прозорого для звуку матеріалу, знаходиться у воді. Через кабель вона сполучена з комутатором 3, який по черзі підключає до неї генератор 4 або приймач-підсилювач акустичних сигналів 5. Останній сполучений з селектором сигналів 6, вихід якого підключений до мікропроцесора 7. Виходи

останнього підключені до індикатора 8 і до інтерфейсного блоку 9. Роботою гідролокатора автоматично управляє мікропроцесор 7. Він подає на генератор 4 сигнал про початок зондування водного простору і команди про параметри цього зондування (частота ультразвуку, тривалість, структура і потужність УЗ імпульсів, періодичність їх повторення і тому подібне). Потім мікропроцесор 7 подає сигнал на комутатор 3, який пропускає електричні коливання від генератора 4 до антени 1. Там вони за допомогою п'єзоелектричного осцилятора перетворюються на потужні акустичні коливання і випромінюються антеною в навколишній водний простір.

Рис. 6.38. Базовий блок гідролокатора Furuno CH - 250, який випускається для застосування на рибопромисловому флоті.

Акустична антена кругового і вертикального сканування встановлюється на підводній частині корпусу корабля.

Гідролокатор може працювати у восьми режимах:

- *відображення эхо-профілю пройденого маршруту;*
- *точне визначення координат об'єктів. - секторне або кругове сканування водного простору по азимуту;*
- *вертикальне сканування;*
- *комбінація секторного і вертикального сканування для оцінки розподілу косяка одночасно в горизонтальній і вертикальній площинах;*
- *прокладення маршруту з уважним обстеженням усіх можливих підводних перешкод;*
- *забезпечення гидролокационного "захоплення" вказаного оператором об'єкту (косяка, підводної перешкоди) і автоматичне стеження за ним пучком УЗ хвиль.*

Інтелектуальні сенсори

Існує багато простіших інтелектуальних сенсорів, в яких використовується активна гідролокація. Один з них - вимірник потоку рідини *Sonartron ST* фірми *Honsberg* показаний на рис.6.39.

Рис. 6.39. УЗ вимірнювач потоку рідини *Sonartron ST* фірми *Honsberg*

У проточну металеву трубу, крізь яку пропускається рідина, один проти одного вбудовані випромінювач і приймач УЗ імпульсів. Ці імпульси проходять уздовж осі потоку. Час запізнювання прийнятого імпульсу відносно моменту випромінювання залежить від швидкості руху рідини. Електронна схема, яка вимірює час запізнювання, перераховує цей

час за даними попереднього калібрування у величину потоку рідини і видає це значення в цифровій формі. Потік води в діапазоні від 0,04 л/хв. до 40 л/хв. вимірюється з точністю до 2,5 %. Сенсор має також аналоговий електричний вихід і захисне електричне реле, що замикається при перевищенні потоком рідини заздалегідь заданої в цифровому виді величини.

Інтелектуальні акустичні сенсори для УЗВ

Одним із застосувань ехолокації вже не у воді, а в повітрі, являється УЗ виявлення присутності об'єкту в контрольованій зоні і вимір відстані до нього. Особливо важливим стає це в складних умовах густого туману, задимленості, запиленій і тому подібне, коли оптичні методи "працюють" погано. А для УЗ хвиль це усе - не перешкода. В якості джерела ультразвуку найчастіше застосовують п'єзоелектричні перетворювачі. Деякі типи УЗ сенсорів відстані, що промислово випускаються, показані на рис.6.40.

Рис. 6.40. УЗ сенсорів відстані, що промислово випускаються.

Випромінювач і приймач УЗ хвиль знаходяться в одному корпусі разом з необхідною для вимірів електронікою і з елементами, що забезпечують спрямованість - концентрацію випромінюваних УЗ хвиль, що приймаються, в певному секторі простору. УЗ хвилі з частотою 65-400 кГц у вигляді короткочасного імпульсу випромінюються у напрямі контрольованої зони 10-200 разів кожну секунду. Якщо в контрольованій зоні з'являється об'єкт, то відбита або розсіяна від нього УЗ хвиля повертається назад до сенсора і сприймається приймачем з деяким запізнюванням. По виміряному часу запізнювання розраховується відстань до об'єкту.

Випускаються УЗ сенсори відстані з різними параметрами, розрахованими як на невеликі відстані - від 15 до 200 мм з точністю до 0,2 мм, так і на середні відстані - від 0,3 до 6 м з точністю до 1 мм, а також на відстані в десятки метрів.

Вихід таких сенсорів може бути як цифровим, так і аналоговим. Якщо до складу УЗ сенсора входить мікрокомп'ютер, то завдяки вбудованим датчикам температури і тиску легко вирішується питання корекції результатів зроблених вимірів з урахуванням залежності швидкості поширення УЗ хвилі в повітрі від вказаних параметрів.

Якщо частота УЗ коливань фіксована, то за допомогою таких сенсорів можна визначати і швидкість руху об'єкту, вимірюючи доплерівське зрушення частоти відбитої хвилі. Якщо кутова діаграма спрямованості УЗ сенсора досить вузька (а це залежить від конструкції

корпусу і наявності параболічного або сферичного рефлекторів) те, поступово повертаючи його в певному кутовому секторі, можна, як і в гідролокаторах, сканувати УЗ зондом і оглядати значнішу зону простору.

Рис. 6.41. УЗ вимірник рівня рідини Omni – L

Рівень рідини визначається з точністю близько 1 мм за часом запізнювання відбитого від поверхні рідини УЗ імпульсу. Багато спеціалізованих інтелектуальних акустичних сенсорів створені і застосовуються для дефектоскопії металевих заготівель (прокату, відливань...) і готових металоконструкцій. У основі їх роботи теж лежить принцип ехолокації, але вже в твердих тілах. У якихось місцях металевої конструкції збуджуються УЗ коливання, в інших - встановлені приймачі УЗ хвиль. Прийняті ними УЗ коливання піддаються математичному аналізу в мікрокомп'ютері. За результатами аналізу можна визначити механічний стан конструкції.

Такі спеціалізовані інтелектуальні акустичні сенсори дозволяють своєчасно виявляти тріщини, порожнечі, сторонні включення і інші дефекти в металевих виробах, явища "втоми" металів, небажані механічні зміни в конструкціях і запобігати можливим аваріям. У разі виникнення ушкоджень трубопроводів, безстикових рейок надшвидкісних залізниць і так далі інтелектуальні УЗ акустичні сенсори дозволяють швидко локалізувати місце ушкодження і відновити функціонування цих важливих магістралей.

Інтелектуальні портативні сенсори для УЗ досліджень

Одним з важливих видів ехолокації є ультразвукові дослідження внутрішніх органів людини, які широко застосовують в медицині. Швидкість поширення УЗ хвиль в тканинах людського тіла складає близько 1540 м/с, тобто близька до швидкості у водному середовищі. Але із-за акустичної неоднорідності людського тіла на межах розділу органів і тканин з різною щільністю і пружністю, відбувається часткове відображення, розсіяння і заломлення УЗ хвиль. Чим більше перепаду щільності, тим вище амплітуда відбитої УЗ хвилі. Це і дозволяє визначати, а потім і відтворювати у вигляді зображення просторові межі між органами, тканинами і різними структурними елементами тканин, їх форму, розміри, взаємне розташування, локальні особливості. Застосовуючи УЗ хвилі високої частоти (1-15 Мгц), вдається досягти високої роздільної здатності - до 0,1 мм. При відображенні від рухливих об'єктів (дихальні переміщення грудної клітки, діафрагми, скорочення серця, пульсація артерій, просування крові по посудинах і тому подібне) змінюється частота відбитою УЗ хвилі (ефект Доплера). Вимірюючи величину зміни частоти, можна вичислити відповідну швидкість руху і візуально виділяти ділянки внутрішніх органів, які рухаються з різною швидкістю, - навіть досить повільно (менше 1 см/с).

На рис. ліворуч показаний сучасний апарат *SonoAce Pico* для УЗ сканування людського тіла. Будучи переносним (357x320x204 мм, маса менше 10 кг), він має практично такі ж діагностичні можливості, як і традиційні стаціонарні апарати для УЗИ. Завдяки цифровій технології формування УЗ пучків і обробки сигналів він дозволяє отримувати кольорові зображення стану внутрішніх органів з високою роздільною здатністю [7].

Рис. 6.42. Портативні апарати для УЗ досліджень : ліворуч - *SonoAce - Pico*; справа - *Fukuda UF - 750XT*

Окрім можливості формування об'ємних зображень і застосування широкосмугових мультичастотних датчиків, він може виконувати функції формування трапецеїдального зображення, збільшення масштабу зображення при дослідженні малих органів. Він розрахований також на застосування микроконвексного датчика, має програми кардіологічних досліджень. Можлива глибина сканування - до 30 см У базову комплектацію входять також електрокардіографічний модуль з програмним забезпеченням, система SonoView Lite для архівації і подальшого перегляду ехограм, містка пам'ять, виходи для одночасного приєднання до базового блоку двох датчиків.

Можливе застосування багатьох прогресивних технологій ультрасонографії :

- *Multi - beam* - технологія цифрового формування УЗ пучків з пригніченням впливу багатократних відображень, нелінійних спотворень, неточності інтервалів затримки і т. п.
- *OTI (Optimum Tissue Imaging)* - технологія формування оптимального зображення тканини завдяки корекції швидкості (вибір оптимальної швидкості для кожної області, щоб забезпечити високу якість зображень одночасно усіх видів тканини, таких як жирова, м'язи або паренхіма печінки).
- *THI (Tissue Harmonic Imaging* - "тканинна" або друга гармоніка) - підвищує якість зображень, їх контраст і лінійну роздільну здатність у пацієнтів з ускладненою візуалізацією (наприклад, з товстими жировими прошарками).
- *OHI (Optimized Harmonic Imaging)* - застосовується в особливо важких для дослідження випадках. FINE (Filtered Image for Noise reduction & Edge enhancement) - технологія поліпшеної фільтрації УЗ сигналів, яка зменшує рівень шумів і забезпечує більш високий контраст.
- *CAFE (Compound Automatic Flash Elemination)* - забезпечує адаптивну нелінійну фільтрацію для видалення кольорових точок, які виникають внаслідок випадкових артефактів. Покращує візуалізацію кровотоку в доплерівських режимах.

Ультразвуковий діагностичний сканер Fukuda UF - 750xt показаний на рис. 6.43.

Рис. 6.43. Ультразвуковий діагностичний сканер *Fukuda UF - 750xt*

Він призначений для невідкладної (на виїздах) УЗ функціональної діагностики серцево-судинних захворювань, щитовидної і молочної залоз, бруньок, печінки, шлунку, жовчного

міхура, статевих органів. Кольоровий рідкокристалічний дисплей з діагоналлю 265 мм забезпечує високу якість зображень. Загальні габаритні розміри сканера 380х220х370 мм, маса - менше 13 кг Оснащений магнітооптичним диском пам'яті на 640 Мбайт, на якому можуть зберігатися до 6 тисяч ехограм. Маючи приблизно такі ж функціональні можливості, як і попередній сканер, він забезпечує також УЗ дослідження слабкого і повільного кровотоку.

До складу програмного забезпечення входять:

- програмні пакети для вимірів, обчислень і автоматичного створення звітів (для акушерства, кардіології, ангіології, радіології, урології, гінекології, хірургії, педіатрії);
- програми об'ємної реконструкції з можливістю мультипланового аналізу, підтримки протоколу безпровідного зв'язку;
- програма формування і підтримки бази цих пацієнтів з можливістю перенесення даних на зовнішні носії і на зовнішній комп'ютер.

Сенсори на поверхневих акустичних хвилях

Досі розглядалися сенсори, які використовують акустичні хвилі в об'ємі газів, рідин або твердих тел. Але є ще і велика група сенсорів, в яких використовується поширення акустичних хвиль по поверхні твердих тіл або в їх приповерхневій області.

Такі хвилі називають *поверхневими акустичними хвилями (ПАХ)* і відповідно *приповерхневими акустичними хвилями (ППАХ)*. Для збудження і детектування ПАХ і ППАХ використовують прямий і зворотній п’єзоелектричний ефект. Найчастіше з цією метою на поверхні п'єзокристала, пьезокерамики або на п'єзоелектричній плівці формують так звані *зустрічно-штирьові перетворювачі (ЗШП)*. Це - електроди, що мають форму гребінки, в яких довжина кожного штиря набагато більше ширини (рис.6.44).

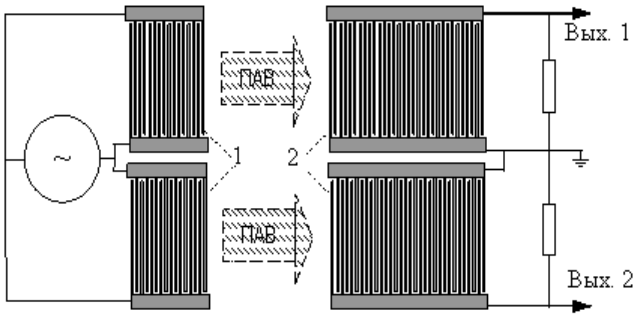


Рис. 6.44. Принцип дії сенсорів на ПАХ:
1 - зустрічно-штирьові перетворювачі електричного сигналу в ПАХ;
2 - зустрічно-штирьові перетворювачі ПАХ в електричний сигнал.

Коли на ЗШП 1 подається змінна напруга, в п'єзоелектричному матеріалі виникають хвилі механічного стискування і розтягування з частотою змінної напруги. Якщо відстань між штирями дорівнює довжині хвилі, то хвилі від усіх штирів виявляються синфазними і посилюють одна іншу. Виникає сильна резонансна поверхнева акустична хвиля. Швидкість поширення ПАХ в п’єзоматериалах складає 3,8-4,2 км/с. Тому ПАХ з частотою 1 ГГц має довжину хвилі приблизно 4 мкм. Поширюючись уздовж поверхні п’єзоелектрика, ПАХ проходить відстань в 1 мм приблизно за 250 нс. Коли хвиля доходить до електродів 2, вона стає причиною виникнення між парою сусідніх штирів змінної електричної напруги тієї ж частоти. Коливання напруги між сусідніми парами штирів, складаються. Тому напруга на виході ЗШП виявляється найбільшою у разі збігу їх фаз, тобто тоді, коли відстань між штирями сусідніх пар дорівнює довжині хвилі [9].

Таким чином, геометрична структура ЗШП забезпечує високу вибірковість приладів на ПАХ. Якщо ця структура строго періодична, то вона функціонує як високодобротний частотний фільтр. Якщо ж повинні прийматися лише сигнали, що певним чином модулюються по амплітуді, частоті, фазі і тому подібне, то використовується і відповідна

геометрична структура ЗШП. Прилад на ПАХ функціонує тоді як високоефективний корелятор, що видає на виході пік напруги тільки тоді, коли просторово-часова структура поверхневої акустичної хвилі точно співпадає з геометричною структурою ЗШП. Прилад фазується і синхронізується з сигналом, який поступає на його вхід, автоматично, тобто сам і тільки у момент повного збігу структури хвилі і структури ЗШП.

Саме з цих причин прилади на ПАХ широко використовують в сучасній радіотехніці: і в мобільному радіозв'язку, і в системі глобального орієнтування GSM, в системах цифрового і локального безпровідного зв'язку і т.п. Із застосуванням ЗШП і ПАХ побудовані ефективні фільтри проміжної частоти, вихідні і багатомодові фільтри, що калібруються лінії затримки з дуже малим загасанням, фільтри Найквіста для цифрового телебачення і цифрового радіозв'язку, лінії затримки для кодового і тимчасового розділення каналів, фільтри систем волоконно-оптичного зв'язку і т.д.

Цікавим застосуванням відносно дешевих сенсорів на ПАХ стала автоматична радіоідентифікація багажу, контейнерів, транспортних одиниць, важливих поштових відправлень. Схема їх радіоідентифікації показана на рис. У багаж, що підлягає пильному контролю, за додаткову плату вкладають невеликий радіоідентифікатор з індивідуальним кодом. У аеропортах, на вокзалах, в морських або річкових портах, на транспортних вузлах і контрольних пунктах встановлюють системи автоматичної радіоідентифікації. До складу такої системи входить *мікрокомп'ютер 1*, що приймає через канали зв'язку запити на перевірку контрольованих вантажів. Отримавши запит з кодами контрольованих вантажів, він через *генератор 2 і радіоантену 3* автоматично організовує випромінювання радіосигналів, що фазо-маніпульованих, на частоті близько 1 ГГц з позивними відповідних вантажів. Радіоідентифікатори, вкладені у вантажі, приймають ці позивні, посилюють і подають на свій індивідуальний ПАХ селектор.

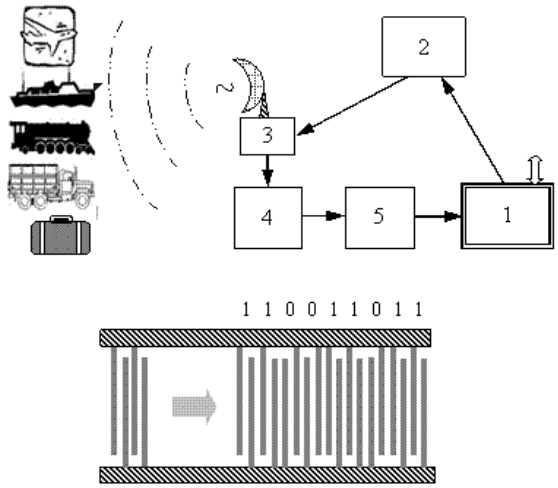


Рис. 6.45. Схема функціонування системи радіоідентифікації багажу. Знизу – структура ЗШП, що відповідає коду "110011011"

Цей відгук приймається *антеною 3*, посилюється *радіоприймачем 4* і передається на фазовий *детектор 5*, який формує двійковий код. *Мікрокомп'ютер 1* порівнює цей код з кодом контрольованого вантажу і, якщо вони співпадають, фіксує це у своїй пам'яті. Потім за допомогою *генератора 2* і *радіоантени 3* випромінюються позивні наступного контрольованого вантажу, і процес повторюється. Після обробки усього запиту мікрокомп'ютер формує відповідь на нього і через канали зв'язку автоматично інформує того, що просить про наявність або відсутність в цьому контрольному пункті відповідних вантажів.

Рис. 6.46. Мікроваги *XP - Micro* компанії Метлер Толедо на ПАХ

З використанням ПАХ елементів нині випускають дуже чутливі мікроваги. Як приклад на рис. 6.46. показані мікроваги *XP - Micro* компанії Метлер Толедо. Зважування маси до 52 г з дискретністю 1 мкг. Габаритні розміри 263 х 490 х 322 мм. Вони мають вбудований мікрокомп'ютер, електронний контроль горизонтального рівня, подвійний термостатований кожух зі знепилюванням, кольоровий сенсорний дисплей, можливість під'єднування до електронної інформаційної мережі, безпровідного зв'язку через інтерфейс *BlueTooth*. Ретельно продумані усі нюанси зважування дуже малих доз дорогих речовин. Зазвичай зважувану дозу кладуть в "*човник*", бюксу або на листочок кальки, і при перенесенні можливі її втрати. У цих вагах забезпечується можливість дозування навішування відразу ж в кінцеву тару через маленьке віконце в дверцях, завдяки чому виключаються небезпечні рухи повітря усередині робочого об'єму вагів при зважуванні. Досягається відтворюваність результатів зважування краще 1,5 мкг, і значно знижуються втрати дуже дорогих реагентів.

Такі високоточні і швидкодіючі ваги використовуються, наприклад, в лабораторіях тонких хімічних і біохімічних аналізів і синтезів в таких сферах застосування, як фармацевтична і косметична промисловість, здобич і обробка дорогоцінних рідкісних металів, геологічна розвідка, мікроелектроніка, кольорова металургія, судова експертиза, наукові дослідження і т.п.

Хімічні і біохімічні сенсори на ПАХ

Якщо на чутливу зону нанести спеціальне покриття (оксиди металів, полімерні плівки і тому подібне), що вибірково сорбувало молекули певного газу або пари з навколишнього повітря, то отримаємо досить чутливий ПАХ сенсор присутності в повітрі відповідних речовин. Вже розроблені і промислово випускаються ПАХ сенсори для контролю наявності більшості важливих органічних і неорганічних газів в технологічному середовищі і в атмосфері приміщень.

За останнє десятиліття були створені також матричні ПАХ сенсори. Їх ще називають мультисенсорами. У них на одному кристалі формується одночасно цілий масив ППАХ сенсорів, на кожного з яких наносять свою чутливу плівку. Більшість розробок виконана в області мультисенсорних газоаналізаторів, в яких контрольований об'єм повітря аналізується на присутність відразу десятків різних речовин.

6.11. Електричні сенсори

У широкому сенсі все або майже усі інтелектуальні сенсори можна віднести до класу електричних. Адже, врешті-решт, будь-які сигнали в інтелектуальних сенсорах перетворюються на електричні сигнали, з якими працює мікрокомп'ютер. В механічних і в акустичних сенсорах майже завжди є чутливі елементи, що перетворюють механічні або

акустичні сигнали на електричні. Така ситуація дуже часто має місце і в усіх інших класах інтелектуальних сенсорів. Електричні сенсори, що є складовими частинами інших сенсорів, зазвичай розглядаються в таких випадках як "*трансд'юсери*", - перетворювачі інших видів сигналів в електричну форму. У них зміна електричних властивостей є вже вторинною, - наслідком первинних змін механічних, акустичних або інших властивостей. Перехід до електричної форми сигналів потрібний лише для зручності їх подальшої обробки. Проте, такі трансд'юсери і у складі інших сенсорів самі по собі залишаються електричними сенсорами.

Електричними властивостями тіл є: їх електричний заряд, електричний потенціал, конфігурація створюваного електричного поля, електроємність і тому подібне. До електричних властивостей речовин належать їх електропровідність або електричний опір, діелектрична постійна і, в загальнішому випадку, - їх комплексна діелектрична постійна. До властивостей електричних ланцюгів можна віднести напругу на тій або іншій ділянці ланцюга; струм, що протікає через них; для ланцюгів змінного струму - імпеданс, амплітуду, частоту і фазу коливань струму, власні резонансні частоти і тому подібне. Якщо будь-яка з цих властивостей змінюється під дією чинників або процесів, за якими вимагається "спостерігати", то ці зміни можна реєструвати і на цій основі будувати певні висновки про об'єкт спостереження.

Рис. 6.47. Класифікація електричних сенсорів по фізичному принципу дії

До активних чутливих елементів відносять транзистори, діоди, нелінійні електронні елементи, що мають ділянки вольтамперної характеристики з негативним нахилом, газорозрядні і інші елементи, усередині яких викликані зовнішнім впливом невеликі зміни відразу ж значно посилюються за рахунок зовнішнього джерела енергії. Зазвичай вважають, що усі активні чутливі елементи є "струмовими", тобто під впливом контрольованого зовнішнього чинника змінюється електричний струм, що протікає крізь них.

Пасивні чутливі елементи класифікують по виду електричної характеристики, що змінюється під впливом контрольованого чинника, на резистивні, ємнісні і так далі. Далі їх можна класифікувати на підвиди залежно від того, під дією якого саме зовнішнього чинника змінюються їх електричні характеристики (пьезорезисторы, терморезистори, фоторезистори ...).

Резистивні сенсори

Одними з простих електричних сенсорів є резистивні сенсори, в яких під дією зовнішнього чинника змінюється опір тієї або іншої ділянки електричному ланцюгу. Як сказано вже вище, їх ми класифікуватимемо, виходячи з того зовнішнього чинника, під дією якого змінюється електричний опір резистора.

Відомим прикладом резисторів, що реагують на механічну дію, є сенсори -"вахтери" для спостереження за цілісністю шибок. По поверхні скла простягають "мереживо" з тонкої, майже непомітної тяганини. Сенсор вимірює і контролює загальний опір цього "мережива" тяганини. Якщо скло розбивається, то деяка тяганина неминуче розривається, внаслідок чого загальний електричний опір змінюється. Реєструючи таку зміну, сенсор подає сигнал тривоги.

Терморезистори

Терморезистори – резистори, у яких електричний опір провідника або напівпровідника залежить від температури.

Значніші за величиною і різні по знаку температурні коефіцієнти електричного опору мають напівпровідники. Напівпровідникові терморезистори прийнято називати *термісторами*. Вводячи в кремній незначні домішки, можна отримати в певних температурних діапазонах як позитивний, так і майже нульовий, а також негативний температурний коефіцієнт опору. Особливо широко в ролі термісторів застосовують оксиди металів. Їх виготовляють у вигляді тонких і товстих плівок, маленьких керамічних пластинок, стержнів, циліндрів, невеликих намистинок і т.д.

Одним з прикладів можливої реалізації інтелектуального сенсора на основі терморезисторів є так звані "PID-регулятори температури" (наприклад, типів T16/P16 і T48), які випускаються промислово. Невеликі по розмірах (50×50×106 мм), вони задовольняють жорстким вимогам промислових застосувань IP65.

Їх входи розраховані на підключення стандартних платинових терморезисторів Pt100 (2 або 3, діапазон зміни опору від 1 до 320 Ом) або терморезисторів типів *S, T, J, N, K, E, R, B.* Виміри відбуваються кожні 0,4 с.

Користувач може вибрати різні режими роботи: пасивне стеження за змінами температури, автоматична сигналізація про вихід температури за задані межі, автоматичне регулювання температури через вихідні силові реле по декількох різних оптимальних алгоритмах. Поточне значення температури чітко висвічується на світлодіодних індикаторах у вказаних користувачем одиницях. Туди ж виводиться і інша важлива інформація. Про розробку аналогічного інтелектуального сенсора температури з погрішністю вимірів, що не перевищує 0,1%.

З використанням мікрокомп'ютерів і набору мініатюрних термісторів, що мають дуже малу власну теплоємність і незначну теплову інерцію, можна будувати складніші інтелектуальні сенсори.

Приклад інтелектуального сенсора для спостереження за змінами об'ємного потоку рідини уздовж стебла або гілок рослини. У таких сенсорах використовують 3 термістори: один - для контролю температури в місці нагріву, другий - для виміру температури стебла на заданій відстані від місця нагріву, третій - для виміру температури довкілля. Сигнали від першого служать для точного регулювання і підтримки заданої температури в місці нагріву. Це важливо, оскільки підвищення температури вище за фізіологічну межу може негативно вплинути на життєдіяльність рослини. Сигнали від другого термістора дозволяють мікрокомп'ютеру вичислити об'ємний потік рідини. А сигнали від третього дають можливість врахувати поправку, пов'язану з віддачею тепла в те, що оточуючий простір.

Їх електричний опір залежить від освітленості. Фоторезистори виготовляють найчастіше з напівпровідників групи $A_{II}B_{VI}$*(CdS, CdSe, CdTe,...)*шляхом напилення тонких шарів або намазування товстих шарів з подальшим спіканням пластинів, рідше - з монокристалів. Зміна їх електричного опору під дією світла відбувається завдяки

внутрішньому фотоефекту, тобто завдяки тому, що при поглинанні квантів світла в напівпровіднику з'являються додаткові вільні носії електричного заряду [15].

Від матеріалу, з якого виготовлений фоторезистор, і від внесених в нього домішок залежить спектральна характеристика, тобто залежність чутливості фоторезистора від довжини хвилі світла, що падає. Спектри чутливості існуючих фоторезисторів перекривають увесь широкий оптичний діапазон спектру від ультрафіолетової до далекої інфрачервоної області. Синтезовані також фоторезистори, які практично повторюють спектральну криву чутливості людського ока. Саме їх рекомендують застосовувати для точної фотометрії, тобто для вимірів характеристик світла в так званих "світлових одиницях" (люменах, люксах, канделах і т.п.).

З використанням фоторезисторів можна побудувати багато видів інтелектуальних сенсорів як дослідницького, так і прикладного характеру. В якості прикладів можна згадати схеми автоматичного визначення витримки у фотоапаратах, в автоматах друку фотознімків, схеми автоматичного управління штучним освітленням і т.д.

П’єзорезистори

Якщо на металевий дріт діє сила, яка розтягує її, то в результаті деформації довжина дроту дещо збільшується, а площа поперечного перерізу дещо зменшується. Через це електричний опір дроту зростає. Таке явище називають п'єзорезистивним (від грецького кореня) або тензорезистивным (від латинського кореня) ефектом.

Значно більш високу тензочуттєвість, ніж металеві, мають напівпровідникові п’єзорезистори, оскільки механізм зміни електричного опору в них набагато складніший. Тензочуттєвість резисторів, наприклад, з кремнію в десятки разів вище, ніж у металевих. Але їх електричний опір також значно сильніше залежить від температури. Для зменшення впливу на результати вимірів неконтрольованих змін температури застосовують мостові схеми. У одно їх плече включений навантажений п’єзорезистор (на який діє вимірювана сила), а в інше - такий самий резистор, але механічно не навантажений. При змінах температури співвідношення опорів і баланс моста не змінюються.

Гігристори

Електричний опір деяких гігроскопічних матеріалів істотно залежить від вологості навколишнього повітря. Резистори з таких матеріалів називають гігристорами і застосовують в сенсорах вологості. Для цього синтезовані спеціальні матеріали: нонілфенілполіетиленглікольефір, гідроксіетілцелюлоза і тому подібне з наповненням вугільним порошком. У складі інтелектуального сенсора можна врахувати зміни цієї залежності з температурою, а також деяке запізнювання зміни електричного опору гигристора при швидких змінах вологості повітря, запам'ятовувати динаміку змін вологості за певний період для подальшої передачі в комп'ютерну мережу, для документування, прогнозування і т.д.

Магніторезистивні сенсори

У магніторезистивних сенсорах використовується здатність деяких матеріалів істотно змінювати свою електропровідність залежно від напряму і напруженості зовнішнього магнітного поля. До таких матеріалів відносяться, наприклад, плівки пермалою (*NiFe*). Найчастіше застосовують структуру, в якій чутливий елемент складається з 4 плівкових резисторів з пермалою, напилених на поверхню кремнію і сполучених у вигляді мостової вимірювальної схеми. Згори магніторезистивні плівки захищають тонким шаром нітриду танталу. Поруч формують мініатюрні плоскі плівкові котушки. Коли через одну з них пропускають електричний струм, створюване ним магнітне поле орієнтує домени пермалоєвих плівок уздовж осі резисторів. Саме у такому стані вони мають найбільшу чутливість. Це робиться кожного разу перед початком серії вимірів.

Через іншу котушку при вимірах пропускають постійний електричний струм, необхідний для компенсації залишкового зовнішнього магнітного поля, перпендикулярного до площини резисторів, і таким чином балансують вимірювальну мостову схему. При появі вимірюваного зовнішнього магнітного поля відбувається розбаланс моста, а вихідний сигнал пропорційний магнітній індукції зовнішнього поля. Усі необхідні схеми формують в тому ж самому кристалі кремнію.

Компенсаційну котушку використовують також для калібрування і для повного балансування моста. Різниця між струмом балансування і початковим компенсаційним струмом пропорційна індукції зовнішнього магнітного поля. Така схема забезпечує високу лінійність вимірів, малу їх залежність від температури і від інших перешкод (наприклад, від наявності поблизу деталей з феромагнітних матеріалів).

Окрім "одновісних" магніторезистивних датчиків, чутливих до магнітного поля одного напряму, випускають також "двовісні" і "тривісні" датчики, в яких 2 або 3 магніторезистивні датчики орієнтовані у взаємно перпендикулярних напрямах. З них виготовляють також сучасні високонадійні компаси без магнітної стрілки і взагалі без рухливих деталей, а також високоточні сенсори напряму руху ("датчики курсу") для авіаційних, морських, автомобільних транспортних засобів.

На рис. 6.48 ліворуч показаний аналоговий магніторезистивний компас HMC6052, в якому використовується двовісний сенсор HMC1052 розміром 3,5×3,5 мм з мінімальним вимірюваним магнітним полем 80 мкГс (магнітне поле Землі близько 600 мГс). Компас працює в діапазоні температур від - 45°С до +120°С, має інтерфейс до ПК.

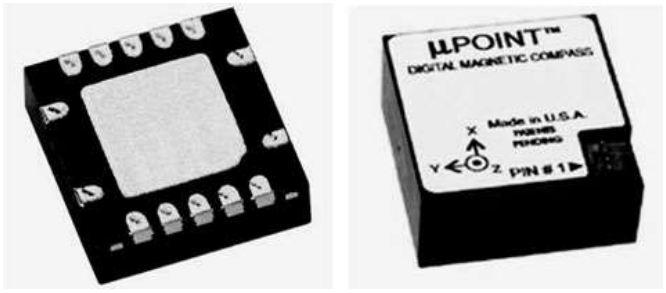


Рис. 6.48. Магніторезистивні компаси

На рис. 6.48. праворуч показаний мініатюрний цифровий гіростабілізований прецизійний компас HMR3600, призначений для визначення азимута, працюючий при будь-якій орієнтації в просторі. Окрім трьох магніторезистивних магнітометрів, до його складу входять три акселерометри і гіроскоп. Компас визначає азимут, подовжній і поперечний крен з точністю ±0,5° при роздільній здатності 0,1°. Застосовується в авіації, мореплаванні, на наземному транспорті, в лазерних далекомірах, блоках управління відеокамерами, при підземній і підводній орієнтації.

Висновки

Сенсор - цей пристрій (прилад, орган, вузол), що перетворює фізичну (фізико-хімічне) зміну в об'єкті спостереження, його дія на чутливий елемент в інформаційний сигнал для користувача . Сенсор - ця сполучна ланка між реальним "фізичним" світом і світом інформаційних моделей, між матерією і інформацією.

Інтелектуальний сенсор - це сенсор, що має у своєму складі мікрокомп'ютер і завдяки цьому здатний виконувати досить складну обробку первинної інформації; враховувати усі необхідні поправки і нелінійності; видавати дані в найбільш зручній для користувача формі; активно впливати на об'єкт спостереження, сприймаючи і аналізуючи викликані цим зміни; робити самоконтроль і самодіагностику; накопичувати і систематизувати дані; підтримувати інформаційний зв'язок із зовнішнім світом; змінювати режими своєї роботи, адаптуючись до умов, що змінюються; легко переходити до виконання інших функцій і т. д.

Контрольні питання до розділу

1. Що таке механічні сенсори переміщення?
2. Що є основою глобальної системи орієнтування?
3. Поясніть принципи роботи глобальної системи орієнтування.
4. 4. Для чого призначений GPS навігатор? Коротко розкажіть, з яких частин він полягає і як функціонує?
5. Назвіть основні групи GPS навігаторів. Чим вони відрізняються?
6. Опишіть можливості застосування авіаційних GPS навігаторів для вимушеної "сліпої" посадки літаків.
7. Як GPS приймачі дозволили по-новому вирішити завдання пересування сліпих людей?
8. Що таке трекер? Яке його призначення і як він функціонує? 9. Назвіть основні види сенсорів лінійного переміщення.
9. Що таке "інклінометр"? Які види інклінометрів Ви знаєте?
10. Що таке “енкодер"? Які види енкодерів Ви знаєте?
11. Що таке "акустичні хвилі"? Чим відрізняються "звуки", "інфразвуки", "ультразвуки", "гіперзвуки"?
12. Назвіть основні види приймачів акустичних сигналів.
13. Які види інтелектуальних акустичних сенсорів Ви знаєте?
14. Чим обумовлені достоїнства сучасних диктофонів?
15. Для чого і де застосовують портативні аналізатори звуків?
16. Що таке "безпровідна гарнітура"? Для чого і як її застосовують?
17. Який принцип роботи спрямованих приймачів звуку?
18. Що таке "лазерний мікрофон"? Як можна від нього захиститися?
19. Як працюють облаштування дистанційного підслуховування за допомогою стетоскопів?
20. Що таке "тонометр"? Чому його відносять до класу акустичних сенсорів? Чому його вважають "активним" сенсором?
21. У чому полягає відмінність електронного тонометра від ручного? Назвіть основні види електронних тонометрів.
22. Які переваги і недоліки автоматичних електронних тонометрів в порівнянні з напівавтоматичними?
23. Що таке "ехолокація", "ехолот"? Чим від них відрізняються поняття "гідролокація" і "гідролокатор"?
24. Для яких цілей і де застосовують гідролокатори?
25. Як працюють УЗ сенсори відстані? Для чого їх застосовують?
26. Чи використовують ехолокацію в твердих тілах? Якщо так, то з якою метою?
27. Поясніть принцип УЗ досліджень органів людського тіла.
28. Назвіть найбільш вражаючі можливості сучасних апаратів для УЗ досліджень людського організму.
29. Розшифруйте абревіатури ПАХ і ППАХ.
30. Що означає “ЗШП"? Де вони застосовуються?
31. Що є "чутлива зона" сенсора на ПАХ?
32. Чому сенсори на ПАХ так охоче застосовують в різних видах мікрохвильового радіозв'язку? Наведіть приклади таких застосувань.
33. За яким принципом класифікують електричні сенсори?
34. Що таке "трансд’юсер"? Чому електричні сенсори часто застосовують в якості трансдьюсеров?
35. Що таке "терморезистори"? Чи є відмінність між "терморезисторами" і "термісторами"?
36. Що таке "фоторезистори"? Поясніть фізичний механізм їх дії. Що таке "спектральна характеристика" фоторезистора?
37. Що таке "п’езорезисторы"? Для чого їх застосовують?

38. Що таке “гігристоры"? Для чого їх застосовують?
39. Що таке "магніторезистивні датчики"? З якого матеріалу їх переважно роблять?

Список рекомендованої літератури

1. Amarasinghe R. et al Design and fabrication of miniaturized six-degree of freedom piezoresistive acceleromete MEMS 2005: 18th IEEE International Conference on microelectromechanical systems. – P. 351 – 354.
2. Anderson R. R., Parrish J. A. The optics of human skin J. Invest. Dermatol. – 1981. – 77. – P. 13 – 19.
3. Bruls W. A. G. and Van der Leun J. C. Forward scattering properties of human epidermal layers. Photochem. Photobiol. – 1984. – 40. – P. 231 – 242.
4. Bruulsema J. T., Essenpreis M., Heinemann L. et al. Detection of Changes in Blood Glucose Concentration in-vivo with Spatially Resolved Diffuse Reflectance. OSA Conf. On Biomedical Optical Spectroscopy and Diagnostics. – 1996.
5. Budnyk M. M., Chaikovsky I. A., Voytovych I. D. et al. Supersensitive magnetocardiographic system for early identification and monitoring of heart diseases (Medical Applications). Управляющие системы и машины. – 2005. – № 3. – С. 50 – 62.
6. Budnyk M. M., Minov Yu. D., Voytovych I. D. et al. Supersensitive magnetocardiographic system for early identification and monitoring of heart diseases (hardware). Управляющие системы и машины. – 2004. – №6. – С. 21 – 30.
7. Budnik N., Sosnitsky V., Vojtovich I. et all. Pulse-relaxation oscillation SQUID-magnitometer. Proc. 13 IMEKO World Congress, Torino (Italy), 1994. – 3. – P. 2383 – 2387
8. Karygiannis and E. Antonakakis, *“MANET and Sensor Network Security”,* ACM/IEEE MSWiM 2006, 9th Annual International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, October 2-6, 2006.
9. K. Wagner, — *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.”* First IEEE International Workshop Sensor Network Protocols and Applications (SNPA'03).
10. Никулин С. А. — Датчики, 2007.
11. Дж. Фрейден — Современные датчики. Справочник.,Москва 2005.
12. Евстифеев А. В. — Микроконтроллеры AVR семейства Tiny и Mega Фирмы «Atmel», Издательский дом —Дюдэка-XXI, 2004.
13. Ivan Stojmenovic, — Hardbook of sensor netwirks algorithms and architectures, Wiley inersciense 2005.
14. Datasheet, 8-bit Microcontroller with 64K/128K/256K Bytes In-System Programmable Flash ATmega1281/V.
15. Datasheet, ZigBee™ IEEE 802.15.4™ Radio Transceiver AT86RF230.

РОЗДІЛ 7. ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ

7.1. Індустрія 4.0

Перша промислова революція була обумовлена появою парових машин. Вона обплутала світ інфраструктурою залізниць.

Друга промислова революція була пов'язана з появою конвеєра та електрики. Вона створила мережу шосе та кабелів у всьому світі.

Третя промислова революція – середина 20-го століття, поява комп'ютерних технологій, цифрова революція, автоматизація виробництва. Ця революція в більшій мірі була пов'язана з інформатизацією і створенням інтернету.

Четверта промислова революція – впровадження кіберфізичних систем і персоналізованого виробництва. Вона поєднує засоби виробництва і власне продукцію. Якщо зараз усі процеси виробництва контролює людина через комп'ютер, то у четвертій промислові революції продукт, який виробляється, сам може взаємодіяти з верстатом, з конвеєром, з споживачем, а сам споживач може на це впливати.

Індустрія 4.0 (Industry 4.0) - провідний тренд «Четвертої промислової революції», яка відбувається на наших очах.

Зараз ми живемо в епоху завершення третьої, цифрової революції, що почалася в другій половині минулого століття. Її характерні риси - розвиток інформаційно-комунікаційних технологій, автоматизація та роботизація виробничих процесів.

Характерні риси Індустрії 4.0 - це повністю автоматизовані виробництва, на яких керівництво всіма процесами здійснюється в режимі реального часу і з урахуванням мінливих зовнішніх умов. Кіберфізичні системи створюють віртуальні копії об'єктів фізичного світу, контролюють фізичні процеси і приймають децентралізовані рішення. Вони здатні об'єднуватися в одну мережу, взаємодіяти в режимі реального часу, самоналагоджуватися і самонавчатися. Важливу роль відіграють інтернет-технології, що забезпечують комунікації між персоналом та машинами. Підприємства виробляють продукцію відповідно до вимог індивідуального замовника, оптимізуючи собівартість виробництва [1].

Розвиток інтернету, інфокомунікаційних технологій (ІКТ), стійких каналів зв'язку, хмарних технологій і цифрових платформ, а також інформаційний «вибух» вирвалися з різних каналів даних, забезпечили появу відкритих інформаційних систем і глобальних промислових мереж, що виходять за межі окремого підприємства і взаємодіючих між собою . Такі системи і мережі надають перетворює вплив на всі сектори сучасної економіки та бізнесу за межами самого сектора ІКТ, і переводять промислову автоматизацію на нову четверту сходинку індустріалізації [2].

Компоненти «Industry 4.0» [3]:

- елементи Інтернету речей;
- штучний інтелект, машинне навчання і робототехніка;
- хмарні обчислення;
- Big Data;
- аддитивное виробництво;
- кібербезпека;
- інтеграційна система;
- моделювання;
- доповнена реальність.

В основі Industry 4.0 лежать *smart manufacture*. На таких підприємствах можна реалізувати виробничі процеси будь-якої складності, при цьому звівши до мінімуму ризик збоїв і забезпечивши ефективне створення «розумних» продуктів. Однією з важливих складових подібних виробництв є безпроводові мережі, які охоплюють всі процеси, машини, ресурси і співробітників, а також дозволяють налагодити обмін даними між компаніями.

В рамках нового виробництва «розумні» продукти можна точно ідентифікувати, дізнатися їх поточний стан, які виробничі процеси вони вже пройшли, а які тільки чекають –

у всіх подробицях. Залежно від отриманої інформації *smart manufacture* вибудовують маршрут прямування продукту і роботу устаткування. Такий підхід дозволяє забезпечити мобільність і поліпшити логістику [4].

Завдяки глобальних мереж «розумні» продукти можна буде відстежувати в протягом усього циклу виробництва в режимі реального часу. У деяких випадках вони навіть зможуть практично автономно контролювати процес свого виробництва, забезпечуючи оптимізацію даних етапів з точки зору логістики, обслуговування та інтеграції з іншими процесами підприємства. Також в подальшому в будь-який момент можна буде інтегрувати в «розумну» продукцію деякі сервісні функції та задати специфічні параметри конструкції, формування замовлення, планування виробництва, експлуатації та утилізації, що особливо важливо при випуску невеликих партій товару.

«Розумні» підприємства будуть здатні враховувати індивідуальні вимоги замовників, в будь-яку хвилину змінюючи режим роботи виробництва і швидко реагуючи на збої в роботі постачальників. Повна прозорість виробничих процесів дозволяє приймати оптимальні рішення і створювати нові бізнес-моделі.

Також для впровадження «Industry 4.0» необхідно розвивати мережеву інфраструктуру, збільшувати пропускну здатність для ресурсоємних додатків і підвищувати якість обслуговування мережі, особливо в тих випадках, коли час виконання завдання критично важливо. Можливий варіант побудови глобальних мереж на «розумному» підприємстві із зазначенням зв'язків між інтелектуальними об'єктами і службами наведено на рисунку 7.1.

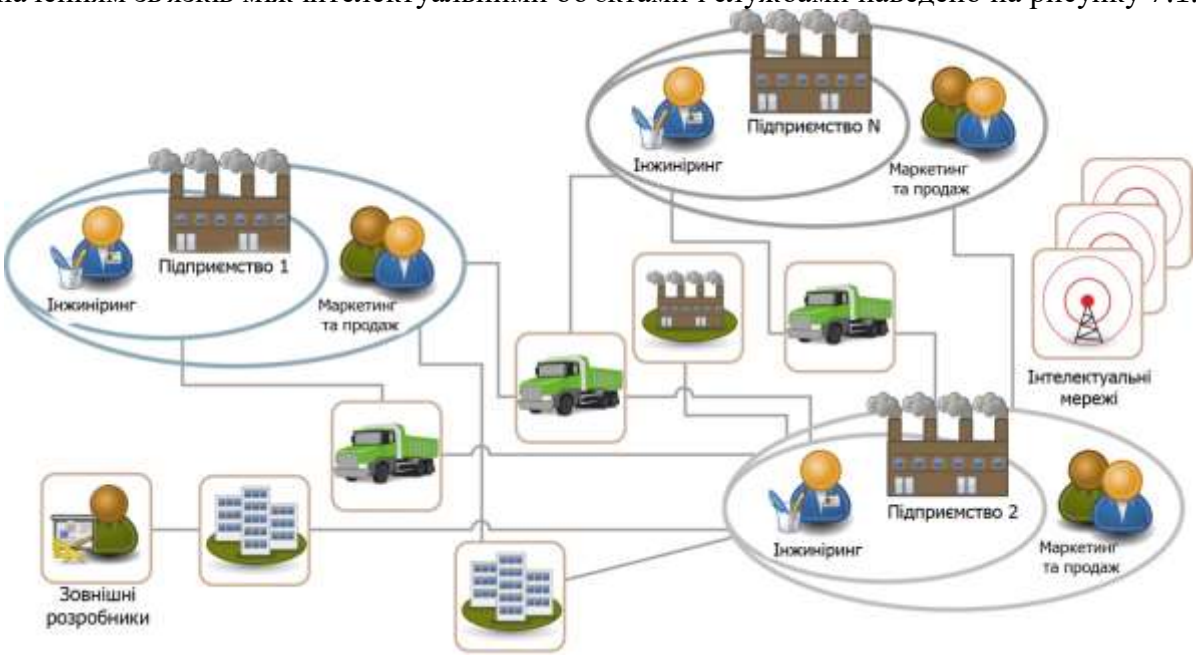


Рис. 7.1. Структура «розумного» підприємства

CPS – це рішення типу «хмара в коробці», призначене для підтримки процесів підприємства і об'єднують їх мереж. За допомогою додатків, наданих цією платформою, можна буде забезпечити надійний зв'язок між співробітниками, об'єктами і системами. Такі додатки передбачають [5]:

- *гнучкість, продуктивність і простоту використання розроблених сервісів;*
- *легке розгортання моделі бізнес–процесів безпосередньо з App Store;*
- *комплексне, безпечне і надійне резервне копіювання всіх бізнес–процесів;*
- *безпеку і надійність всього виробничого процесу – від датчиків до призначених для користувача мереж;*
- *підтримку мобільних платформ і пристроїв;*
- *підтримку спільного виробництва, процесів обслуговування, аналізу і прогнозування в мережах.*

При розробці сервісів і додатків на CPS-платформах необхідно враховувати вимоги вертикальної і горизонтальної інтеграції. При цьому в рамках «Industry 4.0» оркестровка має більш широкий зміст, ніж в разі веб–сервісів: створення загальних служб і додатків повинно бути частиною спільної роботи компаній. Умовний варіант побудови глобальних мереж на базі CPS-платформи із забезпеченням зв'язку між інтелектуальними об'єктами представлений на рисунку 7.2.

Рис. 7.2. Основні об’єкти Industry 4.0

Експерти виділяють чотири базових технології, в результаті впровадження яких очікуються революційні зміни.

Інтернет речей (Internet of Things, IoT). У цій технології Інтернет використовується для обміну інформацією не тільки між людьми, але і між різними «речами», тобто машинами, пристроями, датчиками і т.д. З одного боку, речі, забезпечені датчиками, можуть, обмінюватися даними і обробляти їх без участі людини. З іншого боку, людина може активно брати участь в цьому процесі, наприклад, коли мова йде про «розумний будинок».

Різновидом IoT є *промисловий (індустріальний) інтернет речей (Industrial Internet of Things, IIoT).* Саме він відкриває пряму дорогу до створення повністю автоматизованих виробництв. Починається все з того, що ключові компоненти обладнання забезпечуються різними датчиками, виконавчими механізмами і контролерами; зібрані дані обробляються і надсилаються до відповідних служб підприємства, що дозволяє персоналу оперативно приймати обґрунтовані і виважені рішення. Але завдання-максимум полягає в досягненні такого рівня автоматизації підприємства, при якому на всіх ділянках, де це можливо, машини працюють без участі людей. Роль персоналу при цьому зводиться до контролю роботи машин і реагування лише на екстрені ситуації [6].

Цифрові екосистеми. Це системи, що складаються з різних фізичних об'єктів, програмних систем і керуючих контролерів, що дозволяють уявити таке утворення як єдине ціле. Фізичні та обчислювальні ресурси в такий екосистемі тісно пов'язані, моніторинг і управління фізичними процесами здійснюється з використанням технологій IIoT. Традиційні інженерні моделі гармонійно співіснують з комп'ютерними.

Аналітика великих даних (Data Driven Decision) або просто Великі дані (Big data). Величезні обсяги інформації, що накопичуються в результаті «оцифровування» фізичного світу, можуть бути ефективно оброблені тільки комп'ютерами (в майбутньому, можливо, квантовими), із застосуванням хмарних обчислень і технологій штучного інтелекту (Artificial Intelligence). В результаті людина, яка контролює той чи інший процес, ситуацію, обстановку

має отримувати оброблені дані, максимально зручні для сприйняття, аналізу і ухвалення рішення.

Складні інформаційні системи, відкриті для використання клієнтами і партнерами (цифрові платформи). Це можуть бути цифрові платформи і системи для управління бізнес-процесами, для інтеграції інтернету речей в фізичні бізнес-процеси, для аналізу і прогнозування стану обладнання і т.д.

Четверта промислова революція, крім перерахованих вище сфер прискореного розвитку, може також задіяти широке впровадження 3D-друку, друкованої електроніки, застосування розподілених реєстрів (тобто технології блокчейн, яка стала популярною після створення на її основі криптовалюта), використання віртуальної і доповненої реальності і навіть розробку автономних роботів, які будуть не компонентами автоматизованих ліній, як зараз, а цілком мобільними високоінтелектуальними пристроями, здатними працювати поруч з людьми [7].

За прогнозами Всесвітнього Економічного Форуму, більшість технологій Четвертої революції стане повсякденністю вже в 2027 році. А це означає, що з'являться не тільки розумні будинки, а й розумні міста, безпілотні автомобілі на вулицях, штучний інтелект в офісах і суперкомп'ютери в кишенях [8].

Вперше про програму «Індустрія 4.0» мова зайшла у 2011 році на промисловій виставці в Ганновері, де уряд Німеччини поставив задачу розширити застосування інформаційних технологій у виробництві. Над створенням програми модернізації промислових підприємств країни в цьому напрямку працювала високопрофесійна команда, до якої увійшли представники бізнесу і держави. Мета програми - збереження і збільшення конкурентних переваг підприємств країни.

7.2. Промисловий Інтернет Речей

Принципи побудови "Індустрії 4.0"

Ключовою технологією програми *Індустрія 4.0* вважається Інтернет Речей.

Складовою частиною Інтернету Речей і його головною на даному етапі розвитку технологій рушійною силою є *Промисловий (або Індустріальний) Інтернет Речей (Industrial Internet of Things, IIoT).*

Промисловий Інтернет Речей - це система об'єднаних комп'ютерних мереж і підключених до них промислових (виробничих) об'єктів з вбудованими датчиками і програмним забезпеченням для збору та обміну даними, з можливістю віддаленого контролю і управління в автоматизованому режимі, без участі людини.

На першому етапі впровадження IIoT на промислове обладнання встановлюють датчики, виконавчі механізми, контролери та людино-машинні інтерфейси. В результаті стає можливим збір інформації, яка дозволяє керівництву отримувати об'єктивні і точні дані про стан виробництва. Оброблені дані надаються всім підрозділам підприємства. Це допомагає налагодити взаємодію між співробітниками різних підрозділів і приймати обґрунтовані рішення.

Отримана інформація може бути використана для запобігання позаплановим простоям, поламкам устаткування, скороченню позапланового техобслуговування та збоям в управлінні ланцюжками поставок, тим самим дозволяючи підприємству функціонувати більш ефективно.

При обробці величезного масиву неструктурованих даних, що надходять з датчиків, їх фільтрація і адекватна інтерпретація стає пріоритетним завданням. Тому особливого значення набуває представлення інформації в зрозумілому користувачеві вигляді. Для цього використовуються передові аналітичні платформи, призначені для збору, зберігання і аналізу даних про технологічні процеси і події, що відбуваються в реальному масштабі часу [1].

Промисловий Інтернет Речей дозволяє створювати виробництва, які виявляються більш ощадливими, гнучкими і ефективними, ніж існуючі. Бездротові пристрої з підтримкою

протоколу IP, включаючи смартфони, планшети і датчики, вже активно використовуються на виробництві. Наявні дротові мережі датчиків в найближчі роки будуть розширені і доповнені бездротовими мережами, завдяки чому на підприємствах суттєво розширяться зони застосування систем моніторингу та управління. Наступний етап оптимізації виробничих процесів буде характеризуватися все більш щільною конвергенцією кращих інформаційних і операційних технологій.

Було сформульовано кілька основних принципів побудови "Індустрії 4.0", дотримуючись яких компанії можуть впроваджувати сценарії четвертої промислової революції на своїх підприємствах.

Перший — це сумісність, що означає здатність машин, пристроїв, сенсорів та людей взаємодіяти один з одним через інтернет речей (IoT).

Це веде до наступного принципу — *прозорості, яка з'являється у результаті такої взаємодії.* У віртуальному світі створюється цифрова копія реальних об'єктів, систем, функцій, яка точно повторює все те, що відбувається з її фізичним клоном. Внаслідок цього накопичується максимально вичерпна інформація про всі процеси, які відбуваються з обладнанням, "розумними" продуктами, виробництвом у цілому і так далі. Для цього потрібно забезпечити можливість збору всіх цих даних із сенсорів та датчиків, а також з обліку контексту, у якому вони генеруються.

Технічна підтримка — третій принцип "Індустрії 4.0". Комп'ютерні системи допомагають людям приймати рішення завдяки збору, аналізу та візуалізації всієї інформації, про яку говорилося вище. Ця підтримка також може полягати у повному заміщенні людей машинами при виконанні небезпечних чи рутинних операцій [9].

Четвертий принцип — деталізація управлінських рішень, делегування деяких із них кіберфізичним системам. Ідея полягає в тому, щоб автоматизація була настільки повною, наскільки це взагалі можливо: всюди, де машина може ефективно працювати без втручання людей, рано чи пізно повинно відбутися заміщення людини машиною. Співробітникам при цьому відводиться роль контролерів, які можуть приєднатися в екстрених ситуаціях.

Внаслідок переходу промисловості на ці принципи відбуваються також зміни у бізнес-моделях. Так, замість того, аби сфокусуватись на заощадливому виробництві, компанії прагнуть запровадити випуск персоналізованої масової продукції за принципом Agile і переходять на випуск партій розміром в один-єдиний продукт. При цьому зберігається принцип економії: роботизоване виробництво більш енергоефективне, воно супроводжується меншою кількістю відходів та браку.

Трансформація виробничої галузі називається революцією саме тому, що зміни відбуваються не поверхневі, а радикальні: індустрія перебудовується згори донизу. Змінюються бізнес-моделі, народжуються нові компанії, а всесвітньовідомі бренди з довгою історією просто зникають, якщо не встигають вступити до лав цифрових революціонерів. Клієнти змінили свою поведінку, вони хочуть індивідуального підходу та унікальних товарів [10].

Підприємствам, що звикли виробляти однакові речі, доводиться змінюватись. Впровадження принципів "Індустрії 4.0" дозволяє отримати низку переваг, що не були доступні в традиційних моделях минулого. Наприклад, тепер компанії можуть досягнути індивідуального підходу та персоналізувати замовлення згідно з особистим уподобанням клієнтів, що стрімко підвищує їхню лояльність. Старі заводи та фабрики перетворюються на "розумні" та починають випускати буквально унікальні продукти за індивідуальним замовленням. При цьому знижуються питомі витрати на виробництво одиниці продукції, компанії отримують можливість продукувати унікальний персоналізований продукт за ціною масового стандартизованого продукту.

Приклади впровадження IioT

За індивідуальним замовленням можуть вироблятись і двигуни, і сервери, і взагалі будь-що. На заводі *Fujitsu Siemens* у німецькому місті Аугсбург випускаються комп'ютерні системи та сервери буквально в одному екземплярі для конкретного замовника.

Витрати на випуск продукції за індивідуальним замовленням на підприємстві з високим рівнем автоматизації невеликі: якщо раніше під кожну таку пару кросівок довелося б переналаштовувати обладнання вручну, то зараз комп'ютерна система за лічені секунди робить це самостійно. Роботизація заводів *Tesla,* що випускають електромобілі, дозволила компанії розгорнути виробництво не в Китаї, а в Каліфорнії. Це виявилось дешевше, ніж оплачувати працю китайських робітників і транспортування готових машин. Четверта промислова революція не тільки змінює бізнес окремих компаній — вона впливає на розстановку сил на глобальному рівні. Хто б міг подумати, що виробник автомобілів, якому немає й десяти років (*Tesla* заснована у 2008 році), зможе обігнати по капіталізації лідера другої промислової революції, яка відбулась у результаті винаходу конвеєра та переходу на масове виробництво, — *Ford Motors* [11].

Завдяки новим технологіям й інший відомий виробник — компанія *Adidas* — переносить своє виробництво назад до Німеччини. На новій фабриці всі операції будуть виконувати роботи. Це не тільки оптимізує виробництво, але й суттєво збільшить швидкість.

Рис. 7.3. Роботизація заводів Tesla, що випускають електромобілі, дозволила компанії розгорнути виробництво не в Китаї, а в Каліфорнії

По мірі становлення цифрових екосистем виробничі підприємства з ізольованих систем, які самостійно виконують всі необхідні для виробництва продукції виробничі та бізнес-процеси, будуть перетворюватися у відкриті системи, що поєднують різних учасників ринку; управляти засобами виробництва в цих системах буде не персонал, а хмарні сервіси, кінцева мета всіх цих трансформацій - не випуск продукції, а надання послуг споживачеві.[3]

Вважається, що IIoT-рішення дозволяють підвищити ефективність виробництва в кілька разів, а термін окупності таких проектів в більшості випадків не перевищує декількох місяців.

Наприклад, обладнання заводу *Philips* з виробництва бритв (Голландія) працює в неосвітленому приміщенні, де встановлені 128 роботів. Весь персонал заводу складається з дев'яти працівників [4].

Яскравим прикладом застосування Промислового Інтернету Речей є проект компанії *Harley Davidson*, яка виробляє знамениті мотоцикли. Основною проблемою, з якою зіткнулася компанія, була повільна реакція на запити споживачів в умовах зростаючої конкуренції і обмежена можливість кастомізації дилерами п'яти моделей, що випускаються. У період з 2009 по 2011 рік компанія провела масштабну реконструкцію своїх виробничих майданчиків. В результаті була створена єдиний складальний майданчик, що випускає мотоцикли всіх п'яти моделей з можливістю їх кастомізації, при цьому замовнику пропонується вибір з понад 1300 варіантів [12].

В ході всього виробничого процесу використовуються датчики, керовані системою класу MES. Кожен верстат, кожна деталь має радіопозначку, яка однозначно ідентифікує виріб і його виробничий цикл. Дані від датчиків передаються в платформу обробки даних, що виконує роль інтеграційної шини для збору даних з датчиків і різних інформаційних систем, як внутрішніх виробничих і бізнес-систем компанії *Harley Davidson*, так і інформаційних систем контрагентів компанії.

В результаті *Harley Davidson* досягла вражаючих результатів [13]:

- виробничий цикл вдалося скоротити з 21 дня до 6 годин (кожні 89 секунд з конвеєра сходить мотоцикл, повністю налаштований під свого майбутнього власника);
- реалізовано наскрізне управління виробом (мотоцикл) на всьому його життєвому циклі;
- вартість акцій компанії виросла більш ніж в 7 разів: з рівня 10 доларів в 2009 році до 70 доларів в 2015 році.

Тенденції та технології

Крейг Резник (Craig Resnick), провідний аналітик відомої аналітичної компанії *ARC Advisory Group*, вважає, що в розвитку Промислового Інтернету Речей станом на початок 2017 року простежувалися шість основних тенденцій [14].

1. Головними складовими IIoT стають *передові аналітичні інструменти, штучний інтелект та машинне навчання*. Багато підприємств давно використовують платформи бізнес-аналітики (BI) та інструменти інтелектуального виробництва (EMI). Тепер, завдяки IIoT, виробничники можуть використовувати передові аналітичні інструменти (advanced analytics), штучний інтелект і машинне навчання для оперативного управління на випередження і прийняття рішень на основі поглибленої аналітики. Завдяки цьому Промисловий Інтернет Речей стає стратегічним інструментом, спрямованим на поліпшення виробничих показників [15].

2. *Все більше інтелектуальних пристроїв з'являється «на кордоні».* Переміщення коштів аналітики на «передній край» мережі і, таким чином, ближче до джерел даних, допоможе поліпшити якість виробництва і продукції. Завдяки появі недорогих датчиків і процесорів з'являється можливість збирати і обробляти все більше даних про виробництво «на фронтирі». Граничні (туманні) обчислення з вбудованою аналітикою стають прийнятною альтернативою також у випадках, коли небезпечно запускати аналітику в хмарі або від хмарного рішення відмовилися з якихось інших причин [16].

3. *Поява цифрових двійників.* Завдяки впровадженню технологій IIoT стає можливим створення цифрової копії фізичного об'єкта, яку іноді називають «цифровий двійник». Цю копію використовують для моделювання, тестування і оптимізації даного фізичного об'єкта у віртуальному середовищі перед тим, як застосовувати його в реальному середовищі [17].

4. Аналогічно, дані, що надходять в реальному масштабі часу від інтегрованих в фізичні об'єкти датчиків або від інших джерел, можуть використовуватися для вирішення аналітичних задач, таких як моніторинг стану, діагностика відмови, відповідно до якої і складається аналітика. Отримане в результаті знання може підвищити цінність виробничих активів підприємства за рахунок:

– підвищення ефективності їх використання;

– скорочення часу простою;

– попередження відмов;

– забезпечення безперервних поліпшень продукції в процесі проектування і виробництва.

5. *IIoT допомагає розвивати технології доповненої і віртуальної реальності (AR / VR).*

Підготовка нового персоналу за допомогою симуляторів може стати ефективним способом навчання [18]. Застосовувані в IIoT технології, такі як ігри, доповнена / віртуальна реальність і 3D-занурення з використанням переносних пристроїв, можуть з високим ступенем достовірності імітувати реальну обстановку на підприємстві, функції працівників, елементи управління і фізичні об'єкти.

6. *MQTT як основний протокол обміну повідомленнями в IioT. MQTT (Message Queue Telemetry Transport)* - це спрощений протокол обміну даними, що працює поверх TCP / IP. Він добре підходить для використання в контролерах і датчиках, де потрібно невеликий розмір коду і існують обмеження по пропускній здатності каналу. Така ситуація є типовою для IIoT, тому MQTT розглядається як основний протокол Промислового Інтернету Речей [19].

7.3. Machine Learning

Машинне навчання (МО, Machine Learning, ML) - великий підрозділ штучного інтелекту, що вивчає методи побудови алгоритмів, здатних навчатися [20].

Першу програму на основі алгоритмів, здатних самонавчатися, розробив *Артур Самуель (Arthur Samuel)* в 1952 році, призначена вона була для гри в шашки. Самуель дав і перше визначення терміну «машинне навчання»: це «область досліджень розробки машин, які не є заздалегідь запрограмованими». Більш точне визначення терміну «навчання» дав набагато пізніше *Т. М. Мітчелл*: кажуть, що комп'ютерна програма навчається на основі досвіду *E* по відношенню до деякого класу задач *T* і заходи якості *P*, якщо якість вирішення завдань з T, виміряний на основі P, поліпшується з набуттям досвіду *E* [21].

Вже в 1957 році була запропонована перша модель нейронної мережі, що реалізує алгоритми машинного навчання, схожі на сучасні. В даний час ведеться розробка самих різних систем машинного навчання, призначених для використання в таких технологіях майбутнього, як Інтернет Речей, Промисловий Інтернет Речей, в концепції «розумний» місто, при створенні безпілотного транспорту і в багатьох інших.

Про те, що на машинне навчання зараз покладають великі надії, свідчать такі факти [22].

- В компанії *Google* вважають, що скоро її продукти «перестануть бути результатом традиційного програмування - в їх основу буде покладено машинне навчання»;
- Компанії *Google, Facebook, Apple, Amazon, Microsoft* і китайська фірма *Baidu* вступили в боротьбу за талановитих фахівців у сфері штучного інтелекту;
- *Марк Цукерберг*, генеральний директор *Facebook*, особисто - по телефону і по відеочату - бере участь в спробах його компанії переманити найкращих випускників;
- Відвідуваність на найважливіших академічних конференціях в цій сфері збільшилася майже в чотири рази;
- Такі нові продукти, як *Siri* від *Apple, M* від *Facebook, Echo* від *Amazon* були створені за допомогою машинного навчання [4].

У найзагальнішому випадку розрізняють два типу машинного навчання: *навчання по прецедентах, або індуктивне навчання, і дедуктивне навчання*. Оскільки останнє прийнято відносити до області експертних систем, то терміни «машинне навчання» і «навчання по прецедентах» можна вважати синонімами. Цей метод навчання зараз, як прийнято говорити, в тренді, а ось експертні системи переживають кризу. Бази знань, що лежать в їх основі, важко узгоджувати з реляційною моделлю даних, тому промислові СУБД неможливо ефективно використовувати для наповнення баз знань експертних систем.

Навчання по прецедентах, в свою чергу, поділяють на три основних типи: контрольоване навчання, або навчання з учителем (*supervised learning*), неконтрольоване навчання (unsupervised learning), або навчання без учителя, і навчання з підкріпленням (*reinforcement learning*) [5].

Методи машинного навчання

Крім названих, розробляються і інші методи навчання: активне, багатозадачне, різноманітне, трансферне і т.д. Особливо успішно розвивається в останні роки «глибоке навчання», при використанні якого можуть успішно поєднуватися алгоритми навчання з вчителем і без вчителя.

Контрольоване навчання

Цей метод навчання застосовується у випадках, коли є великі обсяги даних, припустимо - тисячі фотографій домашніх тварин з маркерами (мітками, ярликами): це кішка, а це собака. Необхідно створити алгоритм, за допомогою якого машина могла б по фотографії, яку «не бачила» раніше, визначити, хто на ній зображений: кішка або собака. У ролі «вчителя» в даному випадку виступає людина, яка заздалегідь проставила маркери. Машина сама вибирає ознаки, за якими вона відрізняє кішок від собак. Тому в подальшому знайдений нею алгоритм може бути швидко переналаштований на рішення іншої задачі, наприклад, на розпізнавання курей і качок.

Машина знову-таки сама виконає складну і копітку роботу по виділенню ознак, за якими буде розрізняти цих птахів. А нейромережа, яку навчили розпізнавати кішок, можна швидко навчити обробляти результати комп'ютерної томографії.

Неконтрольоване навчання

Хоча маркованих, розмічених даних накопичилося вже досить багато, даних без маркерів (міток) все ж набагато більше. Це зображення без підписів, аудіозаписи без коментарів, тексти без анотацій. Завдання машини при неконтрольованому навчанні - знайти зв'язку між окремими даними, виявити закономірності, підібрати шаблони, упорядкувати дані або описати їх структуру, виконати класифікацію даних.

Неконтрольоване навчання використовується, наприклад, в рекомендаційних системах, коли в інтернет-магазині на основі аналізу попередніх покупок покупцеві пропонуються товари, які можуть зацікавити його з більшою ймовірністю, ніж інші. Або коли на після перегляду якогось відеокліпу на порталі *YouTube* відвідувачеві пропонують десятки посилань на ролики, чимось схожі на переглянутий. Або коли *Google* у відповідь на один і той же запит ранжує посилання в результатах пошуку для одного користувача інакше, ніж для іншого, оскільки враховує історію пошуків.

Навчання з підкріпленням

Таке навчання є окремим випадком контрольованого навчання, але вчителем в даному випадку є «середовище». Машина (її в цій ситуації часто називають «агент») не має попередньої інформацією про середовище, але має можливість здійснювати в ній будь-які дії. Середовище реагує на ці дії і тим самим надає агенту дані, які дозволяють йому реагувати на них і вчитися. Фактично агент і середовище утворюють систему зі зворотним зв'язком.

Навчання з підкріпленням використовується для вирішення більш складних завдань, ніж навчання з учителем і без вчителя. Воно використовується, наприклад, в системах навігації для роботів, які навчаються уникати зіткнень з перешкодами шляхом набуття досвіду, отримуючи зворотний зв'язок при кожному зіткненні. Навчання з підкріпленням використовується також в логістиці, при складанні графіків і плануванні завдань, при навчанні машини логічним іграм (покер, нарди, го і ін.).

Нейронні мережі і глибоке навчання

Для машинного навчання використовують різні технології та алгоритми. Зокрема, можуть застосовуватися дискримінантний аналіз, байєсовські класифікатори та багато інших математичних методів. Але в кінці XX століття все більше уваги почали приділяти штучним нейронним мережам (ANN). Черговий вибух інтересу до них почався в 1986 році, після істотного розвитку т.зв. «Методу зворотного поширення помилки», який з успіхом застосували при навчанні нейронної мережі.

ANN є системою з'єднаних і взаємодіючих між собою штучних нейронів, виконаних на основі порівняно простих процесорів. Кожен процесор ANN періодично отримує сигнали від

одних процесорів (або від сенсорів, або від інших джерел сигналів) і періодично посилає сигнали іншим процесорам. Всі разом ці прості процесори, з'єднані в мережу, здатні вирішувати досить складні завдання.

Найчастіше нейрони розташовуються в мережі за рівнями (їх ще називають шарами). Нейрони першого рівня - це, як правило, вхідні. Вони отримують дані ззовні (наприклад, від сенсорів системи розпізнавання осіб) і після їх обробки передають імпульси через синапси нейронів на наступному рівні. Нейрони на другому рівні (його називають прихованим, оскільки він безпосередньо не пов'язаний ні з входом, ні з виходом ANN) обробляють отримані імпульси і передають їх нейронам на вихідному рівні. Оскільки мова йде про імітацію нейронів, то кожен процесор вхідного рівня пов'язаний з декількома процесорами прихованого рівня, кожен з яких, в свою чергу, пов'язаний з декількома процесорами рівня вихідного. Така архітектура найпростішої ANN, яка здатна до навчання і може знаходити прості взаємозв'язку в даних.

Глибоке (глибинне) навчання може бути застосоване лише по відношенню до більш складних ANN, що містить кілька прихованих рівнів. При цьому рівні нейронів можуть чергуватися з шарами, які виконують складні логічні перетворення. Кожен наступний рівень мережі шукає взаємозв'язки в попередньому. Така ANN здатна знаходити не тільки прості взаємозв'язки, а й взаємозв'язки між взаємозв'язками. Саме завдяки переходу на нейромережу з глибинним навчанням компанії Google вдалося різко підвищити якість роботи свого популярного продукту «Перекладач». Зокрема, якість перекладу між англійською та французькою мовами підвищився відразу на 7 балів, тобто більш ніж на 20%. Попередня система, яка виконувала фразовий статистичний машинний переклад, домоглася подібного поліпшення за весь час свого існування (з 2006 року) [23].

Машинне навчання для бізнесу

Ринок машинного навчання швидко зростає. З 2016 року його обсяг подолав позначку в $1 млрд, а до 2025 року, судячи з прогнозів, він може збільшитися до $39,98 млрд.[7]

В кінці 2016 року *MIT Technology Review і Google Cloud* провели спільне дослідження на тему «Машинне навчання: новий спосіб отримати конкурентну перевагу». Було опитано 375 кваліфікованих респондентів з різних країн світу, які працюють в дрібних і великих компаніях з різних галузей (промисловість, послуги, фінанси). В результаті дослідження з'ясувалося, що 60% компаній вже використовують машинне навчання (ML), а в третини з них ця технологія перейшла зі стадії інноваційної в стадію зрілості. Більш того, 26% компаній вже отримують за рахунок ML конкурентну перевагу. Чверть компаній інвестують в ML понад 15% від коштів, спрямованих на розвиток IT, і в значній мірі повертають зроблені інвестиції [24].

Машинне навчання і, зокрема, нейронні мережі доцільно використовувати для вирішення бізнес-завдань у випадках, коли:

- накопичено велику кількість різних даних, але програми для їх обробки і систематизації відсутні;
- наявні дані спотворені, не повні або не систематизовані;
- дані настільки різні, що важко виявити зв'язку і закономірності, що існують між ними.

Бізнес-завдання, які можуть вирішуватися засобами машинного навчання і нейронних мереж:

- Прогнозування: попиту, обсягу продажів, наповнення складу, завантаження устаткування і інших ресурсів, подальшого розвитку підприємства і т.п.
- Виявлення: тенденцій, прихованих взаємозв'язків, аномалій, повторюваних елементів і т.п.
- Розпізнавання: фото-, відео-, аудіоконтенту, спроб шахрайства, брехні, внутрішніх загроз, зовнішніх атак на систему безпеки і т.п.
- Автоматизація: роботи операторів в онлайн-чатах, телефонних операторів і т.п.
- Класифікація: аналіз складу покупців, клієнтів, замовників і сегментація їх за різними параметрами.

- Кластеризація: класифікація за параметрами, які з самого початку не були відомі.
- Розробка: чат-ботів [20].

Серед компаній з українським корінням слід зазначити стартап *Neuromation*, який в лютому 2017 року під час ICO залучив $71,6 млн. інвестицій.

Платформа *Neuromation* дозволяє створювати штучне навчальне середовище для глибокого навчання нейронних мереж на великій кількості прикладів. Дані для навчання ANN генеруються з використанням обчислювальних потужностей блокчейн-спільноти. Настільки оригінальне рішення компанія прийняла тому, що раніше, в процесі роботи над системами з використанням комп'ютерного зору, зіткнулася з проблемою браку обчислювальних ресурсів. Оренда ресурсів у хмарних сервісів *Amazon* або *Google* для стартапу виявилася непідйомною. А через бум майнінгу було практично неможливо купити відеокарти. Так з'явилася ідея брати обчислювальні потужності в оренду у майнерів, яка в підсумку перетворилася на створення нейроплатформи [20].

7.4. Smart Factory - розумне виробництво

Поняття «розумна фабрика» (*Smart Factory*), «розумне виробництво» (*Smart Manufacturing*), «фабрика майбутнього» (*Factory of the Feature*) з'явилися зовсім нещодавно і поки не мають строго визначених значень. Зараз вони використовуються як синоніми, хоча поняття «фабрика майбутнього» більш об'ємне і включає в себе не тільки «розумні виробництва», але також віртуальні та цифрові підприємства.

Національний інститут стандартів і технологій США (NIST) визначає термін *Smart Manufacturing* так: це «повністю інтегровані корпоративні виробничі системи, які здатні в реальному масштабі часу реагувати на мінливі умови виробництва, вимоги мереж поставок і задовольняти потреби клієнтів» [21]. У цьому визначенні головне: «в реальному масштабі часу», тобто максимально оперативно, досягаються названі цілі за рахунок інтенсивного і всеосяжного використання інформаційних технологій і кіберфізичних систем на всіх етапах виробництва продукції та її поставки.

«*Розумне виробництво*», поряд з Промисловим Інтернетом Речей, лежить в основі *Індустрії 4.0 (Industrie 4.0).* Таку назву отримала програма німецького уряду з розвитку високих технологій. Характерна риса Індустрії 4.0 - повністю автоматизовані виробництва, на яких керівництво всіма процесами здійснюється в реальному масштабі часу і з урахуванням мінливих зовнішніх умов.

Оскільки поняття «*розумне виробництво*» досить розпливчасте (іноді під ним розуміють активну роботизацію, автоматизацію більшості виробничих і управлінських процесів і навіть просто інновації), а перехід до нього відбувається в кілька етапів, що займають не один рік, робляться спроби розділити це поняття на три. Так, Е. Філос, координатор ІКТ-проектів в сьомий рамковій програмі Європейського Союзу з науково-технічного співробітництва, розділяє фабрики майбутнього на три основних типи - *цифрові (Digital), «розумні» (Smart) і віртуальні (Virtual)*[18].

Digital Factory

Основне завдання Цифровий Фабрики - розробка моделей, що випускаються з використанням засобів цифрового проектування і моделювання. Названі засоби починають використовувати ще на стадії досліджень і розробок, а закінчують створенням *«цифрового макета» (Digital Mock-Up, DMU), «цифрового двійника» (Digital Twin),* дослідницького зразка, випуском дрібної серії або окремих виробів, кастомізованих під вимоги замовника.

Основні системи та технології:

- *Системи CAD/CAM/CAE, що об'єднуються російськомовним терміном САПР (система автоматизованого проектування)*
- *PDM (Product Data Management) - система управління даними про виріб*
- *PLM (Product Lifecycle Management) - прикладне програмне забезпечення дляуправління життєвим циклом продукції*

- *Верстати з ЧПУ*
- *3D-принтери і інші адитивні технології.*

«Розумні» фабрики націлені на серійний випуск виробів, але при збереженні максимальної гнучкості виробництва. Забезпечується це завдяки високому рівню автоматизації і роботизації підприємства. Широко застосовуються автоматизовані системи управління технологічними та виробничими процесами. Технології Промислового Інтернету Речей (IIoT) забезпечують міжмашинну взаємодію обладнання. Виробничі активи підприємства, забезпеченого датчиками і засобами зв'язку, що працюють по протоколу IPv6, здатні випускати продукцію майже (або зовсім) без участі людини. Справитися з різко збільшеними потоками інформації, які надходять від датчиків і автоматизованих систем управління, дозволяють технології обробки великих даних (Big Data).

Основні системи та технології:

- АСУТП - автоматизована система управління технологічними процесами
- APS (Advanced Planning and Scheduling) - синхронне (вдосконалене) планування виробництва
- MES (Manufacturing Execution System) - система управління виробничими процесами
- IIoT ((Industrial Internet of Things) - промисловий (індустріальний) інтернет речей
- Big Data - великі дані.

Віртуальна фабрика - це мережа цифрових і «розумних» фабрик, в яку включені також постачальники матеріалів, компонентів і послуг. Для управління глобальними ланцюгами постачання й розподіленими виробничими активами на такий фабриці використовується ряд автоматизованих систем управління підприємством. При належному ступені інтеграції вони дозволяють розробляти і використовувати віртуальну модель всіх організаційних, технологічних, логістичних та інших процесів, що проходять не тільки на підприємстві, але на рівні розподілених виробничих активів і глобальних ланцюжків постачань, аж до післяпродажного обслуговування.

Основні системи та технології:

- ERP (Enterprise Resource Planning) - планування ресурсів підприємства
- CRM (Customer Relationship Management) - система управління взаємовідносинами з клієнтами
- SCM (Supply Chain Management) - управління ланцюжками постачання.

Фінансові перспективи та етапи впровадження

Потенціал зростання світового ринку «фабрик майбутнього» величезний. Обсяг ринку цифрових фабрик (PLM-системи, адитивні технології, апаратне і числове програмне забезпечення, верстати і т.д.) досягне, за різними оцінками, 260 млрд. доларів до 2020 року і 740 млрд. доларів до 2035 року. Обсяг ринку «розумних фабрик» - відповідно 490 млрд. доларів і 1,35 трлн. доларів. За віртуальним фабрикам експерти очікують зростання в 690 млрд. доларів до 2020 року і майже 1,5 трлн. доларів через 20 років [23].

Можливо, вже реалізуються проекти побудови нових підприємств, максимально наближених до реалізації концепції *Smart Factory* і навіть *Virtual Factory*, проте переклад вже працюючих підприємств на нові принципи планування, виробництва, поставок і післяпродажного обслуговування продукції буде здійснюватися поступово і з максимальним використанням вже наявних виробничих активів. Послідовність переходу істотно залежить від специфіки роботи підприємства і доступності нових технологій

У компанії IT-Enterprise виділяють наступні етапи, які потрібно пройти для того, щоб реалізувати концепцію Smart Factory і закласти основи для подальшого переходу до Virtual Factory[23].

- *Цифровізація виробництва*. Забезпечення персоналу мобільними платформами, установка на обладнання датчиків і промислових контролерів. Установка нового обладнання, яке спочатку вже оснащене цифровими інтерфейсами. Ідентифікація фізичних об'єктів підприємства.

- *Забезпечення мережевої взаємодії.* Завдання збору даних з датчиків в реальному масштабі часу можна вирішити за рахунок підключення всіх пристроїв і датчиків до платформи IT-Enterprise.IIoT. Оперативний обмін інформацією між співробітниками забезпечує корпоративна соціальна мережа IT-Enterprise.Hubber.
- *Побудова цифрового двійника підприємства (digital twin).* Рішення завдання візуалізації реального стану справ на підприємстві. Вироблення чітких правил, за якими можна виявити відхилення від норми, що відбулися при виконанні виробничих і бізнес-процесів. ERP-система IT-Enterprise дозволяє дуже детально і оперативно візуалізувати і відстежувати стан провадження у всьому холдингу, по підприємству, показники роботи підрозділів і конкретного обладнання.

Забезпечення за допомогою мобільних платформ синхронізації даних автоматизованої системи планування та даних, отриманих від обладнання, оперативне корегування планів. Забезпечення достовірності та корисності оперативної інформації.

- *Перехід до завдань планування в реальному масштабі часу на основі достовірної інформації про хід виробничих процесів.*
- *Забезпечення автоматичної реакції системи управління на більшість виробничих ситуацій*. Тобто це рішення, яке вироблено індивідуально для конкретного обладнання, яке індивідуально налаштовується і завдяки цьому система зможе запускати автоматичні реакції на виробничі події з виробництва.

Компанія IT-Enterprise пропонує не тільки розвинену ERP-систему, але також й інші рішення, які дозволили б розпочати перехід до технологій Virtual Factory: CRM, SCM і ін.

7.5. Віртуальна реальність

Технології віртуальної реальності з’явились нещодавно, а терминологія ще не укорінилась.

Віртуальна реальність *(BP, virtual reality, VR, штучна реальність)* - створений технічними засобами світ, який передається людині через її відчуття: зір, слух, дотик і інші. Віртуальна реальність імітує як вплив, так і реакції на вплив. Для створення переконливого комплексу відчуттів реальності комп'ютерний синтез властивостей і реакцій віртуальної реальності проводиться у реальному часі [24].

Не слід плутати віртуальну реальність із доповненою. Їх принципова відмінність у тому, що віртуальна конструює новий штучний світ, а доповнена реальність лише вносить окремі штучні елементи в сприйняття світу реального.

Системами віртуальної реальності називаються пристрої, які більш повно, в порівнянні зі звичайними комп'ютерними системами, імітують взаємодію з віртуальним середовищем шляхом впливу на усі п'ять наявних у людини органи чуття.

Таких систем у повному обсязі поки що не існує, але при створенні віртуальної реальності розробники намагаються домогтися, щоб вона була [25]:

- правдоподібною - підтримувала у користувача відчуття реальності того, що відбувається;
- інтерактивною - забезпечувала взаємодію із середовищем;
- доступною для вивчення - надавала можливість досліджувати великий, деталізований світ;
- що створює ефект присутності - залучала у процес як мозок, так і тіло користувача, впливаючи на максимально можливе число органів чуттів.

Очевидно, досягнення цих цілей можливо лише за використання високопродуктивного апаратно-програмного забезпечення.

Типи віртуальної реальності

На даному етапі розвитку технологій VR серед них можна виділити наступні типи.

Технології VR з ефектом повного занурення, що забезпечують правдоподібну симуляцію віртуального світу з високим ступенем деталізації. Для їх реалізації необхідний

високопродуктивний комп'ютер, здатний розпізнавати дії користувача і реагувати на них в режимі реального часу, і спеціальне обладнання, що забезпечує ефект занурення [26].

Технології VR без занурення. До них відносяться симуляції із зображенням, звуком і контролерами, що транслюються на екран, бажано широкоформатний. Такі системи зараховують до віртуальної реальності, оскільки за ступенем впливу на глядача вони набагато перевершують інші засобів мультимедіа, хоча і не реалізують повною мірою вимоги, що пред'являються до VR [27].

Технології VR зі спільною інфраструктурою. До них можна віднести *Second Life* - тривимірний віртуальний світ з елементами соціальної мережі, який налічує понад мільйон активних користувачів, гру *Minecraft* і інші. Такі світи не забезпечують повного занурення (втім, у Minecraft вже існує версія для віртуальної реальності, що підтримує шоломи *Oculus Rift і Gear VR)*. Але у віртуальних світах добре організована взаємодія з іншими користувачами, чого часто не вистачає у продуктів «справжньої» віртуальної реальності.

Віртуальні світи використовуються не тільки в ігровій індустрії: завдяки таким платформ, як *3D Immersive Collaboration* можна організовувати робочі та навчальні 3D-простору - це називається «спільна робота з ефектом присутності». Забезпечення повного занурення і, одночасно, взаємодії користувачів в віртуальності є одним з важливих напрямків розвитку *VR* [28].

VR на базі інтернет-технологій. До них відноситься перш за все мова *Virtual Reality Markup Language,* аналогічний *HTML*. Зараз ця технологія вважається застарілою, але, не виключено, в майбутньому віртуальна реальність буде створюватися в тому числі - з використанням інтернет-технологій [29, 30].

Принцип роботи VR

Найпоширенішим засобом занурення у віртуальну реальність є спеціальні шоломи/окуляри. На розташований перед очима користувача дисплей виводиться відео в форматі 3D. Прикріплені до корпусу гіроскоп і акселерометр відстежують повороти голови і передають дані в обчислювальну систему, яка змінює зображення на дисплеї в залежності від показань датчиків. У результаті користувач має можливість «озирнутися» всередині віртуальної реальності і відчути себе в ній, як у реальному світі [31].

Для більш реалістичного занурення у світ віртуальної реальності крім датчиків, які відстежують положення голови, в пристроях VR можуть застосовуватися трекінгові системи, які відстежують руху зіниць очей і дозволяють визначити, куди людина дивиться в кожен момент часу, а також відстежують рухи тіла людини з метою повторення їх у віртуальному світі. Таке відстеження може здійснюватися за допомогою спеціальних датчиків або відеокамери [32].

Для взаємодії з віртуальною реальністю традиційних 2D-контролерів (миша, джойстик і ін.) Вже недостатньо, тому їх замінюють 3D-контролерами (маніпуляторами, що дозволяють працювати в тривимірному просторі).

Пристрої зі зворотним зв'язком призначені для того, щоб користувач міг ще повніше відчути все те, що відбувається у віртуальному світі. В якості таких пристроїв можуть використовуватися вібруючі джойстики, що обертаються крісла і т.д [35].

Пристрої і компоненти VR

Вважається, що 80% інформації людина отримує через зір. Тому розробники систем ВР приділяють величезну увагу саме пристроям, що забезпечує формування зображень.

Як правило, їх доповнюють пристроями стереозображення, ведуться роботи по тактильним впливам і навіть імітації запахів [36].

Про вплив на смакові рецептори поки не повідомляється.

Зображення. **Шолом віртуальної реальності**

Сучасні шоломи віртуальної реальності (HMD-display, head-mounted display, відеошлем) містять один або кілька дисплеїв, на які виводяться зображення для лівого і

правого ока, систему лінз для коригування геометрії зображення, а також систему трекінгу, що відстежує орієнтацію пристрою в просторі. За зовнішнім виглядом вони тепер схожі на окуляри, тому їх все частіше називають *VR headsets* (ВР-гарнітури) або просто окуляри віртуальної реальності. Їх можна розділити на три групи [37]:

1. Окуляри, в яких обробку і виведення зображення забезпечує смартфон (Android, iPhone, Windows Phone). Сучасний смартфон - високопродуктивне пристрій, здатний самостійно обробляти тривимірні зображення. Дисплеї смартфонів мають досить високою роздільною здатністю. Практично кожен смартфон забезпечений датчиками, що дозволяють визначати положення пристрою в просторі.

2. Окуляри, в яких обробку зображення забезпечує зовнішній пристрій (*ПК, Xbox, PlayStation* і т.п.). Зовнішнє пристрій повинен бути високопродуктивним, а окуляри забезпечені датчиками положення.

3. Автономні окуляри віртуальної реальності (Lenovo Mirage Solo, спільно з Google, Oculus Quest від Facebook, Samsung Gear VR і ін.) [38].

Шоломи є основним компонентом VR з повним зануренням, оскільки не тільки забезпечують об'ємне зображення і стереозвук, але ще і частково ізолюють користувача від навколишньої реальності.

MotionParallax3D-дисплеї

Такі дисплеї задіють властивий людині механізм сприйняття обсягу - паралакс (motion parallax). Для цього в кожен момент часу для глядача, виходячи з його положення щодо екрану, генерується відповідна проекція тривимірного об'єкту. Переміщаючись навколо сцени, користувач може оглянути її з усіх боків, при цьому всі об'єкти сцени будуть переміщатися одна відносно іншої. Явище параллакса багаторазово підсилює сприйняття обсягу. На відміну від 3D-кінематографа і 3D-TV, які використовують лише бінокулярний зір, технологія MotionParallax3D дозволяє користувачеві розглянути 3D-сцену з усіх боків, як якщо б все її об'єкти були реальні. Зсув глядача щодо екрану, що порушує ефект обсягу в 3D-кіно, в системі MotionParallax3D ефект тільки підсилює.

Система, що використовує механізм параллакса, повинна вловлювати найдрібніші рухи голови користувача і відстежувати їх з високою швидкістю і точністю, щоб мозок не фіксував спотворення геометрії об'єктів, викликані запізненням зміни ізображенія [39]. Затримка повинна складати не більше 20 мс, для інтерактивних ігор - не більше 11 мс [40].

Ці пристрої забезпечують, як правило, неповне занурення, оскільки відтворюються на дисплеях і не ізолюють користувача від навколишнього середовища. Виняток - кімнати віртуальної реальності (*CAVE, cave automatic virtual environment)*. У таких кімнатах на кожну стіну проектується стереоскопічне зображення, розраховане для конкретної точки, в якій і знаходиться користувач.

У підсумку таке зображення оточує людину з усіх боків, занурює його в себе. Деякі експерти вважають [41], що VR-кімнати набагато краще VR-шоломів: забезпечують більш високу роздільну здатність, немає необхідності надягати на голову громіздкий пристрій, в якому деяких навіть заколисує, і самоідентифікація відбувається простіше завдяки тому, що користувач має можливість постійно бачити себе.

Звук

Багатоканальна акустична система дозволяє виробляти локалізацію джерела звуку, завдяки чому користувач може орієнтуватися в віртуальному світі за допомогою слуху.

Тактильні та інші відчуття

Рукавички віртуальної реальності (інформаційні рукавички, datagloves)

Такі рукавички мають датчики, що дозволяють відслідковувати рух зап'ясть і пальців рук.

Технічно це може бути реалізовано різними методами: з використанням оптоволоконних кабелів, тензометричних або п'єзоелектричних датчиків, а також електромеханічних пристроїв (таких як потенціометри) [40].

Наприклад, вчені з компаній *EPFL і ETH Zurich* розробили ультралегкі рукавички (вагою менше 8 грамів на кожен палець і товщиною всього лише 2 мм). Вони забезпечують

«надзвичайно реалістичну тактильну зворотний зв'язок і можуть бути запитані від акумуляторів, завдяки чому забезпечується безпрецедентна свобода руху» [41].

Костюм віртуальної реальності

Цей костюм повинен відслідковувати зміну положення всього тіла користувача і передавати тактильні, температурні і вібраційні відчуття, а в комбінації з шоломом - зорові і слухові [39].

Запахи і смакові відчуття

Роботи з синтезу запахів ведуться вже не один рік [40], але до широкого використання отриманих результатів ще далеко. Про які-небудь значущі досягнення в області передачі смакових відчуттів говорити поки не доводиться.

Для взаємодії з віртуальним середовищем використовуються спеціальні джойстики (геймпади, wands), що містять вбудовані датчики положення і руху, а також кнопки і колеса прокрутки, як у миші. Зараз такі джойстики все частіше роблять беспровідними [38].

У якості пристроїв управління можуть також використовуватися згадані вище інформаційні рукавички і костюми віртуальної реальності.

Як це зазвичай буває при впровадженні нових технологій, кожен з великих постачальників, який вийшов на багатогранний ринок, прагне просувати саме свою продукцію, поширювати свої технічні рішення. Відповідно, провідні компанії, випустивши VR-гарнітури, розробляють або замовляють контент саме для них. Рушійною силою ринку VR на даний момент є віртуальні ігри, в першу чергу, в розрахунку на геймерів, і були випущені гарнітури *Oculus Rift, Samsung Gear VR, HTC Vive, PlayStation VR і др* [38].

Ігри та інший контент, розроблені для однієї гарнітури, що не відтворюються на інший. Ігромани чекають не дочекаються, коли буде налагоджено портирование ігор між гарнітурами різних розробників. Промисловці, рекламісти та представники багатьох інших галузей швидше впроваджували б VR, знаючи, що дороге устаткування не доведеться змінювати через те, що нове, вкрай привабливе ПЗ було розроблено для інших окулярів-рукавичок-костюмів віртуальної реальності.

Постачальники VR прекрасно розуміють, що добре налагоджену співпрацю між ними здатне вивести віртуальну реальність на якісно новий рівень. Тому ще в грудні 2016 року було створено *Глобальна асоціація віртуальної реальності (GVRA)* - некомерційна організація виробників шоломів віртуальної реальності (VR), покликана об'єднати зусилля компаній у розвитку цього напрямку. В її створенні взяли участь компанії *Acer Starbreeze, Google, HTC VIVE, Oculus, Samsung і Sony Interactive Entertainment*.

Згідно з даними сайту GVRA, [40] головне завдання асоціації - сприяти глобальному зростанню і розвитку індустрії VR. Планується створення робочих груп для проведення досліджень і вироблення рекомендацій, що стосуються найбільш важливих для галузі тем. У кінцевому підсумку, ці групи будуть розробляти кращі практики і відкрито ділитися ними.

Однак станом на жовтень 2018 тобто через майже два роки після створення *GVRA*, єдиним матеріалом, що ще на сайті асоціації, став звіт «*Дослідження віртуальної реальності і її потенціал для Європи*», що охоплює період з 2016 по 2017 [41]. Мабуть, досягнення глобальних домовленостей між великими компаніями - завдання не менш складна, ніж розробка власне технологій VR.

Втім, зусилля по уніфікації обладнання тривають. Так, 17-го липня 2017 компанії *NVIDIA, Oculus, Valve, AMD і Microsoft* представили специфікацію *VirtualLink* ™ - відкритий галузевий стандарт, який дозволить гарнітурам VR наступного покоління підключатися до ПК і інших пристроїв з використанням лише одного високошвидкісного USB-кабелю Type-C (замість декількох шнурів і роз'ємів, що застосовуються в даний час).

Відзначається, що VirtualLink спеціально створений для VR. Він забезпечує оптимальну латентність і смугу пропускання, дозволяючи виробникам шоломів і ПК створювати віртуальну реальність нового покоління [38].

Звичайно ж, завдання уніфікації той чи інший спосіб все одно будуть вирішені, як це вже відбувалося з іншими технологіями, головне - щоб це відбулося в найближчі роки.

Віртуальна реальність у промисловості

Приклади різноманітного застосування технологій VR в промисловості наведені в статті «Віртуальна реальність (VR): кращі практики».

Фінансові перспективи

Ставлення до віртуальної реальності в інвесторів неоднозначне. З одного боку, VR-шолом можна купити в будь-якому магазині електроніки. Тільки компанія Sony з кінця 2016 продала більше 1,5 млн. Гарнітур PlayStation VR для своєї консолі. Тисячі компаній створюють відповідний контент. Однак з висновком технології VR на комерційний ринок розробники першої хвилі, мабуть, поквапилися.

У результаті користувачі не лише не отримали обіцяного ефекту повного занурення, але й, зіткнувшись з недосконалістю технології, розчарувалися. Масове поширення VR/AR стримують, по-перше, низька якість VR-контенту, по-друге, розрізненість платформ і відсутність єдиних стандартів при його створенні, по-третє, відсутність чіткої системи дистрибуції, єдиного майданчика, де були б зібрані відповідні продукти.

Відповідно поводиться і ринок. У першому кварталі 2018 р світові поставки гарнітур віртуальної реальності виросли на 16% в річному порівнянні, повідомляють експерти з *Canalys.*16 Але в другій календарної чверті цього року, за оцінками IDC, постачання скоротилися на 33,7%. Втім, аналітики впевнені, що ситуація, що склалася має тимчасовий характер. Поява нових продуктів, перш за все *Oculus Go* і *HTC Vive Pro*, а також нових брендів, повинні повернути ринок у позитивне русло [42].

Аналітики компаній *Gartner і IDC* стверджують, що VR/AR наближаються до стадії технологічної зрілості. Тобто дуже скоро віртуальна реальність стане частиною повсякденного життя. Технологічно все готово до її масового застосування [43].

7.6. Доповнена реальність

Тім Кук, генеральний директор компанії *Apple,* неодноразово заявляв, що AR сьогодні є найбільш перспективною технологією. За його словами, доповнена реальність – настільки ж грандіозна ідея, як і створення смартфону [43].

Визначення доповненої реальності з'явились відносно нещодавно, термінологія ще не закріпилась, детально про це йдеться у статті «Доповнена, віртуальна та інші реальності».

Доповнена реальність (augmented reality, AR) – результат введення у поле сприйняття будь-який сенсорних даних з метою доповнення даних про оточення і поліпшення сприйняття інформації.

Термін «доповнена реальність», ймовірно, був запропонований дослідниками корпорації *Boeing Томом Коделом (Tom Caudell)* у 1990 році [43].

Існує кілька інших визначень доповненої реальності. Зокрема, дослідник *Рональд Азума (Ronald Azuma)* у 1997 році визначив її як систему, яка:

1) суміщує віртуальне і реальне;

2) взаємодіє у реальному часі;

3) працює з 3D.

У концепції *Пола Мілграма (Paul Milgram) і Фуміо Кішіро (Fumio Kishino)* доповнена реальність є частиною **змішаної реальності**, яку також називають **гібридною реальністю (hybrid reality)**.

Ця концепція була запропонована ще у 1994 році. Але, починаючи з 2016 року, компанія *Microsoft* почала активно використовувати термін «змішана реальність» для просування на ринку свого продукту *HoloLens*. І тепер деякі експерти (і постачальники обладнання) визначають терміни наступним чином [44]:

Доповнена реальність (AR) — проектування будь-якої цифрової інформації (зображення, відео, текст, графіка і т.д.) поверх екрану будь-яких пристроїв. В результаті реальний світ доповнюється штучними елементами і новою інформацією. Може бути реалізована за допомогою додатків до звичайних смартфонів і планшетів, окулярів доповненої реальності, стаціонарних екранів, проекційних просторів та інших технологій.

Змішана реальність (MR) — проектування тривимірних віртуальних об’єктів чи голограм на фізичний простір. Дозволяє переміщуватись навколо віртуального об’єкту, оглядати його з усіх боків і, за потребою, всередині. Вимагає, як правило, спеціального обладнання (окулярів чи шоломів) [42].

Саме цими визначеннями ми будемо керуватись у даній статті; у ній йтиметься переважно про доповнену реальність.

Як працює технологія AR

Загальна схема створення доповненої реальності в усіх випадках така: камера пристрою AR знімає зображення реального об’єкта; програмне забезпечення (ПО) пристрою проводить ідентифікацію отриманого зображення візуальне доповнення, поєднує реальне зображення з його доповненням і виводить кінцеве зображення на пристрій візуалізації.

Детальніше технологію створення доповненої реальності ми розглянемо на прикладі використання її для діагностики промислового обладнання або управління ним.

Для роботи з AR на виробництві використовується смартфон, планшет або смарт-окуляри з відеокамерою і відповідним ПЗ. Якщо об'єктив відеокамери спрямований на об'єкт (одиницю обладнання), З нйого або по заздалегідь встановленому маркеру, або після аналізу форми об'єкта [45].

Розпізнавши об'єкт, ПЗ підключається до тривимірного цифрового двійника об'єкта, який розміщений на сервері підприємства або в хмарі.

Потім пристрій AR завантажує необхідну інформацію і накладає її на зображення об'єкта. У результаті співробітник підприємства бачить на екрані (або через окуляри) частково фізичну реальність, частково цифрову. При цьому оператор, керівник цієї одиницею обладнання, і технік-ремонтник, дивлячись на один об'єкт, будуть бачити різну доповнену реальність, відповідно до виконуваних функцій.

Ремонтник може бачити дані про напрацювання або, припустимо, робочу температуру того чи іншого вузла, який обслуговує. Оператору пристрій AR може допомагати управляти об'єктом – завдяки сенсорному екрану, голосом або жестами. При русі співробітника розмір і орієнтація дисплея AR автоматично коригуються, непотрібна інформація зникає, а нова з’являється.

Тривимірна цифрова модель створюється або за допомогою *САПР* (зазвичай ще на етапі розробки об'єкта), або шляхом оцифрування даної одиниці обладнання. Цей цифровий двійник збирає інформацію про стан об'єкта, що отримується від нього самого, з інформаційних систем та із зовнішніх джерел. З його допомогою ПО доповненої реальності масштабує і точно розміщує на зображенні об'єкта або навколо нього актуальні дані [46].

Рис.7.4. Приклад використання AR у рішені *SmartEAM* компанії *IT-Enterprise* на підприємстві ІНТЕРПАЙП СТАЛЬ

Пристрої, що реалізують AR

Пристрої, здатні створювати доповнену реальність, можна розділити на наступні групи.

Мобільні пристрої. До них відносять планшети, смартфони, окуляри доповненої реальності, лінзи доповненої реальності.

На *планшети* і *смартфони* має бути встановлено спеціалізоване ПЗ. Наприклад, на смартфони і планшети можна встановити браузери доповненої реальності, такі як *Wikitude, Layar, Blippar*, або спеціальні пропозиції (зокрема, *City Lens для Windows Phone*). Ці браузери можуть показувати найближчі до місцерозташування користувача визначні місця, магазини, кав'ярні, пункти прокату, пункти обслуговування і т.п., а також виконувати корисні функції.[3]

Окуляри доповненої реальності — це окремий повноцінний пристрій, розроблений безпосередньо для роботи з AR. Вони, почасти, вміють проектувати голограми та інформацію у реальний простір, але не прив'язуються до їх фізичних об'єктів. Фактично, це просто екран перед очима. Найбільш відомі окуляри *Google Glass* (у 2018 р. звичайним користувачам були доступні версії 2.0 та 3.0, компаніям — версія 2017-го року, Google Glass Enterprise Edition). З ними конкурують *Vuzix Blade, Epson Moverio, Sony SmartEyeglass*. У порівнянні з *Google Glass*, ці та інші окуляри доповненої реальності дешевше і більше доступні – звичайні користувачі можуть купити їх на офіційних сайтах.

А окуляри *Microsoft HoloLens, Magic Leap One и Meta 2* — це вже окуляри змішаної реальності, тобто вони дозволяють працювати з віртуальними об'єктами, прив'язаними до реального світу [47].

Лінзи для доповненої реальності поки ще лишаються технологією майбутнього. Розробники прагнуть перетворити лінзи у прозорий екран, що містить систему управління, мініатюрну камеру, антену, світлодіоди та інші оптоелектронні компоненти.Зокрема, компанія Samsung вже подала патент на «розумні» контактні лінзи, роботи у цьому напрямку веде і компанія Google. Але на ринок подібні пристрої вийдуть не раніше, ніж 5–10 років [48].

Стаціонарні пристрої. Це може бути телевізор, екран комп'ютера, ігровий комп'ютер типу *Kinect.* На екран телевізора виводиться вже доповнене зображення (особливо часто це буває під час трансляції футбольних і хокейних матчів), приклад для комп'ютера — карти *Google* в режимі «*Satellite*», коли на супутниковий знімок накладаються назви вулиць і визначні місця. Іноді використовуються широкоформаті екрани, а також проекційні системи, здатні накладати зображення не лише на екрани, але і на будь-які поверхні.

Спеціальні засоби. До них відносять, наприклад, спеціалізовані шоломи військових пілотів. На скло шолома виводиться необхідна пілоту важлива інформація і він може сприймати її, не переводячи погляд на панель приладів, тим самим економлячи дорогоцінні секунди. Багато з подібних систем дозволяє здійснювати цілевказання шляхом повороту голови чи рухом очних яблук пілота.

Шолом пілота-винищувача п'ятого покоління F-35 використовує вже настільки сучасні технології, що пілот може бачити навіть крізь непрозорий корпус літака. Це найдорожчий шлем у світі – його вартість перевищує 400 тис доларів. А британські інженери розробили для військових пілотів шлем з уже вбудованою системою нічного бачення [49].

На захисному склі «розумного шолома» може бути відображена швидкість мотоциклу, маршрут, текстові повідомлення і багато іншого. Схожу технологію використовують і для відображення інформації на лобовому склі автомобіля [49].

Компанія *Boeing* протягом останніх 20 років шукала систему, здатну скоротити час на виробництво кабельних джгутів і усунення помилок при їх виготовленні. Бортові системи літаків містять багато компонентів, пов'язаних між собою дротами і кабелями. Їх загальна довжина у літаку Боінг-747, наприклад, складає 250 кілометрів [50].Укладка і з'єднання дротів виробляється за спеціальним шаблоном, після чого скріплюється у джгути, а на кінці кабелів встановлюють роз'єми. Така робота займає багато часу і загрожує помилками. На початку 2014 р. компанія впровадила рішення з доповненої реальності на платформі окулярів *Google Glass*. За рахунок впровадження технології AR вдалося скоротити час виробництва на 25% і знизити кількість помилок на 50% [50].

Компанія *Lockheed Martin* використовує технології доповненої реальності у процесі збірки літака F-35. За основну платформу використовуються AR-окуляри *Epson Moverio BT-200,* обладнані датчиками руху і глибини. Коли технік монтує на шасі деталь тормоза, в окулярах він бачить усі дані про те, де і в якому порядку варто проводити збірку і під'єднувати кабелі. За даними компанії *NGRAIN*, впровадивши цю систему, програмне забезпечення дозволяє інженерам працювати швидше на 30% і з точністю до 96% [50]. Концерн *Fiat Chrysler Automobiles (FCA)* застосував у своїй роботі проекційну AR-систему *OPS Solutions*. Тепер на кожному етапі процесу складання робочі отримують наочну інформацію про свій наступний крок.

Машинобудівне підприємство *AGCO (США)* в 2015 р. обладнало ділянки великими дисплеями, на які виводився тривимірний склад виробів і повний комплект документації, необхідний для швидкого і якісного складання виробів (тракторів та іншої сільськогосподарської техніки). У 2017 року підприємство перейшло на використання окулярів *Google Glass,* завдяки чому контроль якості прискорився на 20%.

Портативні віртуальні візуалізатори *PVAITV і MibiPV*, розроблені спеціально для інженерів та IT-фахівців, дозволяють сканувати обладнання і виявляти помилки/несправності, які необхідно усунути. Програма вказує, де знаходиться пошкоджений роз'єм або від'єднаний шнур [51].

Робочі *General Electric* при складанні вітряних турбін на заводі у Флориді зв'язуються з експертами через окуляри доповненої реальності, показують збиране обладнання в поле зору і отримують відповіді на питання від фахівців, конструювати турбіни, за допомогою тих же окулярів. Аналіз показує зростання продуктивності на 34% у порівнянні з використанням попередніх технологій складання обладнання [52].

Крім все більш активного застосування в промисловості доповнена реальність використовується у комп'ютерних іграх, маркетингу (зокрема, у вуличному маркетингу, коли великий екран з AR розташовується в людному місці), в моді, соціальних мережах, медицині та хірургії, туризмі, в пресі, музейній справі - список прикладів застосування AR постійно поповнюється.

Один важливий факт, який свідчить про безумовну перспективність AR - створення в 2015 році альянсу *Augmented Reality for Enterprise Alliance (AREA).* До цього альянсу входять такі великі компанії, як *Bosch* і *Boeing.* Мета альянсу - безкоштовний (для американського ринку) і відкритий обмін кращими практиками, отриманих уроків і технологічними ресурсами, які будуть допомагати підприємствам ефективно впроваджувати AR. 11 квітня 2017 року проголошено про розробку учасниками цього альянсу ключових галузевих керівних документів. Документи розроблялися за сприяння *UI Labs, Lockheed Martin, Caterpillar і Procter & Gamble.*

Контрольні питання до розділу

1. Чим була обумовлена Перша промислова революція ?
2. Чим була обумовлена Друга промислова революція ?
3. З чим пов'язана Третя промислова революція ?
4. Що собою представляє Четверта промислова революція ?
5. Що собою преставляє Індустрія 4.0 ? Наведіть її характерні риси.
6. Які елементи відносяться до компонентів «Industry 4.0» ?
7. Що собоою представляють «розумні» підприємства ?
8. Що собою представляє рішення типу «хмара в коробці» ? для чого воно призначене ?
9. Які основні об'єкти входять в Industry 4.0 ?
10. Які існують основні принципи побудови "Індустрії 4.0"?
11. Які основні тенденції простежуються для розвитку Промислового Інтернету Речей ?
12. Що таке машинне навчання (Machine Learning) **?**
13. Які розрізняють типи машинного навчання ?

14. Наведіть методи машинного навчання. В чому їх відмінність?
15. Що собою представляє «розумне виробництво» (*Smart Manufacturing*) ?
16. Координатор ІКТ-проектів в сьомий рамковій програмі Європейського Союзу з науково-технічного співробітництва, розділяє фабрики майбутнього на наступні основні типи:
    a) *цифрові (Digital);*
    b) *аналогові (Analog);*
    c) *«розумні» (Smart);*
    d) *реальні (Real);*
    e) *віртуальні (Virtual)*.
17. Наведіть основні системи та технології, які використовуються в «розумному виробництві» (*Smart Manufacturing*) при створенні *«цифрового макета» (Digital Mock-Up, DMU) або «цифрового двійника» (Digital Twin)*.
18. Наведіть основні системи та технології, які використовуються в «розумному виробництві» (*Smart Manufacturing*) при створенні «розумних фабрик» (*Smart Factory*).
19. Наведіть основні системи та технології, які використовуються в «розумному виробництві» (*Smart Manufacturing*) при створенні *«віртуальних фабрик» (Virtual Factory).*
20. Які етапи виділяє компанія IT-Enterprise, які потрібно пройти для того, щоб реалізувати концепцію Smart Factory і закласти основи для подальшого переходу до Virtual Factory?
21. Що собою представляє віртуальна реальність? Наведіть типи віртуальної реальності.
22. В чому полягає принцип роботи віртуальної реальності?
23. Які існують пристрої та компоненти віртуальної реальності? Наведіть приклади.
24. Що собою представляє лоповнена реальність? Принцип роботи доповненої реальності.
25. Наведіть приклади пристроїв, які реалізують доповнену реальність.

Список рекомендованої літератури

1. https://www.crn.ru/news/detail.php?ID=117807
2. http://ua.automation.com/content/promyshlennaja-avtomatizacija-i-internet-veshhej
3.www.tadviser.ru/index.php/Статья:IIoT_-_Industrial_Internet_of_Things_(Промышленный_интернет_вещей)
http://www.forbes.ru/tehnologii/337091-treker-dlya-stanka-kogda-v-rossiyu-pridet-promyshlennyy-internet-veshchey
4.https://www.crn.ru/news/detail.php?ID=113441
5. www.accenture.com/t20160909T042713__w__/usen/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf
6.http://www.cnews.ru/news/line/promyshlennyj_internet_veshchej_sposoben
7.https://blog.schneider-electric.com/machine-and-process-management/2017/02/23/six-iiot-technology-trends-watch-2017/
8. http://ua.automation.com/content/6-shagov-k-informacionnoj-bezopasnosti-asu-tp
9. http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение
10. http://people.eecs.berkeley.edu/~russell/temp/q-and-a.html
11. Mitchell, T. (1997). Machine Learning. McGraw Hill. p. 2. ISBN 978-0-07-042807-2 https://vc.ru/21767-the-great-ai-awakening
12. http://iitp.ru/upload/publications/6256/vyugin1.pdf
13. https://vc.ru/21767-the-great-ai-awakening
14. https://rb.ru/story/machine-learning-in-business/

15.https://s3.amazonaws.com/files.technologyreview.com/whitepapers/MITTR_GoogleforWork_Survey.pdf
16. http://alhimiya.com/blog/neural-networks.html
17. https://rb.ru/news/ai-alibaba-best/
18. https://rb.ru/story/machine-learning-in-business/
19.https://www.manufacturingtomorrow.com/article/2017/02/what-is-smart-manufacturing--the-smart-factory/9166
20.https://books.google.com.ua/books?id=oeEVAwAAQBAJ&num=8&source=gbs_slider_cls_metadata9_mylibrary
21. https://technet-nti.ru/article/fabriki-buducshego
22. http://www.ng.ru/science/2018-02-27/100_industry270218.html?id_user=Y
23. https://www.youtube.com/watch?v=5EWh1icuS0M&feature=youtu.be
24. https://www.explainthatstuff.com/virtualreality.html
25. https://tproger.ru/translations/vr-explained/
26. http://www.tadviser.ru/index.php/Статья:Виртуальная_реальность_(VR,_Virtual_Reality)
27. http://googlecardboard.ru/v/kak-nazyvayutsya-vr-ochki/
28. https://web.archive.org/web/20150217161553/http://nttl.ru/technology/
29. https://funtecs.com/osnovy-virtualnoi-realnosti/
30. https://rb.ru/opinion/vr-and-vr/
31. http://vrvision.ru/polnyj-spisok-perchatok-virtualnoj-realnosti-2018/
32. https://actu.epfl.ch/news/ultra-light-gloves-let-users-touch-virtual-objects/
33. https://hightech.fm/2018/04/29/disney-3
34. https://habr.com/company/mailru/blog/407721/
35. http://digistream.ru/virtualnaya-realnost/ochki-virtualnoj-realnosti-dlya-smartfona-i-pk/
36. https://www.gvra.com
37. https://www.gvra.com/research/
38. https://sites.google.com/view/virtuallink-consortium/home
39. https://www.vestifinance.ru/articles/102736
40. https://ko.com.ua/na_mirovom_rynke_vr-garnitur_glubokij_proval_125961
41. https://lenta.ru/articles/2017/07/07/ar/
42. https://hbr-russia.ru/innovatsii/tekhnologii/a24121
43. https://i-look.net/news/augmented-reality-browsers.html
44. https://www.unipage.net/ru/p/google_glass_3
45. http://controlengrussia.com/innovatsii/dopolnennaya-real-nost/ar/
46. https://www.prosoft.ru/cms/f/466284.pdf
47. http://tofar.ru/kak-rabotaet-ar.php
48. http://krasvozduh.ru/zavod-boing/
49. https://gigazine.net/gsc_news/en/20160715-boeing-google-glass
50. https://www.popularmechanics.com/flight/a13967/lockheed-martin-augmented-reality-f-35/
51. https://ar-conf.ru/ru/news/razvitie-dopolnennoy-realnosti-v-aviakosmicheskoy-otrasli-34872
52. http://www.forbes.ru/tehnologii/344377-zhizn-v-forme-j-riski-i-vozmozhnosti-uskoreniya-diffuzii-tehnologiy

РОЗДІЛ 8. ТЕХНОЛОГІЇ ТА ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ

8.1.Технології та протоколи передачі даних на довгі відстані в IoT мережах

В найближчому майбутньому до Інтернету речей будуть підключені велика кількість пристроїв. Більша доля цих пристроїв буде мати живлення від батарейок. У зв'язку з цим, однією з основних характеристик є тривалість роботи обладнання без втручання людини.

Для того щоб розв'язати цю проблему були створені нові мережі спеціально для IoT. Ці мережі називаються *LPWAN* (*Long Power Wide Area Network*). Основними технологіями цих мереж є *NB-IoT, Weightless, LoRa, SIGFOX* та інші. Ці технології з'явилися через те, що необхідно буде підключати велику кількість датчиків та приладів для централізованого збору інформації на хмарних серверах [1]. Надалі буде наведено основні технології мережі *LPWAN*.

8.1.1. Технологія LoRaWAN

Поява технології *LoRaWAN* викликало великий резонанс на ринку бездротового зв'язку, що спричинило необхідність прийняти єдиний стандарт для глобальних мереж з низьким енергоспоживанням - *LPWAN (Low Power Wide Area Network).*[10] Абревіатура LoRa об'єднує в собі метод модуляції LoRa у бездротових мережах *LPWAN*, розроблений *Semtech* та відкритий протокол *LoRaWAN.*

LoRa (Long Range) - це технологія і однойменний метод модуляції. Метод модуляції LoRa запатентований компанією Semtech, заснований на технології розширення спектру (*spread spectrum modulation*) і варіацію лінійної частотної модуляції (*chirp spread spectrum, CSS*), за якої дані закодовано широкосмуговими імпульсами з частотою, що збільшується, або зменшується на деякому тимчасовому інтервалі [1].

Таке рішення, на відміну від технології прямого розширення спектра, робить приймач стійким до відхилень частоти від номінального значення та спрощує вимоги до тактового генератора, що дозволяє використовувати недорогі кварцові резонатори. LoRa використовує пряму корекцію помилок (*forward error correction, FEC*), працює в субгігагерцовому діапазоні частот.

LoRa дозволяє демодулювати сигнали на рівні 20 дБ нижче рівня шумів, тоді як більшість систем з частотною маніпуляцією (*frequency shift keying, FSK*) можуть коректно працювати з сигналами на рівні не нижче 8-10 дБ над рівнем шумів. Модуляція *LoRa* визначає фізичний рівень, який може використовуватися в мережах з різними архітектурами: mesh-мережі, зірка, точка-точка та інші.

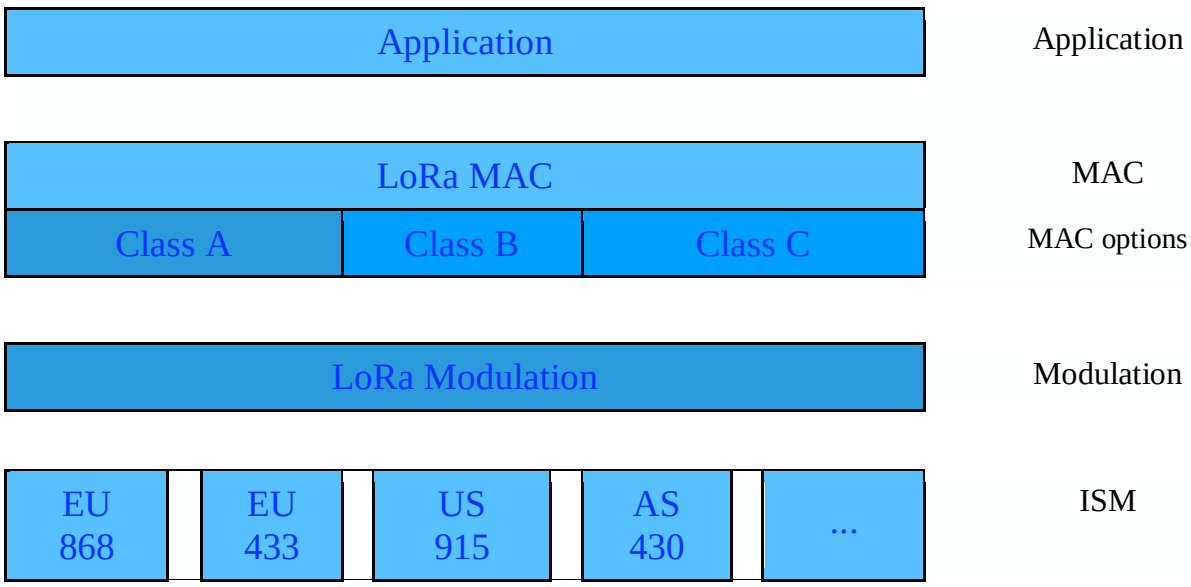


Рис. 8.1. Архітектура технології LoRaWAN

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

LoRaWAN (Long Range Wide Area Network) — відкритий протокол канального рівня для мереж з високою ємністю та великим радіусом дії і низьким власним використанням енергії, який *LoRa Alliance* стандартизувала для мереж *LPWAN* [2].

Разом з протоколом *LoRaWAN* можуть працювати декілька видів пристроїв.

Типи пристроїв LoRaWAN

Ці пристрої в *LoRaWAN* поділяються на:

- *Двонаправлені кінцеві пристрої "класу А"* (*Bi directional End Devices, Class A)*. Подібні пристрої застосовуються, коли вимагається підтримувати мінімальну потужність при переважання передачі даних з сервером.

Кінцевий вузол ініціює сеанс зв'язку шляхом відправки пакету даних, після чого виділяє два вікна, в перебігу яких чекає дані від сервера. Відповідно, можливість передачі даних між сервером і кінцевим пристроєм виникає тільки після відкриття сеансу кінцевим пристроєм.

- *Двонаправлені кінцеві пристрої "класу Б"* (*Bi directional End Devices, Class B*). Відрізняється від пристроїв "класу А", оскільки має можливість за розкладом відкривати додаткові вікна прийому. Для складання розкладу кінцевий пристрій здійснює синхронізацію за спеціальним сигналом від шлюзу. Таким чином, наявність додаткового вікна надає змогу серверу обмінюватися даними у попередньо обумовлений момент часу.

- *Двонаправлені кінцеві пристрої "класу С" з максимальним приймальним вікном (Bi directional End Devices, Class C).* Відрізняються практично безперервним вікном прийому даних і закривають його лише на час передачі даних. Така особливість, дозволяє застосовувати їх для вирішення завдань, пов'язаних з великим обсягом даних.

Архітектура мережі LoRaWAN

Архітектура LoRaWAN складається з таких основних елементів: кінцеві вузли, шлюзи, мережевий сервер, а також сервер додатків [3]

Кінцеві вузли (End Nodes) - пристрої, що здійснюють, вимірювання, контроль та управління. Вузол складається з наборів датчиків вимірювання та керуючі елементи. Мають зазвичай живлення від батарейок. Для того щоб економити енергію вузли виконують передачу даних на деякий невеликий проміжок часу, після чого відкривається два тимчасові вікна для прийому даних.

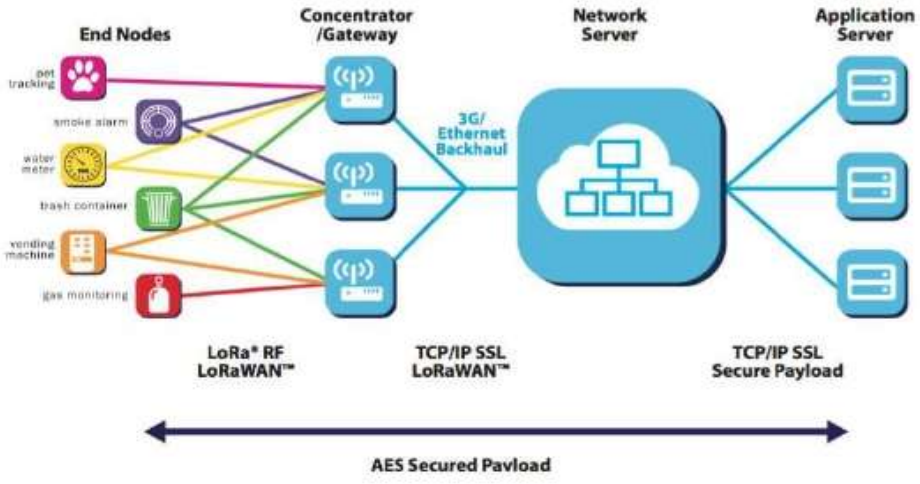


Рис. 8.2. Архітектура мережі LoRaWAN

Шлюз LoRa (Gateway/Concentrator) - це пристій, який приймає дані через радіоканал від кінцевих пристроїв та передає їх в транзитну мережу. До транзитних мереж можна віднести *WiFi, Ethernet*, стільникові мережі і будь-які інші телекомунікаційні канали. Кінцеві пристрої та шлюз утворюють мережеву топологію типу — зірка. Доволі поширеним є те, що пристій складається з багатоканальних пристроїв прийому та передачі, це дозволяє обробляти сигнали, які одночасно надходять по декількох каналах, або кілька сигналів, отриманих від одного каналу.

Таким чином, кілька схожих пристроїв можуть забезпечити повне покриття мережі і прозору двонаправлену передачу даних між мережевим сервером та кінцевими вузлами.

Мережевий сервер (Network Server) — віддалений центр управління мережею. За його допомогою відбувається регулювання швидкості, аналіз, обробка та зберігання даних, що були прийнятими з шлюзу.

Сервер програм (Application Server) - пристрій для збору інформації з кінцевих вузлів та віддаленого контролю їх роботи [4].

Один *LoRa-шлюз* допускає обслуговування до п'яти тисяч кінцевих пристроїв, що досягається за рахунок:

- Особливостей топології мережі.
- Адаптивної швидкості передачі даних і адаптивної вихідний потужності пристроїв, що задаються мережевим вузлом.
- Тимчасовим поділом доступу до середовища.
- Частотним поділом каналів.
- Особливістю *LoRa* модуляції, що дозволяє в одному частотному каналі одночасно демодулювати сигнали, що передаються на різних швидкостях.

8.1.2. Технологія SigFox

SigFox - це технологія, яка приносить нову мережу та інформаційну стратегію *IoT*. Розробник, група з *Labège*, Франція з однойменною назвою, *SigFox* - це мережевий оператор, який займається впорваджанням *IoT* у бізнес індустрію.[5] Архітектура мережі *SigFox* досить сильно схожа на мережі стільникових операторів зв'язку таких як *GSM* та *GPRS*, але являється менш затратною та більш енергоефективною. [5]

Зона, яку покриває *SigFox* складає близько 30-50 км в міський та сільський місцевості. В містах де дуже багато шумів, діапазон роботи 3-10 км.

На рис. 8.3 представлена архітектура мережі технології *SigFox*. Загальна топологія мережі була розроблена для забезпечення масштабованої, високопродуктивної мережі, з дуже низькою витратою енергії.

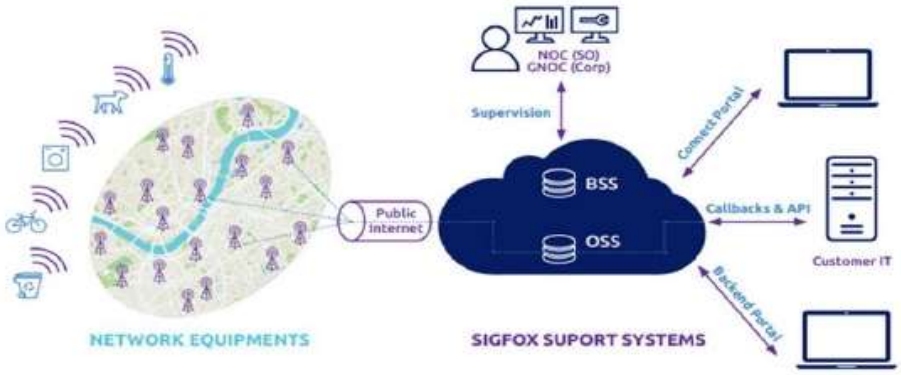


Рис. 8.3. Архітектура мережі SigFox

SigFox використовує надвузьку смугу частот *UNB (Ultra Narrow Band)*, на основі радіо технології для підключення пристроїв до глобальної мережі. Використання *UNB* - ключовий

фактор у забезпечені дуже низького рівня потужності передавача, який буде використовуватися під час стану підтримки надійного з'єднання для передачі даних.

У Європі широко використовується діапазон 868,8 МГц (як визначено в ETSI і CEPT), а у США 915 МГц (як визначено FCC).

Пристрої передають свої повідомлення до базової станції *SigFox.* За допомогою *point-to-point (P2P)* протоколу на базову станцію *Sigfox* підключають до своєї Інтернет бази даних, після отримання і декодування повідомлення, дані надсилаються до її Інтернет бази даних. Нарешті, хмарний сервер *SigFox* посилає повідомлення на клієнтські сервери та IT платформи через інтерфейси прикладного програмування (APIs).

Технологія *SigFox* спрямована на низьку вартість пристроїв, де потребується широка зона покриття.

Є цілий ряд додатків, яким необхідна ця технологія бездротового зв 'язку. Області, в яких можуть бути використані мережі *SigFox* включають в себе:

- дім та споживчі товари;
- енергетичні комунікації;
- охорона здоров'я;
- транспорт;
- віддалений моніторинг та контроль;
- безпека.

Стандарт має ряд переваг у порівнянні з іншими базовими технологіями LPWAN мереж. Серед переваг *SigFox* можна відзначити:

- велика зона покриття;
- висока проникаюча спроможність;
- довга робота від однієї батареї, приблизно до 20 років роботи сенсора від 2-х батарей AA;
- наднизьке енергоспоживання;
- низька вартість.

Як і всі технології сучасного світу, енергоефективна мережу SigFox, на жаль, також має і негативні характеристики:

- низька швидкість передачі даних;
- залежність від стільникової інфраструктури;
- обмежена завадостійкість.

Більшість країн Європи та США використовують саме цю технологію.

8.1.3. Стандарт NB-IoT

NB-IoT - стандарт стільникового зв’язку створений для приладів телеметрії з низьким об’ємом передачі даних. Створений *3GPP*, як розвиток мобільних стільникових мереж перша версія цього стандарту була представлена в 2016 році [6].

NB-IoT, або ще його називають стандарт *LTE-CAT*. M2, має досить велику кількість переваг таких, як низьке енергоспоживання, яке гарантує час роботи батареї до 10 років, широку зону покриття, можливість швидкої модернізації мережі, а також високу надійність.

NB-IoT — це розвиток стільникового зв’язку, який дозволяє операторам працювати з такими направленнями IoT, як системи інтелектуального відслідковування та обліку. Технологія *NB-IoT* розглядається як еволюція від стільникового зв’язку до Інтернету речей. Це бездротова різновидність глобальних мереж з низьким споживанням енергії і зроблена для взаємодії між додатками *M2M*.

Для *NB-IoT* можуть використовуватися практично всі ті самі діапазони частот, що і для 2G/3G/4G в "низьких" діапазонах. Це 20 діапазон (800МГц), 8 діапазон (900МГц), 3 діапазон (1800МГц). Більш високі частоти сенсу використовувати немає через більше затухання сигналу.

Варіанти розміщення NB-IoT в режимі Stand – Alone

Є три способи виділення частотного ресурсу для NB-IoT:

- *Stand – Alone (автономний)* [6].

Виділений частотний канал шириною в 200кГц. Цей варіант найбільш ефективний для роботи NB-IoT, але й найбільш витратний. Справа в тому, що в цьому випадку може знадобитися від 300 до 600 кГц дуже цінного спектру разом із захисними інтервалами. В цьому випадку взаємні інтерференції з іншими технологіями мінімальні (Рис.8.4.).

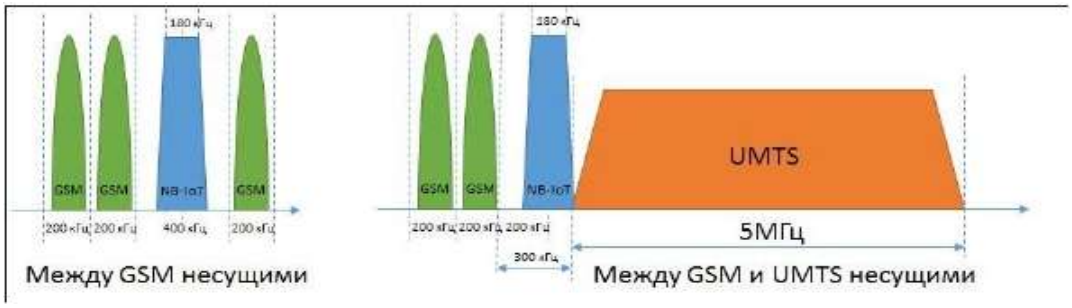


Рис. 8.4. Розміщення NB-IoT в режимі Stand – Alone

- *In Band(в середині полоси)*

У цьому випадку для *NB-IoT* виділяються ресурси всередині існуючої LTE несучої, але *NB-IoT* несуча має підвищену потужність на 6дБ порівняно з ресурсними блоками LTE. Цей варіант добре підходить для економії частотного ресурсу, але при цьому є проблема взаємного впливу з LTE мережею

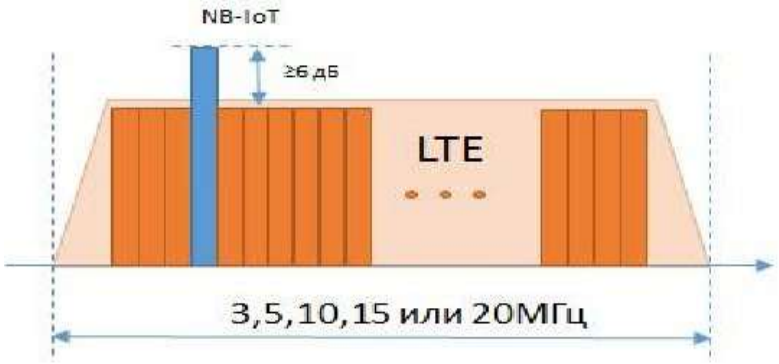


Рис. 8.5. Розміщення NB-IoT в режимі In Band(в середині полоси)

- *Guard Band(в захистній полосі частот)*

В цьому випадку NB-IoT запускається в так званому захисному інтервалі. Наприклад, в смузі LTE 10МГц, по 500 кГц вільного спектру, що використовується в якості захисного інтервалу. Так само як і в режимі *in Band* для більшої дальності *NB-IoT* несуча має підвищену потужність на 6-9 дБ порівняно з ресурсними блоками LTE (Рис. 8.6). Цей варіант використання дозволяє одночасно заощадити частотний ресурс і зменшити взаємний вплив з LTE мережею, хоча в цьому випадку погіршуються параметри позасмугових випромінювань для LTE.

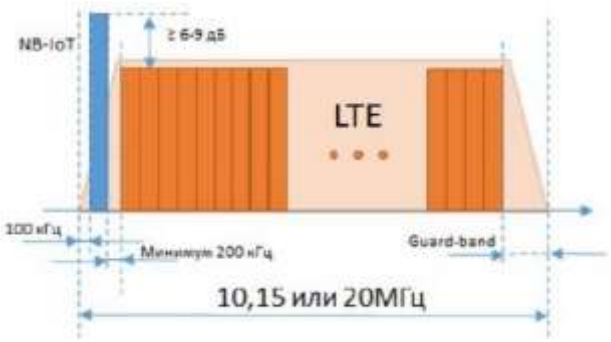


Рис. 8.6. Розміщення NB-IoT в режимі Guard Band (в захистній полосі частот)

8.1.4. Технологія Weightless-P

Weightless-P *— це технологія LPWAN, яка використовується для IoT.*

Вона використовується в тих випадках, коли потрібна довга служба батареї від одного заряду, двонаправлений зв'язок, а також коли потрібна підтримка високої щільності кінцевих пристроїв [7]. Особливостями цієї технології є широка зона покриття, масштабованість мережі, довгий термін роботи батареї та безпека.

Ця технологія підтримує певний невеликий діапазон груп модуляцій та пропонує можливість двонаправленого зв'язку для забезпечення високої якості зв'язку. Одна базова станція може обслуговувати більшу кількість кінцевих пристроїв, ніж інші технології LPWAN.

Базова станція має контроль над своєю мережею і кінцевими пристроями в будь-який час в інших технологіях базова станція не має таких можливостей.

Weightless-P більш розвинута технологія і вона підтримує гарантовану доставку повідомлень, тому їй не потрібно відправляти повідомлення по декілька разів, як в *LoRa*, *SigFox* і через це відбувається економія заряду пристроїв. Також в цій технології використовується метод підтримки адаптивної швидкості передавання інформації і через це забезпечується збільшення терміну служби батареї та підвищується продуктивність роботи мережі.

Також *Weightless-P* підтримує адаптивну зміну швидкості передачі даних, що забезпечує оптимальну продуктивність мережі і збільшує термін служби батареї кінцевих пристроїв, оскільки він регулює фактичну швидкість передачі даних в залежності від близькості кожного вузла до базової станції.

Чим ближче до базової станції кінцеві вузли, тим більш висока швидкість передачі даних, що призводить до більш короткого ефірного часу і більш низької вихідної потужності. Та навпаки вузли, які найбільш віддалені від базової станції, використовують найнижчу швидкість передачі даних і найвищу вихідну потужність.

Більш оптимізований та невеликий по розмірам протокол забезпечує зменшення вартості системи та простоти експлуатації в порівнянні з NB-IoT та іншими стільниковими M2M системами.

Технологія використовується в різних системах спостереження, моніторингу за станом здоров'я людини, розумних речах та ін.

Таблиця. 8.1 Порівняльна характеристика технологій передачі даних на довгі відстані в мережі IoT

Характеристики	LoRaWAN	SigFox	NB-IoT	Weightless-P
Метод модуляцій	CSS	DBPSK/GFSK	GFSK/BPSK/QPSK	GMSK/PSK
Діапазон	ISM	ISM	Ліцензований	ISM
Швидкість	0,3-50 кбіт/с	100 кбіт/с	UL: 1-144 кбіт/с DL: 1-200 кбіт/с	0,2-100 кбіт/с (адаптивна)
Смуга	Широкосмуг.	Вузькосмуг.	Вузькосмуг.	Вузькосмуг.
	до 500 кГц	100 кГц	200 кГц	12,5 кГц
Максимальний час автономної роботи пристроїв	> 10 років	До 20 років	До 10 років	3-5 років
Частота	868,8 МГц (Європа) 915 МГц (США) 433 МГц (Азія)	868,8 МГц (Європа) 915 МГц (США)	800/900/1800 МГц	169/433/470/780/868/915 МГц
Безпека	AES-64/128	AES з HMACs	AES-256	AES-128/256
Дальність	До 2,5 км у місті, до 45 км за містом	До 10 км у місті, до 50 км за містом	до 2 км	До 2 км у місті

8.2. Технології та протоколи передачі даних на короткі відстані в IoT мережах

8.2.1.Технологія Z-Wave

Z-Wave — це безпроводова радіотехнологія з низьким енергоспоживанням [7]. Z-Wave працює в діапазоні частот до 1 ГГц та оптимізована для передавання простих команд для управління з досить малими затримками (зміна гучності телевізору, виключення/включення побутової техніки, зміна яркості екрану тощо).

Вибір частот був зроблений не випадково. Для того, щоб зменшити кількість перешкод від інших технологій, якими вже користуються багато людей, наприклад Wi-Fi сильно навантажений на частоті 2,4 ГГц і тому вже зараз в нашій країні переходять на частоту 5 ГГц.

Технологія *Z-Wave* - ключ до того, щоб мати повний контроль над вашою домашньою безпекою і енергією, з мінімальними клопотами [7].

За допомогою технології *Z-Wave* можливо мати свою власну домашню систему автоматизації, програмувати всі основні елементи будинку, такі як освітлення, нагрівання, готування, охолодження і навіть вашу домашню безпеку.

Переваги не закінчуються цим, хоча це - складна система, вона дуже проста у використанні, а також вона ще є енергозберігаючою та економить наш дорогоцінний час.

Система працює за допомогою дистанційного керування і використовує радіохвилі малої потужності. Ця сіткоподібна мережа покриває всі області будинки, оскільки радіохвилі можуть проходити через стіни, поверхи та меблі, роблячи можливість з'єднання надійним майже на 100%.

Z - Wave Alliance підтриманий корпорацією *Intel,* яка зробила стратегічні інвестиції в компанію *Zensys,* технологію безпроводових комірчастих мереж Z, що розробила, - Wave. Z -

Wave, є системою управління цифровим будинком, побудовану на базі mesh- мережі з дуплексним безпроводовим радіозв'язком FSK. Пропускна спроможність 40 кбіт/с. Відстань: близько 30 метрів на "відкритому повітрі", в приміщенні зменшується залежно від будівельних матеріалів і т.д. *Z - Wave* використовує 900МГц ISM смугу частот, 908.42МГц в США и і 68.42МГц в Європі. Було прийнято рішення відмовитися від роботи на частоті 2,4ГГц, оскільки сигнал 908/868ГГц поширюється приблизно в 2,5 рази далі, чим еквівалентний 2.4ГГц сигнал. Це дозволяє *Z - Wave* радіо потребляти меньше енергії, чим порівнянні безпроводові пристрої, працюючі в смузі 2.4ГГц. Окрім цього смуга 2.4ГГц занадто завантажена, приміром Wi - Fi мережами.

В порівнянні з конкурентами, *Z - wave* пристрої виділяються максимальною простотою і низькою вартістю. Максимальне число вузлів мережі (232) явно недостатньо для промислового застосування, проте, цілком вистачає для домашніх користувачів. Типовий *Z - Wave* чіп містить:

- Радіо трансівер,
- 32 кб flash пам'яті, включаючи *Z - Wave* протокол і додатки,
- Системні інтерфейси, включаючи цифрові і аналогові інтерфейси для приєднання зовнішніх пристроїв, таких як сенсори,
- 3des движок для забезпечення конфіденційності і аутентифікації,
- Тріак контроллер, щоб зменшити вартість додатків, що вимикають світло.

8.2.2. Технологія NFC

Технологія NFC (Near Field Communication) - створена компаніями такими, як *Sony* та *NXP Semiconductors* - являє собою комбінування наявних безконтактних технологій зв'язку та радіочастотної ідентифікації [8].

Технологія *NFC* призначена для обміну різною інформацією, наприклад, картинками, музичними файлами, номерами телефонів, або ключами цифрової авторизації між двома розташованими близько один до одного пристроями з підтримкою NFC. Це можуть бути смарт-картка, будь-які портативні пристрої, а також зчитувальні пристрої RFID. Дана технологія може використовуватися в якості ключу доступу до даних або служб (електричний замок, або безготівкова оплата).

На відміну від усіх інших технологій безконтактного зв'язку, які можуть передавати дані тільки від активного пристрою до пасивного, NFC може здійснювати обмін інформації між двома активними пристроями [9].

NFC використовується для взаємодії з пристроями радіочастотної ідентифікації RFID. Для забезпечення сумісності між картами RFID та мобільним телефоном різних виробників виконується перевірка цифрового протоколу і проводиться вимірювання всіх важливих властивостей радіочастотного сигналу: тимчасових характеристик, чутливості та амплітуди приймача в активному режимі, частоти несної амплітуди сигналу.

Рис. 8.7. Взаємодія пристроїв

При передачі інформації від активного пристрою до пасивного пристрою використовується амплітудна маніпуляція ASK. При обміні обидва пристрої рівноправні.

Кожен пристрій має власне джерело живлення, тому сигнал несної відключається відразу після закінчення передачі.

За рахунок індуктивного зв'язку між опитуваним і прослуховуючим пристроями пасивний пристрій впливає на активне. Зміна імпедансу прослуховуючого пристрою викликає зміну амплітуди або фази напруги на антені опитуваного пристрою. Після цього відбувається з'єднання двох пристроїв та передача даних. Як тільки ми роз'єднуємо два пристрої більш, ніж на 20 см розривається електромагнітний зв'язок і перестають передаватися дані автоматично.

В дійсності NFC можна вважати, по суті, продовженням вже досить відомої технології радіочастотної ідентифікації RFID [10]. Як відомо, RFID повсюдно використовується в безконтактних картах і мітках. Однак NFC може не тільки зчитувати інформацію з будь - яких пасивних електронних міток, але і здатна забезпечувати двосторонній безпроводовий зв'язок між пристроями.

8.2.3. RFID

RFID (Radio Frequency IDentification) *– метод автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються в так званих транспондерах, або RFID – мітках* [10].

Будь-яка *RFID* - система складається із зчитувального пристрою (зчитувач, рідер) та транспондеру (він же RFID - мітка, іноді також називають RFID-тег).

Більшість *RFID*-міток складається з двох частин.

Перша – інтегральна схема для обробки та зберігання інформації, демодулювання та модулювання радіочастотного сигналу і деяких інших функцій.

Друга - антена для прийому і передачі сигналу. А також для роботи цих міток потрібне програмне забезпечення — програми, за допомогою яких здійснюється аналіз та збір інформації, одержуваної із RFID-міток [11].

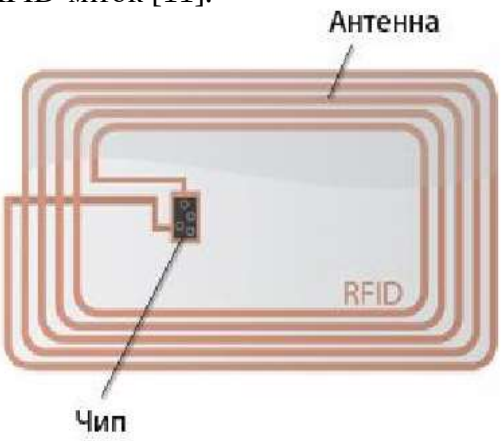


Рис. 8.8. Будова RFID-мітки

Мітки бувають двох видів *активні* та *пасивні. Активні мітки* мають власне джерело живлення, тому вони можуть самі посилати сигнал і зчитуватися з досить великої відстані. *Пасивні мітки* не мають власного джерела енергії і активізуються, тільки після того, коли надходить сигнал до пристрою зчитування і тоді передають записану в них інформацію.

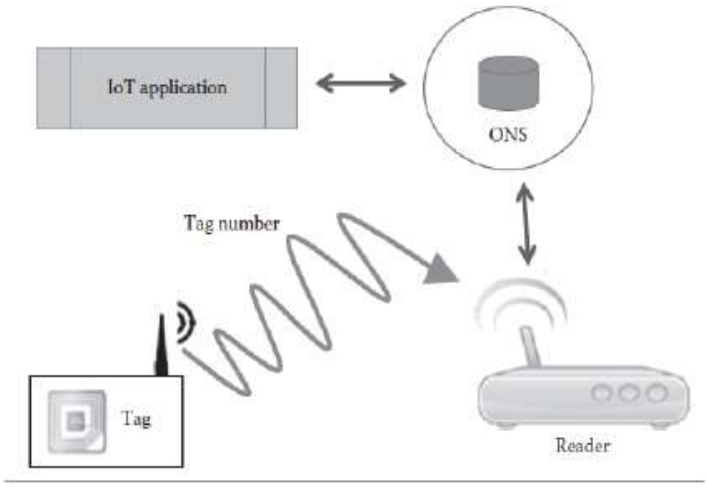


Рис. 8.9. Компоненти RFID системи

Тег RFID має дві основні компоненти: електронний мікросхеми для зберігання ідентичності об'єкта та антени, що дозволяє чіпу спілкуватися з системою читання тегів. Зв'язок між тегом і читачем тегів відбувається за допомогою радіохвиль. Два основних компоненти системи RFID:

- радіоприймач;
- читач тегів.

RFID-мітки можуть використовуватися для управління товарними запасами або відстеження часу на спортивних змаганнях [10]. Магнітні мітки не замінюють штрих-коди, а їх доповнюють можливістю дистанційного зчитування. Мітками можуть маркувати велику рогату худобу для запису інформації про проходження ветеринарного огляду. Рішення для транспорту допомагають ідентифікувати автомобіль, навіть якщо вона рухається на великій швидкості. Деякі авіалінії користуються мітками для ефективного відстеження великих потоків багажу. Також RFID вбудовується у біометричні паспорти, кредитні картки для безпечного доступу в захищені області.

Деякі мітки можуть бути прочитані на відстані декількох метрів від прямої видимості пристрою зчитування. Більшість міток представляють собою звичайний текстовий запис та штрих-код в якості доповнення для прямого зчитування у випадках несправності радіочастотної електроніки.

Електронний код продукту (EPC) - це унікальний ідентифікатор, що зберігається в тезі RFID, що допомагає ідентифікувати та відслідковувати елементи в сценарії керування ланцюжком постачання. *EPCglobal* – це організація, що розробила EPC, а *EPCglobal* також готує та підтримує стандарти, пов'язані з *RFID* та *EPC*. *RFID* може бути використана як ключова технологія для пристроїв IoT з наступних причин:

- Відкритість;
- Масштабованість;
- Надійність;
- Підтримка ідентифікаторів об'єктів та відкриття сервісів.

8.2.4. Bluetooth Low Energy

Безпроводова технологія з низьким енергоспоживанням *Bluetooth (BLE)* – це частина специфікації *Bluetooth,* яка починається з покоління *Bluetooth* 4.0 і на даний момент закінчується *Bluetooth* 5.0 [13].

Пристрої, що використовують BLE, споживають менше енергії, ніж інші версії *Bluetooth* - пристрої попередніх поколінь. У багатьох випадках пристрої зможуть працювати більше року на одній невеличкій батарейці типу таблетка без підзарядки. Завдяки цьому, можна буде використовувати датчики невеликих розмірів, які будуть постійно працювати та взаємодіяти з іншими пристроями.

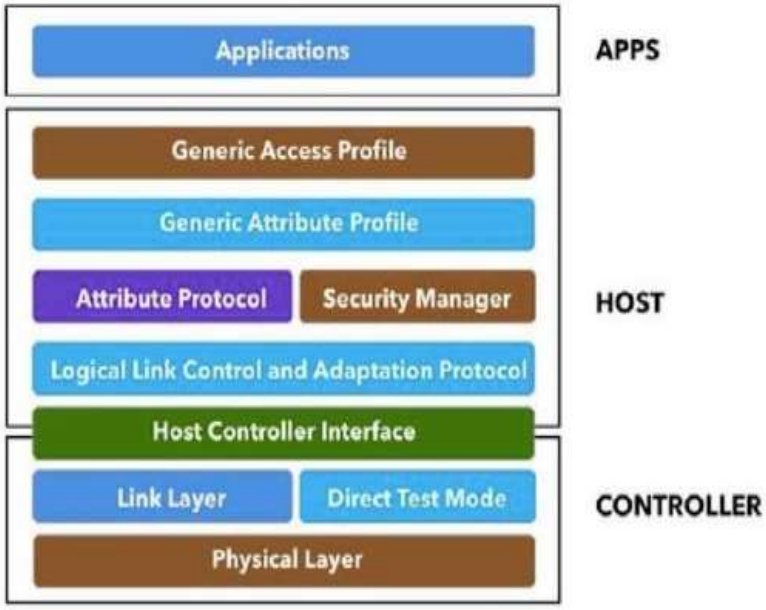


Рис. 8.10. Архітектура BLE

Основними рівнями BLE є:

- *Додаток – реалізує корисну для кінцевого користувача логіку роботи [14].*
- *Основний пристрій, або хост – надає верхні рівні стеку протоколів Bluetooth.*
- *Контролер – займається нижніми рівнями стеку протоколів Bluetooth.*

Рівень додатків – найвищий рівень стеку протоколів.

Рівень хосту містить такі підрівні:

- *GAP (Generic Access Profile) – профіль загального доступу;*
- *GATT (Generic Attribute Profile) – профіль загальних атрибуті;*
- *ATT (Attribute Protocol) – протокол атрибутів;*
- *SM (Security Manager) – менеджер безпеки;*
- *L2CAP (Logical Link Control and Adaptation Protocol) – протокол логічного з'єднання та адаптації;*
- *HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні хосту.*

Рівень контролеру зв'язан за допомогою протоколу HCI та має такі рівні:

- *HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні контролеру;*
- *LL (Link Layer) – канальний рівень;*
- *PHY – фізичний рівень.*

BLE призначений для тих пристроїв, які мають невеликі розміри, тобто для пристроїв, у яких важлива компактність і куди не можна встановити повноцінний акумулятор, або батарею великого об'єму [14]. *Bluetooth LE* споживає в 10-20 разів менше енергії і цілком здатний передавати дані в 50 і більше разів швидше та на відстані більше 100 метрів, ніж класичні *Bluetooth* рішення.

Крім перерахованих вище переваг, BLE має високу безпечність, надійність, низьку затримку при підключенні та низьку споживчу потужність. Є ще одна важлива особливість даного стандарту, вона полягає в адаптивності переналаштування частоти, тобто відбувається захист від помилок при передачі сигналу, BLE швидко змінює свою робочу частоту, вибираючи найбільш оптимальну для усунення перешкод, проблем переповнення і для зниження інтерференції.

Специфікація *Bluetooth* 5.0 була створена, з орієнтацією на Інтернет речей. Це остаточно показало, що стандарт прагне "захопити" ринок пристроїв.

В порівнянні з попередньою версією 4.0 була підвищена швидкість передачі даних майже до швидкостей HSPA і LTE ранніх версій, при цьому енергоспоживання залишилося в колишніх показниках.

Важливим показником для побудови мереж Інтернету речей як раз є енергоефективність. В даний момент дана специфікація є мало поширеною через те що вона з'явилася нещодавно. Bluetooth 5 як і всі попередні версії має зворотну сумісність. Цілком можливо, через декілька років кожний мобільний пристрій буде підтримувати 5 версію цього стандарту, що є найважливішою перевагою цієї технології над іншими.

8.2.5. Wi-Fi HaLow

Wi-Fi HaLow — це протокол безпроводової мережі, опублікований у 2017 році, як доповнення до стандарту бездротової мережі IEEE_802.11 [15]. Цей протокол працює на непотребуючій ліцензування частоті 900 МГц, для забезпечення розширеного діапазону Wi-Fi мереж, порівняно зі звичайними мережами Wi-Fi, працюючими в діапазонах 2,4 ГГц і 5 ГГц. Його низьке енергоспоживання також є перевагою, таким, що дозволяє створювати великі групи станцій або датчиків, які взаємодіють щоб поширювати сигнали, підтримуючи концепцію інтернет-речей (Internet of Things, IoT). Низьке енергоспоживання протоколу конкурує з *Bluetooth* і має додаткову перевагу - вищі швидкості передачі даних і більш широкий діапазон покриття.(див. рис.8.11) [15].

*Wi-Fi HaLo*w дозволить розширити можливості енергоефективного сценарію використання розумного будинку, автомобілів, а також в торгівлі, промисловості, сільському господарстві тощо.

Wi-Fi HaLow розширює Wi-Fi в діапазоні 900 МГц, даючи можливість з'єднання пристроїв малої потужності, таких як датчики та портативні комп'ютери. Wi-Fi HaLow успадкує позитивні якості попередніх протоколів, такі як надійний захист інформації, широку сумістність обладнання та простоту встановки.

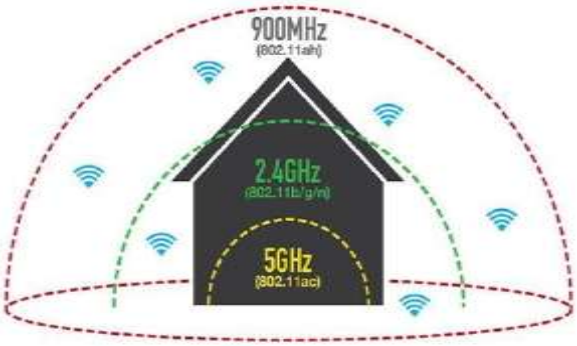


Рис. 8.11. Діапазон покриття Wi-Fi HaLow

Пристрої з підтримкою *Wi-Fi HaLow* будуть також працювати у діапазонах 2,4 та 5 ГГц, що дасть можливість інтегрування в екосистему, яка на даний момент налічує більше 7 млрд пристроїв. Також *Wi-Fi HaLow* буде мати підтримку підключення по IP, це дозволить працювати з хмарами, що дуже важливо для IoT. Також буде можливість підключатися до одієї точки доступу близько 1000 пристроїв.

Таблиця. 8.2.Порівняльна характеристика технологій та протоколів передачі даних на короткі відстані в IoT

Характеристики	**RFID**	**NFC**	**BLE**	**Z-Wave**	**Wi-Fi HaLow**
Смуга частот	6/13,5/433/863-870/902-928 МГц 2,4/5-27 ГГц	13,56 МГц	2,4 ГГц	868/915 МГц	Під діапазон 1 ГГц
Швидкість передачі даних	500 кбіт/с	106/212/424/848 кбіт/с	1 Мбіт/с	9.6, 40 та 100 кбіт/с	До 4 мбіт/с
Радіус дії	0,1-5 м	0,1 м	70 м	100 м	100 – 1000 м
Пропускна здатність на канал	10 МГц для 6 МГц 14 МГц для 13,5 МГц	Змінна	40 каналів з шириною в 2 МГц	300-400 кГц	1/2/4/8/16 МГц
Модуляція	-	ASK,BPSK	GFSK	FSK/GFSK	BPSK, QPSK, 16-/64-/256-Qam,OFDM
Топологія	Point to Point Point to Multipoint	Peer to peer	Singl-Hop	Mesh	Star
Безпека	Шифрування	Шифрування	AES-128	AES-128	WPA

8.3. Сенсорні мережі

Їх основне призначення заключається не тільки в обміні даними між вузлами по децентралізованій самоорганизуючій мережі, але й в зборі інформації, що передається (в основному, данных) від датчиків (температури, тиску, вологості, рівня радіації, акустичних коливань) в центральний вузол з метою її наступного анализу або обробки.

Необхідність безпровідних сенсорних мереж на ринку також тісно пов'язана з концепцією інтелектуалізації таких объєктів як дім, офіс і виробничі приміщення, де міська людина проводить до 90% свого часу, а також з концепцією створення кібернетичних виробництв (повністю оснащених роботами), основною задачею яких є впровадження безпровідних технологій на рівні АСУ ТП [16,17,18].

Що стосується концепції «роумного дому» і створення максимального комфорту на роботі, то в останній час такі безпровідні технології як ***Home RF (Shared Wireless Access Protocol - SWAP)*** і ***Bluetooth*** прийшли на заміну добре відомим проводовим рішенням *LonWork* та *HomePNA,* завоював свою нишу на ринку звя'зку для домашної автоматизації і в сучасних будівлях адміністративно-офісного типу.

Сучасні безпроводові сенсорні мережі домашнього, офісного і промислового використання, орієнтовані в освному на передачу даних, представлені технологіями *ZigBee* і *ZigBeePro* (їх попередні назви *HomeRFlite, Firefly* та *RF-EasyLink*); *Bluetooth; WHart (IEC)* і ISA 100.11a. Стандарт IEEE802.15.4 — основа безпровідних самоорганізуючих сенсорних мереж

Перераховані вище технології представлені різними протоколами верхнього рівня моделі OSI. Не дивлячись на різне призначення, усі стеки протоколів цих технологій (за виключенням *Bluetooth*) розроблені на базі єдиного стандарту LR WPAN IEEE802.15.4, який описує протоколи нижнього рівня (PHY и MAC) моделі OSI і пропонується в якості єдиного низькошвидкісного енергосберігаючого стандарта для безпровідних персональних мереж WPAN [19].

Пізніше у міжнародного стандарта IEEE802.15.4 з'явилось доповнення у вигляді IEEE802.15.4a, яке дозволяє на фізичному рівні повисисти швидкість передачі даних з 250 Кбіт/с до 1 Мбіт/с в 2,4-ГГц ISM-діапазоні і вище, тобто до 480 Мбіт/с з радіусом дії до 2 м (DS UWB) в частотному діапазоні 3…10 ГГц [19].

Одночасно зі стандартом IEEE802.15.4a був створений ще один високошвидкісний стандарт — WPAN скороченого радіусу дії *ECMA 368 (MB UWB)* у вигляді ISO/IEC26907 (см. табл. 8.3) з врахуванням стандартів *WiMedia/MBOA* и рішень по IEEE802.15.3a [19].

Таблиця 8.3. Порівняння стандартів сімейств 802.15 и 802.11

Стандарт/характеристика	**802.15.4 ZigBee™**			**802.15.1 Bluetooth**	**ECMA 368 (802.15.3a for High Rate WPAN),WiMedia (MB UWB OFDM)**	**802.15.4a DS-UWB Chirp (CSS)**	**802.11b Wi-Fi**
Додатки	Моніторинг, управління, мережі датчиков, домашня/промислова автоматика			Голос, дані, заміна кабелей (провідного на безпровідний канал)	Потокові мультимедійні дані, заміна кабелей аудіо/відеосистем		Дані, голос, відео, LAN
Переваги	Ціна, енергосбереження, розміри мережі, вібір частотних діапазонів, DSSS и PSSS			Ціна, енергосбереження, передача голоса, FH	Висока швидкість, енергосбереження		Великий діапазон по швидкості, DSSS
Частота	868 МГц	915 МГц	2,4 ГГц	2,4 ГГц	3,1…10,6 ГГЦ	2,4 ГГц; 3,1…10,6 ГГЦ	2,4 ГГц
Макс. швидкістьь	20 Кбіт/с	40 Кбіт/с	250 Кбіт/с	1, 3, 24 Мбіт/с (доп. 55 Мбіт/с)	53,3; 80; 106,7 МГц Доп.: 160, 200, 320, 400, 489 Мбит/с	250 Кбіт/с, 1 Мбіт/с (chirp); 110 Мбіт/с (10 м), 200 Мбіт/с (4 м); (доп. 480 Мбіт/с)	1 Мбіт/с 2 Мбіт/с 11 Мбіт/с
Вихідна потужність, ном.	От 0 дБм (1 мВт)			0 дБм (клас 3) 4 дБм (клас 2) –30…20 дБм (клас 1)	0 дБм	<100 мВт (110 Мбіт/с) <250 мВт (200 Мбіт/с)	20 дБм
Дальність	1—10 м (укорочений радіус дії) 10—100 м (збільшений радіус дії)			1— 5 м (клас 3 — укорочений радіус) до 15 м (клас 2) 100 м (клас 1)	5…50 м	10 м (110 Мбіт/с) 4м (200 Мбіт/с) 2 м (480 Мбіт/с)	10 м 100 м
Чутливість (специфікація)	–92 дБм	85 дБм	–70 дБм	–75 дБм	–	–76 дБм	
Розмір стека	4…32 Кбайт			Больше 250 Кбайт		–	Більше 1 Мбайт
Срок служби батареї (енергозсбереження)	100—1000+ днів			1—7 днів	Немає статистики Теоретично більше 1000 днів		0,5—5 днів
Розмір мережі	65536 (16-бітні адреси), 264 (64-бітні адреси)			Мастер +7		До 127/хост	32

Обсяг інформації, що формується одним сенсорним вузлом, порівняно невеликий, однак більшість сервісів Інтернету речей побудовано на принципі обробки інформації від безлічі вузлів, що принципово відрізняється від архітектур, прийнятих в класичних мережах, типу абонент - вузол зв'язку для телефонії, клієнт - сервер для передачі даних [15].

Таким чином, ми стикаємося з новою архітектурою: багато джерел - багато одержувачів, крім того, обсяг трафіку від сенсорного вузла може бути як дуже маленьким, так і дуже великим. Звичні прикладні протоколи для передачі повідомлень не розраховані на таке використання.

Оскільки IoT являє собою сенсорну мережу розглянемо загальну архітектуру сенсорної мережі.

Стандартизацією сенсорних мереж займається багато міжнародних організацій, серед яких *ISO, IEC, ITU-T, IEEE* та інші. Так дослідницька група по сенсорних мережах *SGSN (Study Group on Sensor Networks)* об'єднаного технічного комітету *ISO/IEC JTC 1 (Joint Technical Committee 1)* визначила базову архітектуру сенсорної мережі та її основні інтерфейси.

Сенсорний вузол складається з:

- апаратного забезпечення;
- базового програмного забезпечення;

- прикладного програмного забезпечення.

В складі архітектури визначені чотири базових інтерфейси:

1. Інтерфейс між базовим і прикладним програмними забезпеченнями сенсорного вузла.
2. Інтерфейс між базовим програмним і апаратним забезпеченнями сенсорного вузла (сенсори, актуатори та/або комунікаційний вузол і так далі).
3. Безпроводові або проводові інтерфейси між вузлами мережі.
4. Інтерфейс між сенсорною мережею та зовнішнім середовищем (провайдери послуг, користувачі).

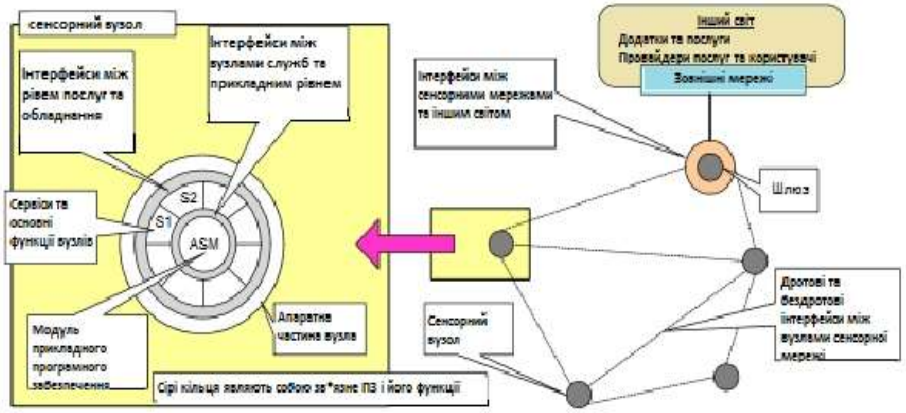


Рис. 8.12. Структура сенсорного вузла

Дані мережі складаються з мініатюрних обчислювальних пристроїв з датчиками, актуаторами і трансіверами (прийомопередавачами), що працюють в заданому діапазоні радіочастот.

Такий вузол БСМ називають сенсорним вузлом або просто сенсором. Сенсорний вузол являє собою плату розміром зазвичай не більше одного кубічного дюйма. На платі розміщуються процесор, пам'ять - флеш і оперативна, цифро-аналогові і аналого-цифрові перетворювачі, радіочастотний приймач, джерело живлення і різні датчики, актуатори. Таким чином, апаратна частина вузла безпроводової мережі може бути розділена на наступні чотири підсистеми:

1) комунікаційна підсистема - забезпечує безпроводовий зв'язок з іншими вузлами в сенсорній мережі і містить радіо приймач;

2) обчислювальна підсистема – забезпечує обробку даних і функціональність вузла і складається з мікроконтролера MCU, до складу якого входять процесор, оперативна SRAM, незалежна EEPROM і флеш-пам'ять, аналого-цифровий перетворювач ADC, таймер, порти входу/виходу;

3) сенсорна підсистема - забезпечує з'єднання сенсорного безпроводового вузла із зовнішнім світом, до складу якої можуть входити аналогові і цифрові сенсори, актуатори;

4) підсистема електроживлення - забезпечує енергетичне постачання всіх елементів безпроводового сенсорного вузла і включає пристрої генерації і акумулювання енергії, а також регулювання напруги.

Датчики можуть бути найрізноманітнішими. Частіше використовуються датчики температури, тиску, вологості, освітленості, вібрації, розташування, рідше - магнітоелектричні, хімічні (наприклад, що вимірюють вміст CO, CO2, рівень радіаційного фону), звукові і деякі інші. Набір застосовуваних датчиків залежить від функцій, які виконуються бездротовими сенсорними мережами.

Рис. 8.13. Апаратна частина вузла сенсорної мережі

Отримані від датчика електричні сигнали часто не готові для обробки, тому вони проходять через стадію перетворення. Наприклад, сигнал часто вимагає підсилення для 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) в цифровий сигнал. В результаті сигнал виходить в цифровій формі і він готовий до подальшої обробки в процесорі і зберігання в пам'яті мікроконтролера. При наявності виконавчих механізмів можлива також передача керуючих впливів від вузлів мережі до зовнішнього середовища через актуатор. Живлення сенсорного вузла здійснюється зазвичай від невеликої батареї.

Крім розміру, є й інші жорсткі обмеження для вузлів БСМ, вони мають:

- споживати дуже мало енергії;
- працювати з великою кількістю вузлів на малих відстанях;
- мати низьку вартість виробництва;
- бути автономними і працювати без обслуговування;
- адаптуватися до навколишнього середовища [5].

Багаторівнева архітектура мережі IoT складається з:

1. *Рівень об'єктів*, також відомий як рівень пристроїв, містить фізичні пристрої, які використовуються для збирання та обробки інформації з екосистеми IoT. Фізичні пристрої включають різні типи датчиків, такі як ті, які зазвичай базуються на технологіях мікроелектромеханічних систем (MEMS).

Датчики можуть бути оптичними, датчиками світла, датчиками, що реагують на жести та близькість, датчиками дотику та відбитків пальців, датчиками тиску та ін. Методи стандартизованого підключення і відтворення повинні використовуватися рівнем об'єктів, щоб інтегрувати та налаштовувати неоднорідні типи датчиків, що належать до пристроїв системи IoT. Дані пристрою, які збираються на цьому рівні переносяться на рівень абстракції об'єкта за допомогою безпечних каналів.

2. *Рівень передачі даних*, які збираються з об'єктів і передаються на рівень керування сервісом за допомогою безпечних каналів передачі.

Передача даних може відбуватися за допомогою будь-якої з таких технологій:

- *RFID*
- *3G*
- *GSM*
- *UMTS*
- *Wi-Fi*
- *Bluetooth low energy*
- *Infrared*
- *ZigBee*

У цьому шарі також присутні спеціалізовані процеси для обробки таких функцій, як хмарне обчислення та керування даними.

3. *Рівень управління сервісом* діє як проміжне програмне забезпечення для системи IoT. Цей шар надає конкретні послуги своєму запиту на основі адрес і імен. Забезпечує гнучкість програмістів IoT у роботі над різними типами неоднорідних об'єктів незалежно від їхніх платформ. Цей шар також обробляє дані, отримані від транспортного рівня. Після обробки даних приймаються необхідні рішення щодо надання необхідних послуг, які потім виконуються за допомогою мережевих протоколів.

4. *Рівень додатків* забезпечує різноманітні види послуг, які вимагає замовник. Тип послуги, що запитується клієнтом, залежить від конкретного випадку використання, прийнятого замовником. Наприклад, якщо розумний дім є розглянутим випадком використання, тоді клієнт може вимагати певні параметри, такі як нагрівання, вентиляція та кондиціонування (HVAC), а також значення температури та вологості.

Цей рівень забезпечує різноманітні види інтелектуальних сервісів, які пропонуються різними гілками розвитку IoT. Деякі з провідних гілок IoT є:

- «розумні» міста;
- «розумна» енергія;
- «розумна» турбота про здоров’я;
- «розумні» будинки;
- «розумний» транспорт;
- «розумна» індустрія.

5. Бізнес рівень виконує загальне управління усіма діями та службами IoT. На цьому рівні використовуються дані, отримані від мережевого рівня, для створення різних компонентів, таких як бізнес-моделі, графіки та блок-схеми. Цей рівень також несе відповідальність за розробку, аналіз, впровадження, оцінку та моніторинг вимог системи IoT, здатний використовувати великий аналіз даних для підтримки прийняття рішень. А також на рівні виконується порівняння отриманих проти очікуваних результатів для підвищення якості послуг.

Основні стандарти

З самого початку розвитку індустрії сенсорних мереж для об'єднання різнопланових пристроїв була потрібна технологія, яка дозволила б об'єднати усі пристрої в єдину мережу на базі протоколу безпровідного зв'язку, який був би одночасно простим і недорогим у використанні, але, в той же час, досить надійним для упевненої передачі даних на відстані, порівнянні з розміром окремої будівлі.

У травні 2003 року була випущена перша версія стандарту 802.15.4 (малопотужні *WPAN*), в подальші два роки були створені відразу два консорціуми, розробляючі і використовуючі технології, грунтовані на цьому стандарті, і покликані впровадити ці технології в сферу автоматизації будинку - *Z - Wave Alliance* і *ZigBee Alliance.*

ZigBee Alliance включає більше 150 членів, включаючи такі компанії як *Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Philips, і Samsung*. Компанія *Ember,* початковий розробник технології *ZigBee,* нещодавно підписала угоду з компанією *STMicroelectronics* про спільну розробку повного спектру рішень наступного покоління, які базуються на технології *ZigBee,* у тому числі устаткування, додатків і програмного забезпечення. *ZigBee* базується на специфікації 802.15.4 версій 2003 роки, максимальна швидкість облаштувань ZigBee – 250 кбіт/с. *ZigBee* базується на специфікації 802.15.4 версій 2003 роки. *ZigBee* працює на трьох *ISM* смугах частот з максимальною швидкістю в 250kbps. Але на нижчих частотах, 908/860MHz, нові *Z - Wave* чіпи забезпечують таку ж або велику швидкість в порівнянні з 802.15.4. Продуктивність RF Z - Wave і ZigBee модулів вимірюване в незашумленному оточенні, такому як відкритий простір з пристроям, що знаходяться на одній лінії однаково.

Проте 802.15.4 має певну перевагу в зашумленному оточенні, із-за складнішої техніки модуляції і розширення спектру. Мережеві можливості *ZigBee* значно ширші, ніж *Z-Wave*:

значно більший розмір мережі (до 64 тисяч пристроїв), декілька варіантів топологій (зірка, mesh і дерево) і т.д.

ZigBee визначає три види пристроїв :

- *Мережевий координатор*. У кожній мережі може бути тільки один, знаходиться в корені мережевого дерева.
- *FFD (Full Function Devices).* Повнофункціональні пристрої, які можуть виконувати функції маршрутизаторів.
- *RFD (Reduced Function Devices).* Крайові пристрої, які не можуть бути маршрутизаторами.

Тільки *FFD* пристрою можуть формувати *mesh*-мережі, тому *ZigBee* також визначає топологію мережі "зірка", яка може включати *RFD* пристрою на кінцях мережі. Також визначена можливість побудови гібридної мережі, що називається кластерним деревом. Таким чином, виходить, що усі можливості *Z - Wave* мережі можуть бути реалізовані як мала частина функціональності *ZigBee*. Проте, це обертається ускладненням протоколу, дорожчанням пристроїв, а також більш високим енергоспоживанням. *ZigBe*е є єдиною стандартизованою безпроводовою технологією, спочатку націленою на наступні додатки моніторингу і контролю, розподілені мережі датчиків, на розгортання безпроводових інформаційних мереж для недорогих малопотужних систем, використовуваних в комерційній, промисловій і домашній автоматиці :

- системи управління освітленням (промислові, муніципальні і домашні);
- промислова і домашня автоматика і управління (опалювання, вентиляція і кондиціонування, допоміжні пристрої і устаткування);
- споживча електроніка, побутова техніка (пральні машини, кавоварки, кондиціонери, повітряні фільтри і так далі);
- периферійне устаткування ПК : миша, клавіатура, ігрові приставки, джойстики;
- системи сигналізації і безпеки, аварійного сповіщення, системи контролю доступу, безконтактні ключі, датчики диму, газу, руху, полум'я, температури, тиску і так далі;
- облаштування медичної діагностики пацієнта, моніторинг стану спортсменів, біодатчики і медичне устаткування;
- віддалене управління і контроль технологічних процесів, управління апаратами, що рухаються, верстатами, промисловим устаткуванням, холодильними установками, облаштуваннями дистанційного збору даних, телеметрія;
- моніторинг систем водо-, газо і теплопостачання, системи управління і інструментального контролю електроенергії, системи житлово-комунального господарства (ЖКГ);
- безпроводові облаштування обміну інформацією, радіомодеми, радіопередача аудіосигналу і фотозображень;
- автомобільна електроніка (системи контролю тиску в шинах, протиугінні системи, системи ідентифікації і діагностики) і т. д.

Однією з основних переваг стандарту *ZigBee/802.15.4* є простота установки і обслуговування подібних пристроїв. Особливості специфікації ZigBee дозволяють з легкістю розгортати безпроводові персональні мережі. Одно з ключових переваг безпровідної системи - це можливість надати людям і пристроям мобільність, а також можливість перепланування. Mesh networks - комірчасті мережі, мережі передачі даних, передачі інформації, що забезпечують можливість, між двома точками по різних шляхах) є ключовим моментом, що забезпечує таку мобільність [16].

Архітектура стека *ZigBee,* базується на стандартній семирівневій моделі *Open Systems Interconnection (OSI)*, але визначає тільки ті рівні з необхідною функціональністю. Стандарт IEEE 802.15.4-2003 визначає два нижні рівні: фізичний рівень (PHY) і підрівень контролю доступу до середовища (MAC).

ZigBee Alliance, грунтуючись на цьому базисі визначає мережевий рівень (NWK) і основу для рівня додатків. Каркас для рівня додатків включає підрівень підтримки додатків (*application support sub - layer (APS*)), об'єкти облаштувань *ZigBee* (*ZigBee device objects (ZDO))* і об'єкти додатки, визначені виробником (manufacturer - defined application objects).

MAC підрівень стандарту *IEEE 802.15.4-2003* контролює доступ до радіо каналу використовуючи *CSMA - CA*. Також в його обов'язки може входити передача сигнальних фреймів, синхронізація і забезпечення надійної передачі даних.

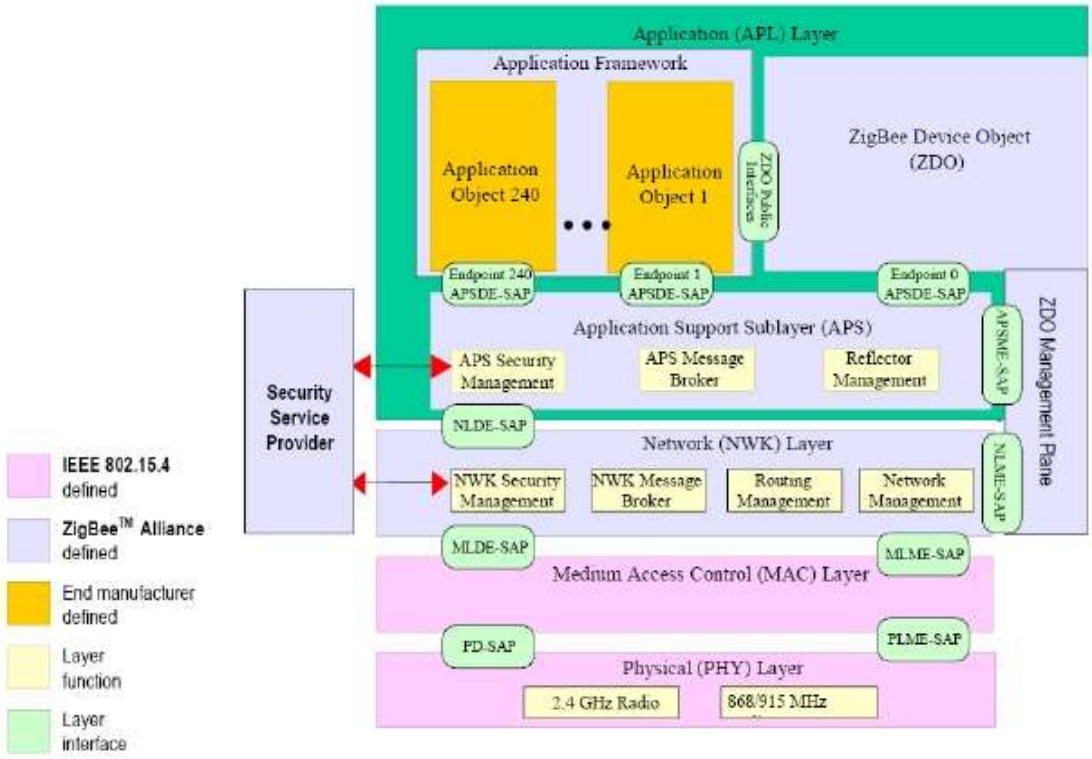


Рис. 8.14. Архітектура стека ZigBee

NWK рівень *ZigBee* повинен забезпечувати механізми:
- Приєднання до мережі і від'єднання від неї
- Додавання шифрування до фреймів
- Маршрутизації фреймів
- Відкриття і підтримка маршрутів між пристроями
- Забезпечення інформації про найближчих сусідів
- Зберігання інформації про сусідні облаштування.

NWK рівень координатора *ZigBee* несе відповідальність за створення новий мережа і привласнення адреса приєднався пристрій.

Рівень додатків *ZigBee* складається з підрівня підтримки додатків *(application support sub - layer (APS)), Application Framework (AF)), ZDO,* і об'єкти додатки, визначені виробником.

Функції підрівня APS включають:
- Підтримку таблиць для зв'язування пристроїв залежно від їх вимог.
- Передачу повідомлень між сусідніми облаштуваннями.

ZDO несе відповідальність за:
- Визначення ролі пристрою усередині мережі (наприклад, *ZigBee* координатор або крайовий пристрій).
- Ініціцація і/або відповідь на запит про зв'язування .
- Встановлення безпечного зв'язку між мережевими пристроями.

ZDO також приєднує нові пристрої до мережі і визначає які функції вони виконують.

Мережеві топології ZigBee

Мережевий рівень *ZigBee (NWK)* підтримує топології зірка, дерево и *mesh*-мережа. При використанні топології зірка, мережа контролюється одним пристроєм, яке називається *ZigBee* координатор. Координатор відповідає за ініціалізацію та підтримку пристроїв в

мережі. При використанні топологій дерево і *mesh*-мережа *ZigBee* координатор відповідає за розгортання мережі і за вибір відповідних ключових параметрів мережі, але мережі може розширятися з використанням *ZigBee* маршрутизаторів. При використанні топології дерево маршрутизатори передають данні й контролює повідомлення в мережі, використовуючи ієрархічну стратегію маршрутизації [17].

Mesh-мережі повинні дозволяти однорангову комуникацію.

На фізичному рівні стандарт IEEE 802.15.4 визачає 3 різні діапазони частоти. В Європі використовується діапазон частот 868 МГц, в США – 915 МГц, діапазон 2,4 ГГц використовується глобально.

Таблиця. 8.4. Смуги частот та швидкості передачі даних

Частота (МГц)	**Полоса частот(МГц)**	**Модуляція**	**Швидкість передачі данних (Кб/с)**
868	868-868.6	BPSK	20
915	902-928	BPSK	40
2450	2400-2483.5	O-QPSK	250

Таблиця. 8.5. Канали та методи обчислення їх частот

Центральна Частота (МГц)	**Число каналів**	**Канал (k)**	**Центральна частота канал (МГц)**
868	1	0	868.3
915	10	1 - 10	906+2(k-1)
2450	16	11 – 16	2405+5(k-11)

Класифікація безпроводових сенсорних мереж

При класифікації сенсорних мереж виникають визначені об’єктивні труднощі, пов’язані з занадто великим переліком можливих задач, що вирішуються подібними системами. Пропонується використовувати наступну модель 3-х факторної класифікації:

I. По вимогам до оперативності передачі показників пристроїв апаратних і програмних датчиків:

1) *Миттєвої передачі*: передача свідчень ініціюється відразу після моменту їх фіксації.

2) *З низькою латентністю*: передача свідчень здійснюється з незначною тимчасовою затримкою, складовою, як правило, одиниці або десятки секунд.

3) *З високою латентністю*: передача одиничних свідчень або груп вибірок здійснюється через значні тимчасові інтервали.

II. За типом організації електроживлення мережі :

1) *Стаціонарні*: живлення усіх вузлів, незалежно від функціонального навантаження, здійснюється від зовнішньої мережі електроживлення або від елементів живлення високої ємності.

2) *Напівстаціонарні*: електроживлення вузлів, що піддаються найбільшому мережевому навантаженню, здійснюється від зовнішньої мережі електроживлення або від елементів живлення високої ємності; крайові вузли мають автономні елементи живлення.

3) *Автономні:* ретранслятори і рядові вузли мережі мають власні обмежені автономні джерела живлення.

III. По розрахунковому терміну служби мережі :

1) *Короткочасного функціонування:* від декількох годин до декількох днів.

2) *Середньострокові функціонування:* до декількох місяців.

3) *Довгострокові функціонування:* до декількох років.

Найбільше охоплення мають 2 основні типи систем : довгострокового функціонування з низькою латентністю і стаціонарні системи довгострокового функціонування з миттєвою реакцією [18].

Підходи, вживані при побудові подібних систем, розрізняються діаметрально. Найбільший інтерес при цьому представляє саме перший клас систем. Дослідження показують, що в цьому випадку необхідно застосовувати простіші мережеві топології (зірка і кластерне дерево), складні алгоритми маршрутизації і тимчасової синхронізації, специфічні методики розділення каналу передачі даних.

Організація доступу до каналу передачі даних

Основні особливості безпроводових сенсорних мереж в порівнянні з усіма іншими системами організованої передачі даних очевидні - це малий радіус радіозв'язку окремого вузла, обмеженість і неможливість поповнення джерела живлення, низькі обчислювальні потужності і малий обсяг доступної пам'яті; високі вимоги до масштабованості вживаних алгоритмів, адаптивність до стрибкоподібних змін топології. Усі вищенаведені особливості накладають деякі рамки на вживані у безпровідних сенсорних мережах стеки протоколів загалом, і на алгоритми тимчасової синхронізації зокрема.

Традиційні методи тимчасової синхронізації, вживані в традиційних мережах передачі даних, абсолютно неприйнятні у безпровідних сенсорних мережах. Головні причини цього - орієнтація традиційних протоколів на досягнення максимально можливих параметрів синхронізації на шкоду загальному завантаженню мережі і обчислювальним потужностям окремих вузлів, тоді як з точки зору сенсорних мереж існує тільки один критерій якості алгоритму тимчасової синхронізації - найменше енергоспоживання крайового пристрою у складі системи. Якраз саме з цієї точки зору і необхідно проводити вибір і оптимізацію алгоритмів.

Види топологій

Найбільш розумними з енергетичної точки зору видаються топологи точка-точка, — зірка (рисунок 8.15 *а*)) і кластерне дерево (рисунок 8.15 *с*). Основна перевага цих топологий полягає в тому, що кожен пристрій заздалегідь знає очікувані часи виходу на зв'язок своїх безпосередніх сусідів, оскільки їх, як правило, обмежена кількість. Є можливість заносити дані на кожен конкретний сусідній пристрій в таблиці маршрутизації. У свою чергу, багатоосередкова (окремий випадок - повнозв'язна) топологія значно менш бажана з енергетичної точки зору з ряду причин. По - перше, це чисто апаратні обмеження обчислювальних можливостей і обсягу пам'яті у вживаних недорогих мікроконтролерах. Як правило, обсяг ОЗУ подібних пристроїв обмежується, у кращому разі, одним - двома кілобайтами, чого явно бракує для формування і обробки повноцінних таблиць маршрутизації.

Це пов'язано з тим, що повноцінні таблиці повинні містити дані про потужність сигналу від сусідніх пристроїв (можливо, навіть за декілька сеансів зв'язку); їх мережеві ідентифікатори; можливо, ключі шифрування даних для кожного сусіднього пристрою (причому ключів може бути і декілька); тимчасові інтервали виходу на зв'язок і дані, необхідні для самих операцій тимчасової синхронізації і т.д.

По-друге, кожному окремому пристрою необхідно виходити на зв'язок з більшою періодичністю, що чинить пряму дію на тривалість функціонування пристрою. По-третє, подібна організація мережі накладає більше жорсткі рамки на алгоритми синхронізації, оскільки крайовому вузлу необхідно працювати в єдиному тимчасовому полі, саме менше, з усіма пристроями в зоні безпосередньої радіовидимості.

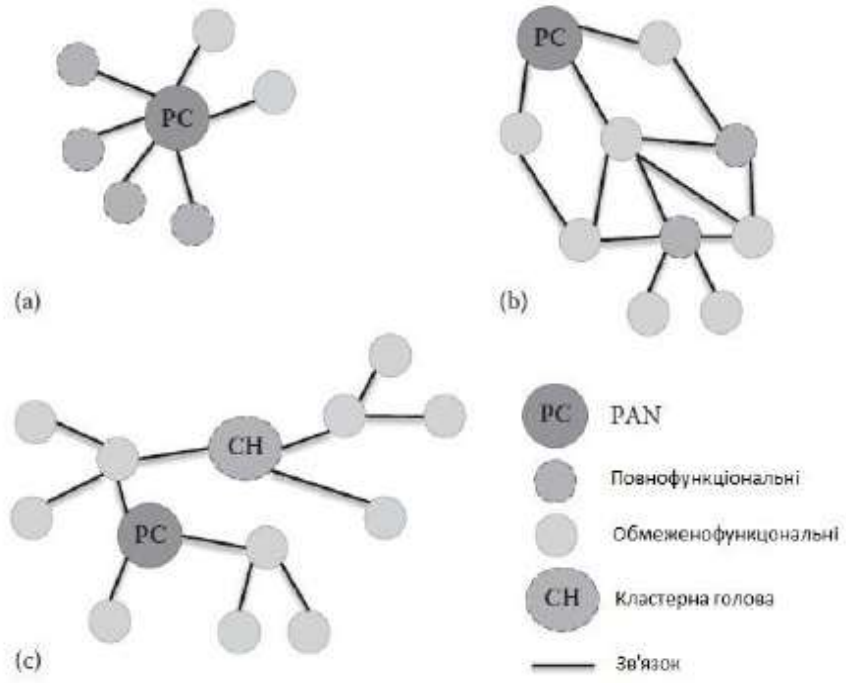


Рис. 8.15. Види топологій сенсорних мереж

Топологія типу — зірка є, мабуть, найпростішою в реалізації. У такій мережі автономними є тільки крайові пристрої. Центральним пристроєм є координатор мережі, що працює від зовнішнього джерела живлення і володіє, частенько, великими обчислювальними можливостями, чим рядові вузли мережі. Для реалізації подібних мереж найбільш прийнятним видається використання алгоритму CSMA/CA (алгоритм з виявленням частоти, що несе, і відвертанням колізій) без синхронізації доступу до радіоканалу. Описати його можна таким чином: у разі, якщо відносно каналу передачі даних приймається рішення про можливість передачі (канал вільний, несуча не виявлена), то через інтервал часу, рівний деякому випадковому числу із заданого інтервалу часу T1, облаштування передає кадр даних. Початок часу передачі вибирається випадковим чином для відвертання колізії з кадром даних від іншого пристрою [19].

Якщо було прийнято рішення про те, що канал зайнятий (несуча виявлена), спроба передачі поновлюється через інтервал часу, рівний деякому випадковому числу із заданого інтервалу часу T2. Прийом кадру даних може підтверджуватися кадром-квитанцією. Прийом вважається правильним у разі відсутності помилок в кадрі даних. Ця перевірка робиться кодом CRC. Якщо кадр-квитанція отримана з помилками, спроба передачі кадру даних робиться повторно.

Цей алгоритм, як вже говорилося раніше, придатний, переважно, для мереж з топологією — зірка, в яких координатор PAN повинен постійно "слухати" ефір. Можливо застосовувати подібний алгоритм і для мереж з топологією точка-точка, але за умови, що усі мережеві пристрої повинні постійно слухати ефір.

Значно складніший випадок - мережа, організована у вигляді *кластерного дерева*. Доступ до фізичного середовища передачі даних в мережах цього класу робиться вже, переважно, в синхронному режимі. Можливий, звичайно, варіант розбиття суперкадру на окремі інтервали, в кожному з яких тип доступу до каналу різниться. В цьому випадку доступ до радіоканалу в мережі робиться під управлінням координатора, який періодично випромінює сигнали-маяки (B). При цьому доступ до радіоканалу і розклад — сну мережевих пристроїв — прив'язані до сигналів маяків від координатора. Часовий інтервал між двома сигналами маяків (BI) від координатора розбитий на дві частини: активну і неактивну. Під час неактивної частини координатор і усі інші пристрої можуть знаходитися

в режимі сну. Під час активної частини координатор дозволяє доступ мережевим пристроям, що прокинулися. Активна частина, власне, і носить назву суперкадру. Тривалість суперкадру розділена на два інтервали. Під час першого інтервалу (*CAP*) надається доступ на конкурентній основі відповідно до алгоритму *CSMA/CA* [19].

Сенсорні мережі ідеальні для багатьох застосувань. Приклади таких застосувань включають моніторинг важливих інфраструктур таких, як енергомережі, збір даних в складних і небезпечних умовах, військові операції. У більшості додатків необхідно гарантувати безпеку сенсорних мереж також, як і їх застосувань, в несприятливих умовах, особливо, коли помилка додатків (напр. необхідний захист інфраструктур) може привести до катастрофічних наслідків, здатних вплинути на безпеку, цю структуру і суспільство в цілому. Іншими словами сенсорні мережі і їх застосування повинні працювати, згідно з очікуваннями, в несприятливих умовах, де існує загроза атаки, навіть якщо деякі вузли вийдуть з ладу або буде розкритий їх захист. Проте деякі унікальні властивості сенсорних мереж роблять досить важкою саму проблему реалізації безпеки.

По-перше, сенсорні вузли зазвичай мають обмежені енергоресурси із-за потреби в зниженні вартості. В результаті стає небажаним саме використання таких механізмів, як криптографія з відкритим ключем на цих вузлах.

По-друге, сенсорні мережі частенько розгортаються, як автоматичні, таким чином піддаються фізичним діям. Сенсорні вузли можуть бути захоплені, і будь-яка інформація на захоплених вузлах може потенційно бути відкрита загарбникові. Таким чином, будь-який механізм захисту для сенсорних мереж має бути стійкий до захоплених вузлів.

По-третє, більшість додатків сенсорних мереж залежать від локальних обчислень і з'єднань, із-за обмежених енергоресурсів вузла. Проте, певний загарбник може атакувати будь-який вузол сенсорної мережі і використати інформацію, передану з вузлів з порушеним захистом для злому інших вузлів в цьому районі. Усе це посилює дисбаланс між загрозою і захищеністю.

Атаки в сенсорних мережах

У безпроводових сенсорних мережах можна виділити наступні різновиди атак.

DOS - атака з постановкою активних радіоперешкод. У рамках цієї атаки, порушник глушить радіопередачі сенсорної мережі за допомогою потужного радіопередавача, працюючого в тій же смузі частот. Ясно, що такій атаці не може протистояти будь-який протокол. Проте можливість протистояти такій атаці не слід включати в список вимог до протоколу з наступних причин [20]:

- DOS - атака легко може бути виявлена базовою станцією і припинена за допомогою фізичних заходів (локалізація і усунення джерела перешкод);
- Якщо виключити хуліганські явища, реалізація такої атаки не є метою порушника. Метою дійсного порушника швидше буде заплановане спотворення в потрібному напрямі картини свідчень сенсорної мережі в цілому або її окремій області.

Атака відтворенням. На мережевому рівні - багато протоколів передбачають розсилку сусідам сигнального пакету. Відтворюючи ці пакети можна впливати на формування топології мережі. На рівні передачі даних небезпека уявляє відтворення підтвердження про прийом пакету. За допомогою такого відтворення можна переконати сенсор, що помилкова радіопередача була успішно прийнята.

Тунельна атака. У разі цієї атаки пакети, отримані в одному кінці мережі, швидко передаються по високошвидкісному каналу зв'язку на інший кінець мережі і там відтворюються. Може бути особливо небезпечною у поєднанні з іншими видами атак.

Виборча маршрутизація. У разі оволодіння порушником декількома сенсорами, він може управляти ними і здійснювати маршрутизацію тільки вигідних йому повідомлень.

Фальсифікація маршрутної інформації. Багато протоколів маршрутизації передбачають ухвалення рішень про побудову топології мережі на основі інформації, що отримується від сусідніх сенсорів. Ця інформація може включати такі характеристики як, число ходів до базової станції або вартість доставки пакету. Фальсифікуючи цю інформацію,

порушник може зробити скомпрометований сенсор особливо привабливим для сусідів, перенаправивши через нього значну долю трафіку сенсорної мережі [21].

Атака "розмноженням". Припустимо, що використовується загальний ключ канального шифрування на усю сенсорну мережу. Тоді, скомпрометувавши один сенсор, порушник може його розмножити, створивши віртуальні сенсори з різними ідентифікаторами. Замість цих сенсорів радіопередачу вестиме порушник. Розподіл ключів шифрування.

Методи управління ключем, вимагають використання криптографічних функцій, які забезпечують конфіденційність, аутентифікацію і цілісність мережі. Криптографічні функції можуть забезпечувати ці послуги безпеки, виконуючи примітивні функції, різними методами генерації і розподілу ключа. Вибір і розташування криптографічних функцій по мережі впливає на споживання енергії окремих вузлів і, таким чином, змінює баланс енергії по усій мережі. Деякі функції характеризуються симетричними витратами енергії, коли приймач і передавач оброблюваного повідомлення споживає відносно рівну кількість енергії, наприклад алгоритми симетричної криптографії.

У інших випадках споживання енергії ассиметрично з різними витратами на передавачі і приймачі повідомлення, наприклад алгоритми ассиметричной криптографії відкритого ключа. Кількість енергії, спожитої функцією безпеки на заданому мікропроцесорі, головним чином визначається споживаною процесором потужністю, тактовою частотою і кількістю тактових імпульсів, потрібних процесору, щоб розрахувати функцію безпеки. Криптографічний алгоритм і ефективність застосування програмного забезпечення визначають число тактів, необхідних для виконання функції безпеки.

Контрольні питання до розділу

1. Технологія LoRaWAN. Особливості застосування.
2. Які типи пристроїв використовуються в LoRaWAN?
3. Наведіть архітектуру мережі LoRaWAN. З яких вузлів вона складається?
4. Один *LoRa-шлюз* допускає обслуговування до п'яти тисяч кінцевих пристроїв, що досягається за рахунок:
   a) Особливостей топології мережі.
   b) Адаптивної швидкості передачі даних і адаптивної вихідний потужності пристроїв, що задаються мережевим вузлом.
   c) Тимчасовим поділом доступу до середовища.
   d) Частотним поділом каналів.
   e) Особливістю LoRa модуляції, що дозволяє в одному частотному каналі одночасно демодулювати сигнали, що передаються на різних швидкостях.
   f) Часовим поділом каналів.
5. Технологія SigFox. Особливості. Зона покриття в містах та сількій місцевості.
6. Наведіть архітектуру мережі *SigFox*.
7. В яких областях можуть бути використані мережі *SigFox* ?
8. Наведіть переваги та недоліки технології *SigFox.*
9. Стандарт NB-IoT. Особливості застосування.
10. Наведіть варіанти розміщення NB-IoT в режимі Stand – Alone.
11. Технологія Weightless-P. Особливості застосування.
12. Технологія Z-Wave. Переваги та недоліки.
13. Наведіть склад типового *Z - Wave* чіпу.
14. Технологія NFC. Призначення. Особливості застосування.
15. Метод автоматичної ідентифікації об’єктів RFID. Будова RFID-мітки.
16. Наведіть компоненти RFID системи.
17. Технологія *Bluetooth Low Energy*. Архітектура *Bluetooth Low Energy*.
18. Протокол *Wi-Fi HaLow.* Особливості роботи.
19. Сенсорні мережі.Основні стандарти, які використовуються для IoT.

20. Наведіть структуру сенсорного вузла.
21. Наведіть структуру апаратної частини вузла сенсорної мережі.
22. Крім розміру, є й інші жорсткі обмеження для вузлів БСМ, вони мають:
    a) *споживати дуже мало енергії;*
    b) *працювати з великою кількістю вузлів на малих відстанях;*
    c) *мати низьку вартість виробництва;*
    d) *бути автономними і працювати без обслуговування;*
    e) *адаптуватися до навколишнього середовища* .
23. З яких рівнів складається багаторівнева архітектура мережі IoT. Особливості рівнів.
24. Архітектура стека *ZigBee.*
25. Наведіть класифікацію безпроводових сенсорних мереж?
26. Які існують види топологій сенсорних мереж?
27. Атаки в сенсорних мережах.

Список рекомендованої літератури

1. ОБЗОР И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ LPWAN СЕТЕЙ // електрон. текст. Дані URL: www.sut.ru/doci/nauka/review/20164/33-48.pdf
2. История появления технологии LoRa // електрон. текст. дані URL: https://nekta.tech/technology/
3. ЧТО ТАКОЕ LORA? // електрон. текст. дані URL: http://lo-ra.ru/lora/
4. MAC Layer Protocols for Internet of Things: A Survey // електрон. текст. дані URL: https://www.mdpi.com/1999-5903/11/1/16/htm
5. Sigfox Technology // електрон. текст. дані URL: https://www.betasolutions.co.nz/Blog/17/Sigfox-Technology-Review
6. NB-IoT: как он работает? Часть1 // електрон. текст. дані URL: https://m.habr.com/ru/company/ru_mts/blog/430496/
7. Z-Wave Technical Basics // електрон. текст. дані URL: https://www.domotiga.nl/attachments/download/1075/Z-Wave%20Technical%20Basics-small.pdf
8. Технология NFC — связь на близком расстоянии // електрон. текст. дані URL: http://www.russianelectronics.ru/leader-r/review/2187/doc/57689/
9. Технология NFC принципы работы и преимущества // електрон. текст. дані URL: http://www.fotokomok.ru/texnologiya-nfc-principy-raboty-i- preimushhestva/
10. RFID-технология // електрон. текст. Дані URL: https://www.idexpert.ru/technology/121/
11. RFID-технологии и магнитные метки // електрон. текст. дані URL: http://allta.com.ua/what-is-rfid
12. Bluetooth с низким энергопотреблением // електрон. текст. Дані URL: https://ru.m.wikipedia.org/wiki/Bluetooth_%D1%81_%D0%BD%D0%B8%D0%B7%D0%BA%D0%B8%D0%BC_%D1%8D%D0%BD%D0%B5%D1%80%D0%B3%D0%BE%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%D0%BC
13. The Basics of Bluetooth Low Energy (BLE) // електрон. текст. Дані URL: https://www.novelbits.io/basics-bluetooth-low-energy/
14. ПРИМЕНЕНИЕ BLUETOOTH-ТЕХНОЛОГИИ В ИНТЕРНЕТЕ ВЕЩЕЙ // електрон. текст. Дані URL: https://cyberleninka.ru/article/v/primenenie-bluetooth-tehnologii-v-internete-veschey
15. Wi-Fi HaLow (IEEE 802.11ah) — дальнобойное беспроводное подключение с низким энергопотреблением для интернета вещей // електрон. текст. дані URL: https://www.ixbt.com/news/2016/01/05/wi-fi-halow-ieee-802-11ah.html
16. Жураковский Б. Ю. Обробка інформації в сенсорних мережах / Б. Ю. Жураковский, І. Р. Пархомей, В. А. Дружинін. // Адаптивні системи автоматичного управління. – 2018. – №1. – С. 42–57. URL: http://www.irbis-nbuv.gov.ua/cgi-

bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=asau_2018_1_7

17. Zhurakovskiy B. Assessment. Technique and Selection of Interconnecting Line of Information Networks [Електронний ресурс] / B. Zhurakovskiy, N. Tsopa // 3rd International Conference on Advanced Information and Communications Technologies (AICT). – 2019. – Режим доступу до ресурсу: DOI: 10.1109/AIACT.2019.8847726. *Proceedings (2019) 71-75.* (*Scopus*).
18. Features of processing signals from stationary radiation sources in multi-position radio monitoring systems, / [Druzhynin, V., Toliupa, S., Pliushch, O., Stepanov, M., Zhurakovskyi, B.] // CEUR Workshop Proceedings, 2746, pp. 46-65 . – 2020. – Режим доступу до ресурсу: http://ceur-ws.org/Vol-2746/(*Scopus*).
19. Жураковський Б. Ю. Комп'ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 372 с. – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/36641
20. Karygiannis and E. Antonakakis, *"MANET and Sensor Network Security",* ACM/IEEE MSWiM 2006, 9th Annual International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, October 2-6, 2006.
21. K. Wagner, ―*Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures."* First IEEE International Workshop Sensor Network Protocols and Applications (SNPA'03).

РОЗДІЛ 9. ШТРИХОВЕ КОДУВАННЯ

Еталонна модель IoT від Міжнародного союзу електрозв'язку (МСЕ-Т), яка описана в Рекомендації Y.2060, дає визначення різноманітним пристроям, які в неї входять, в тому числі і носію даних. *Носій даних (Data Carrier)* - безбатарейний об'єкт перенесення даних, підключений до фізичної речі і має можливість надавати інформацію придатному для цього пристрою збору даних. Ця категорія включає одновимірні та двовимірні штрих-коди, в тому числі і QR-коди, наклеєні на фізичні речі.

На сьогоднішній день офіційно існує більше 50-ти типів одновимірних (1D) і більше 70-ти двовимірних (2D) штрих-кодів і їх кількість постійно збільшується. Одномірні і двовимірні штрих-коди найбільш відомі і широко поширені, однак бувають і інші види штрих-коду, менш відомі.

Отже, за видами, штрих-коди поділяються на:

• Лінійні одномірні (1D) (також їх називають GS1 або RSS - цю абревіатуру намагаються не використовувати, так як є така ж з іншим значенням);

• Двовимірні (2D), в тому числі матричні і композитні;

• Особливі кольорові штрих-коди, їх відносять до розряду тривимірних (Color C Code (CCC) або 3D);

• Чотиривимірні (4D);

• Композитні - розміщені поруч будь-який лінійний штрих-код і двовимірні MicroPDF417 (композитний штрих-код тип А) або PDF417 (композитний штрих-код тип С).

Лінійні (одновимірні) - це штрих коди, що читаються в одному напрямку (зазвичай, по горизонталі). Найбільш розповсюдженний є такі лінійні символіки: EAN, UPC, Code39, Code128, Codabar, Interleaved 2 of 5. Лінійні штрих коди дозволяють кодувати невеликий об'єм інформації (до 20-30 символів - зазвичай цифр) за допомогою нескладних штрих-кодів, що читаються недорогими сканерами .

Двовимірними називаються символіки, розроблені для кодування великого обсягу інформації (до декількох сторінок тексту). Двовимірний код зчитується за допомогою спеціального сканера двомірних кодів і дозволяє швидко і безпомилково вводити великий обсяг інформації. Розшифровка такого коду проводиться в двох вимірах (по горизонталі і по вертикалі).

Тривимірні «Color C Code» з'явилися порівняно відносно недавно - в 2010 році. На відміну від одновимірного або двовимірного штрих-коду вони можуть містити в собі будь-яку цифрову інформацію: документи, зображення, звук, анімацію і т.д. Однак не всі кольорові штрих-коди відносяться до розряду тривимірних.

Чотиривимірні штрих-коди зустрічаються вкрай рідко, та й технології їх створення та розшифровки поки нерозповсюджені. Обсяг кодованої інформації в них може бути ще більше, ніж в тривимірних кодах, вони можуть вміщати цілі сторінки сайтів, фото, рекламні та інші відео ролики і т.д.

9.1. Особливості штрихових кодів

Існує багато різних типів штрих коду розроблених для оптимізації одного чи кілька критеріїв:

Висока інформаційна щільність, або високий дозвіл. Мініатюрні типи штрих-коду можуть бути надруковані і використані на виробах, де місце для кріплення обмежено, наприклад, друковані плати.

Оптимальне розташування даних, коли можливість помилок читання практично нульова. Це дуже важливо для застосувань штрих коду в медицині.

Легкість дешифрування. Деякі типи штрихових кодів використовують технологію кодування, яка широко підтримується виробниками сканерів. Штрих коди, наприклад, що використовуються в роздрібній торгівлі, мають точно визначений зміст даних. Вони структуруються для забезпечення зручності великої кількості користувачів.

Деякі типи штрих коду розроблені з підтримкою значної кількості наборів символів, тоді як інші підтримують лише цифрові дані.

Найбільш широке розповсюдження на сьогоднішній день отримав Двовимірний код (або 2-D код) - найбільш загальне найменування для всього цього класу символік.

Назви *стековая символіка* (stacked symbology) або *багаторядний код* (multi-row code) більш точно відображають сутність серії кодів, в яких дані кодуються у вигляді кількох рядків звичайних одновимірних штрих-кодів.

Назва матричний код (*Matrix code*) застосовується для позначення двовимірних кодів, заснованих на розташуванні чорних елементів усередині матриці. Кожен чорний елемент має однаковий розмір і позиція елемента кодує дані.

Звичайний штрихкод має "вертикальну надмірність", що означає що одна і та ж інформація повторюється по вертикалі. Це дійсно одновимірний штрих. Висота штрихів може бути зменшена без втрати інформації. Однак, вертикальна надмірність дозволяє штрихкоду, що має дефекти друку (наприклад плями або просвіти) зберігати можливість прочитання.

Двомірний код містить інформацію як по горизонталі, так і по вертикалі. Фактично, всі алфавіти є аналог двомірного коду. Оскільки обидва напрямки містять інформацію, втрачається можливість використання вертикальної надмірності. Для запобігання втрати читабельності і забезпечення швидкості зчитування повинна використовуватися інша технологія. Боротьба з помилками забезпечується досить просто - большиство двомірних кодів використовують спеціальні контрольні суми, що дозволяють гарантувати достовірність інформації, що вводиться.

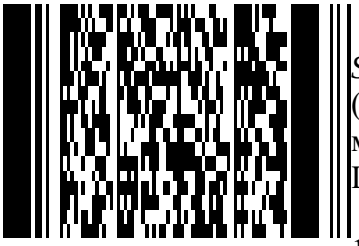
2-D символіки стали більш прийнятними зі збільшенням використання сканерів з лазерним променем і з приладами CCD. Тепер можна читати такі коди просто провівши або махнувши рукою зі сканером над символікою. Швидкість такого руху, дозвіл сканера і дистанція сканер-символіка залишаються такими ж критичними як і з контактними зчитувачами і одновимірними штрихкодами.

Спочатку двомірні коди розроблялися для додатків, що не дають місця, достатнього для розміщення звичайного штрихкодового ідентифікатора. Першим застосуванням для таких символів стали фасування лікарських препаратів в охороні здоров'я. Ці фасування малі за розмірами і мають мало місця для розміщення штрих-коду. Електронна промисловість також проявляє інтерес до кодів високої щільності і двомірним кодами в зв'язку зі зменшенням розмірів елементів і виробів [1].

Можливість кодування портативної бази даних зробила двомірні коди привабливими для додатків, в яких мінімізація розміру коду не є основною вимогою. Наприклад, зберігання імені, адреси та демографічної інформації на картках прямої комерційної розсилки (direct mail business reply cards). Якщо повернута картка містить тільки ідентифікатор, який використовується як ключ до бази даних, то ймовірно, що картки доведеться звіряти з величезною базою даних, що містить мільйони імен. Це зажадає великих витрат на комп'ютерну обробку та зберігання такої бази. Якщо вся важлива інформація буде надрукована одночасно з печаткою пропозиції на картці, істотного збільшення витрат не відбудеться, а інформація буде швидко введена з картки в комп'ютер. Працівникові набагато зручніше зчитати двомірний штрих-код за допомогою портативного пристрою, ніж звертатися до комп'ютера, розташованого в офісі.

9.2.Ніайбільш популярні двовимірні штрихові коди

Штриховий код PDF 417



Стекова символіка *PDF417* була введена в 1991 році фірмою *Symbol Technologies*. PDF походить від скорочення Portable Data File (Портативний Файл Даних), штрихкодову символ складається з 17 модулів, кожен з яких містить 4 штриха і пробілу (звідси номер 417). Штрихкод відкритий для загального користування.

Структура коду підтримує кодування максимального числа від 1000 до 2000 символів в одному коді за інформаційної щільності від 100 до 340 символів. Кожен код містить стартову і стопову групи штрихів, що збільшують висоту штрих-коду.

Код *PDF417* зчитується за допомогою спеціального лазерного або CCD-сканера. Символіка штрихового коду PDF417 представляє хороші можливості для кодування призначених для користувача даних в компактному і зручному для автоматичного зчитування та вигляді. Для того, щоб забезпечити високий рівень надійності зчитування конкретного символу *PDF417* сканерами штрихових кодів, при завданні його параметрів перед друком необхідно враховувати ряд рекомендацій. Розділимо їх на дві групи:

1) Рекомендації на відносні розміри елементів штрихового коду;

2) Рекомендації по вибору рівня корекції помилок.

Рекомендації на відносні розміри елементів штрихового коду.

Кожен символ *PDF417* являє собою прямокутну матрицю, складену з знаків символу, кожному з яких відповідає кодове слово - число від 0 до 928. Знак символу - це послідовність з чотирьох штрихів і чотирьох прогалин, ширини яких кратні деякій величині, званої шириною модуля або просто модулем . Ширини всіх штрихів і прогалин знака можуть бути від 1 до 6 модулів, а сукупна ширина всіх його елементів повинна дорівнювати 17 модулів.

Значення ширини модуля має бути одним і тим же для всіх знаків даного символу. Висотою модуля називається висота одного рядка символу *PDF417*. Всі рядки повинні мати однакову висоту. ГОСТ, що описує специфікацію символіки *PDF417*, рекомендує наступні співвідношення між шириною (X) і висотою (Y) модуля:

а) для символів, рівень корекції помилок в яких не менше мінімального рекомендованого (див. пункт 2): $Y \geq 3X$;

б) для символів, рівень корекції помилок в яких менше мінімального рекомендованого: $Y \geq 4X$;

Також бажано, щоб у всіх випадках $Y \leq 6X$.

Нижче зображені три символи *PDF417*, в яких закодовані одні й ті ж дані, але в перших двох з них не враховані рекомендації, тому їх автоматичне зчитування може бути ускладнене:

В останньому символі рекомендації враховані, він добре підходить для автоматичного сканування:

Важливо, щоб навколо символу *PDF417* була залишена вільна зона - область кольору фону, вільна від зображень і написів. ГОСТ рекомендує, щоб ширина вільної зони, що оточує символ *PDF417* по периметру, дорівнювала 2X.

Рекомендації по вибору рівня корекції помилок.

Специфікація символіки *PDF417* передбачає можливість корекції помилок або, інакше кажучи, можливість повноцінного зчитування частково пошкодженого символу. Пошкодженням ми називаємо будь-яке спотворення символу, викликане поганою якістю друку, попаданням бруду, перекриттям його іншими об'єктами, а також невдалими умовами сканування (ракурс, освітлення, відстань до сканера) і іншими явищами, через які зображення символу *PDF417,* що отримується сканером, буде неякісним. Корекція помилок реалізується за рахунок того, що в символі кодуються не тільки призначені для користувача дані, але ще й спеціальна послідовність кодових слів, званих кодовими словами корекції помилок.

У специфікації *PDF417* передбачені 9 рівнів корекції помилок, кожному з яких відповідає своє кількість кодових слів корекції помилок. Якщо s = 0 ... 8 - це рівень корекції помилок, то відповідне йому кількість кодових слів дорівнює 2 (s + 1). Створення цієї послідовності здійснює конкретний генератор символів *PDF417*. Рівень виправлення помилок задається користувачем. Чим вище рівень корекції, тим більші пошкодження символу допустимі при збереженні можливості зчитування. Наприклад, при s = 0 зчитування стає неможливим при пошкодженні навіть одного знака символу (див. Пункт 1), тоді як рівень s = 4 гарантує зчитування символу, в якому пошкоджено до 15 знаків символу, а в деяких випадках і до 30.

ГОСТ містить рекомендації щодо вибору рівня корекції помилок в залежності від кількості кодових слів, що містять призначені для користувача дані.

Таблиця 9.1. Рівні коректування помилок

Кількість кодових слів даних користувача	Мінімальний рівень коректування помилок
От 1 до 40	2
От 41 до 160	3
От 161 до 320	4
От 321 до 863	5

Необхідна кількість кодових слів призначених для користувача даних можна приблизно обчислити виходячи з характеру даних, дотримуючись рекомендацій:

а) якщо дані представляють собою тільки послідовність цифр, то шукана кількість кодових слів даних буде приблизно дорівнює кількості цифр, діленому на 2.9;

б) якщо дані є текстовими, то кількість кодових слів можна оцінити як кількість текстових знаків, поділене на 1.8;

в) в інших випадках приблизну кількість кодових слів даних дорівнюватиме розміру призначених для користувача даних в байтах, діленому на 1.2.

Це лише загальні рекомендації. Більш кращим є забезпечення високої якості друку символу, в порівнянні з компенсацією низької якості друку збільшенням рівня корекції помилок.

При високу ймовірність появи в символі *PDF417* пошкоджених або повністю стертих знаків символу, рівень корекції помилок може бути збільшений, в тому числі до рівня 8. Однак, в цьому випадку є ризик того, що в силу обмежень на загальна кількість кодових слів в символі *PDF417*, закодувати в одному символі всі призначені для користувача дані і послідовність кодових слів корекції помилок, що відповідає обраному рівню корекції, виявиться неможливим. В цьому випадку рекомендується використовувати передбачений специфікацією режим *Макро PDF417*, що представляє собою механізм поділу даних на блоки та подання їх у вигляді набору з декількох символів *PDF417*, або звернутися до інших двовимірним символіки, які дозволяють більш ефективно кодувати великі обсяги даних. Наприклад, символіка *Aztec* приблизно на 40% ефективніше *PDF417* кодує цифрові дані.

Штриховий код Micro PDF 417

Символіка штрихового коду *MicroPDF417* побудована на базі символіки *PDF417* і має з нею багато спільного. Основна відмінність полягає в більш компактному кодуванні даних. Специфікація символіки приведена в міжнародному стандарті ISO / IEC 24728: 2006.

Штрих-код *MicroPDF417* дозволяє закодувати в одному символі:

• до 150 байт інформації;

• до 250 літерних символів (включаючи символи табуляції, перекладу рядка і повернення каретки);

• до 366 цифр.

Крім того, є можливість розбити повідомлення на блоки, які розміщуються в різних символах *MicroPDF417,* але зчитуються єдиним сполученням. Для цього в стандарті передбачений механізм склейки штрих-кодів (Structured Append). Кількість штрих-кодів з яких складається повідомлення може досягати 99 999.

MicroPDF417 рекомендується застосовувати, як альтернативу *PDF417* при обмеженнях на розмір області друку штрих-коду. На рис. 9.1 представлені штрих-коди *PDF417* і *MicroPDF417*, що кодують одні й ті ж дані, крім того у символів тей розмір мінімального елемента (модуля). Видно, що площа, яку займає символом *MicroPDF417,* майже в 2 рази менше.

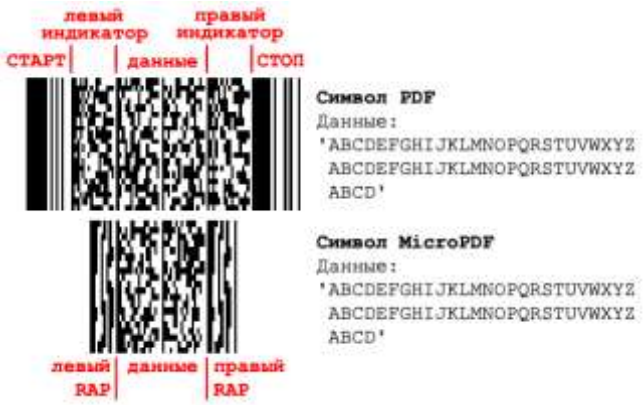


Рис. 9.1. Зіставлення розмірів штрих-кодів *PDF417* і *MicroPDF417*

Таке значне зменшення розмірів досягається за рахунок заміни стартових, степових і індикаторних стовпців *PDF417* на більш компактні стовпчики ідентифікаторів рядків *(Row Address Pattern, RAP) MicroPDF417.* Сусідні рядки в цих стовпцях відрізняються лише одним модулем, завдяки чому стовпці легко локалізувати в процесі зчитування штрих-коду. Кількість рядків символу *MicroPDF417* і рівень корекції помилок визначається за даними витягнутих з двох стовпців ідентифікаторів рядків. Рівень виправлення помилки фіксований для кожного розміру символу. Може бути виправлено до 64% пошкоджень. Виграш в компактності *MicroPDF417* досягається за рахунок зниження надійності зчитування при пошкодженнях зображення символу.

У порівнянні з *PDF417*, символіка *MicroPDF417* менш гнучка, і має наступні обмеження: максимальне число стовпців даних - 4, максимальне число рядків - 44. Стовпці даних *MicroPDF417* формуються аналогічно *PDF417*. У символах, що містять три чи чотири стовпці даних, є центральний стовпець ідентифікаторів рядків (рис.9.2).

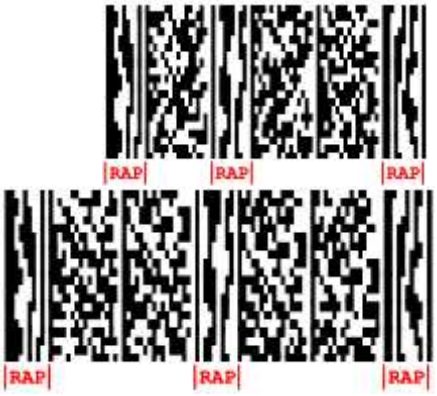


Рис. 9.2. Штрих-коди *MicroPDF417* з центральним стовпчиком ідентифікаторів рядків

PDF417 і *MicroPDF417* теоретично можливо вважати лазерним сканером, але на практиці дуже часто, через ігнорування рекомендацій до розмірів і друку символів штрих-коду, зробити це виходить тільки за допомогою image сканера. Рекомендацій стандарту потрібно дотримуватися, щоб забезпечити надійне зчитування штрих-кодів сканерами різних виробників.

Штриховий код Aztec Code

Aztec Code введений *Енді Лонакром (Andy Longacre)* з фірми *Welch Allyn Inc.* в 1995 році і відкритий для загального використання. *Aztec Code* розроблений для легкої друку і легкої розшифровки. Штрихкод являє собою квадратну матрицю з концентричними квадратами в центрі, які служать для визначення позиції коду щодо сканера і мірної лінійкою по краю коду.

Тип штрих-кодів *Aztec* є представником сімейства двомірних матричних штрих-кодів, і тому для нього справедливо все сказане вище. Зображення такого штрих-коду є квадратною монохромну матрицю, складену з темних і світлих модулів, в центрі якої знаходиться набір квадратних концентричних кілець.

Найменший штрихкод *Aztec* має площу 15x15 модулів, найбільший - 151x151. Мінімальний код *Aztec* кодує 13 цифр або 12 букв, а максимальний - 3832 цифри або 3067 букв або 1914 байт даних. Символіка не вимагає вільної зони навколо штрих-коду. Існують 32 градації розміру коду з можливістю вибіркової інсталяції захисту від помилок за методом *Ріда-Соломона (Reed-Solomon)* від 5% до 95% від області коду. Рекомендований рівень - 23% ємності коду плюс 3 кодових слова.

Кодуються всі 8-бітові значення. Величини 0 - 127 представляються у вигляді набору символів ASCII, значення 128-255 представляються як ISO 8859-1, Latin Alphabet No.1. Крім даних можна закодувати два службових символу: FNC1 для сумісності з деякими існуючими додатками і ECI (escape-послідовність) для стандартизованої кодування повідомлень.

Особливості *Aztec:*

- Розмір від 15x15 до 151x151 модулів;
- Чітка структура штрих-коду *Aztec* дозволяє відмовитися від вільної зони (чистої області навколо штрихового коду). Він може бути розташований впритул до тексту, іншим штрих-кодами і т.п .;
- Сканери VMC зчитують штрих-коди типу *Aztec* повернені під довільним кутом, в дзеркальному відображенні або інвертовані за кольором;
- Обсяг інформації, що кодується в одному штрих-коді: від 6 довільних байт (або 12 букв / 13 цифр) до 1914 довільних байт (або 3067 букв / 3832 цифр). Значення вказані для рекомендованого стандартом рівня корекції помилок;
- Система корекції помилок призначена для збереження цілісності даних при пошкодженні штрих-коду. Рівень виправлення помилки користувач може задавати

самостійно, виходячи з передбачуваних умов застосування штрихового коду. Зокрема, стандарт *Aztec* дозволяє створити штрих код, який буде зчитуватися при пошкодженні до 90% його площі (за умови збереження ключових елементів його структури);

- Структурне з'єднання дозволяє розподіляти інформацію на кілька штрих-кодів (до 26-ти), що може бути корисно при розміщенні штрих-кодів в умовах обмежень на місце розташування і розміри (наприклад, іноді зручніше розташувати поруч кілька невеликих штрих-кодів, ніж один великий). Також структурне з'єднання може використовуватися для кодування великих обсягів інформації, що не вміщується в одиночний штрих-код;

- Можливість кодувати довільні 8-ми бітові послідовності, наприклад, літери різних алфавітів і будь-які дані в призначеному для користувача форматі; Підтримка настроювальних символів, застосовуваних для настройки сканера за допомогою штрих-коду;

- Підтримка рун - невеликих (11x11 модулів) штрих-кодів, що містять один байт інформації;

- Підтримка функціонального коду 1 (FNC1);

- Формат *Aztec* відкритий для загального користування.

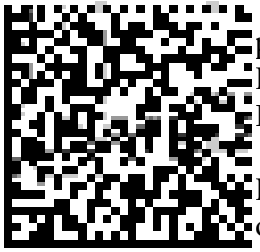
Впровадження штрих-кодів *Aztec*:

- Ряд транспортних компаній, що здійснюють авіа- та залізничні перевезення, розміщують штрих-код *Aztec* на своїх квитках і посадочних талонах. Існують і повністю безпаперові схеми, коли квитком є штрих-код, який пасажир отримує через Інтернет, і виводить на екран свого мобільного телефону;

- Польські реєстраційні документи на автомобіль містять штрих-код *Aztec*;

- Банківські документи ряду банків містять штрих-код *Aztec,* що містить всю інформацію документа. Таким чином, при необхідності введення даних в деяку автоматизовану систему, оператор може просто сканувати штрих-код, а не набирати все дані на клавіатурі [2].

Штриховий код Data Matrix



Data Matrix від фірми *CiMatrix* є двомірний код, розроблений для розміщення великого обсягу інформації на обмеженій площі поверхні. Був розроблений в 1991 році і описаний в міжнародному стандарті ISO / IEC 16022: 2006.

Штрихкод *Data Matrix* може зберігати від одного до 500 символів. Код може масштабуватися від 1-мм щільності до 14-дюймової площі. Це означає, що код *Data Matrix* має теоретичну максимальну щільність 500 мільйонів символів на дюйм. На практиці щільність, звичайно, обмежується роздільною здатністю друкуючих пристроїв і сканерів [3].

Дані, що кодуються розташовуються усередині прямокутного шаблона пошуку символіки, який являє собою L-подібний куточок і набір чергуються чорних і білих модулів по периметру символа. Алгоритми зчитування *Data Matrix* спочатку виявляють шаблон пошуку, а потім на підставі його здійснюють декодування. Невеликі пошкодження або примикання до шаблону пошуку елементів, що не відносяться до штрих-коду призводять до неможливості декодування *Data Matrix*.

Data Matrix, як і інші 2D штрих-коди, має надлишкову структуру, що дозволяє декодувати дані при частковому пошкодженні символу. Істотний вплив на розробку стандарту символіки *Data Matrix* надав попередній йому багатостроковий штрих-код *PDF*-417. Структура кодування даних дуже схожа з *PDF-417*. Ці дві символіки дозволяють більш ефективно кодувати невеликого розміру цифрові послідовності ніж літеро-цифрові. Нижче по тексту порівняння стандарту *Data Matrix* буде проводиться з стандартом *Aztec,* тому що Aztec є новішим і продуманим 2D штрих-кодом, розробленим з урахуванням успіхів і невдач всіх попередніх символік.

Найсуттєвішою перевагою *Data Matrix* в порівнянні з іншими 2D штрих-кодами, які широко використовуються, є той факт, що *Data Matrix* дозволяє на мінімально можливій площі закодувати невеликі послідовності даних. Для порівняння, якщо необхідно закодувати

6 цифр, то *Data Matrix* штрих-код вийде розміром всього 10х10 модулів, а *Aztec* - 15х15 модулів. Перевага *Data Matrix* втрачається при збільшенні обсягу кодируемой інформації до 72 цифр (розмір штрих-коду - 24х24 модуля). При розмірах символу 132х132 модуля в штрих-коді *Data Matrix* можливо розмістити 2608 цифр, в той час як в *Aztec* аналогічного розміру увійде майже 3000 цифр. На літеро-цифрових даних *Data Matrix* менш ефективний і вже на стрічках в 10 символів займає стільки ж площі скільки і *Aztec*. Виграш по площі при невеликих обсягах кодованих даних пояснюється тим, що в штрих-коді *Data Matrix* міститься дуже мало службової інформації, яка описує розміри і структуру даних штрихового коду, що негативно позначається на надійності зчитування *Data Matrix*. Програш *Data Matrix* при кодуванні великих обсягів даних пояснюється перш за все зростанням розміру шаблону пошуку символу, який збільшується прямо пропорційно периметру символу (у *Aztec* шаблон пошуку у великих штрих-кодів не змінюється).

Примітним є той факт, що стандарт *Data Matrix* допускає використання не тільки квадратних, а й прямокутних штрих-кодів, що в різних ситуаціях дозволяє більш ефективно використовувати доступну площу для розміщення символу. Стандарт *Aztec* для більш ефективного використання площі передбачає розбиття блоку даних на кілька символів штрих-коду з їх подальшою склеюванням. Стандарт *Data Matrix* так само дозволяє розбити блок даних між символами, а потім склеїти його після зчитування, але реалізація цієї склейки не настільки гнучка як в *Aztec* і, мабуть тому, практично не використовується.

Код має кілька інших цікавих особливостей. Оскільки інформація кодується абсолютною позицією елемента в середині коду, тобто позицією щодо меж коду, код не так чутливий до дефектів друку, як традиційний штрихкод. Схема кодування має високий рівень надмірності, дані роззосереджені в середині штрихкодового символу. Це дозволяє зберігати можливість прочитання коду при його частковому пошкодженні або втраті частини коду. Кожен код має вимірювальні лінійки, які виглядають як суцільна лінія по одному краю символу і рівномірно розташовані квадратні точки однакового розміру по іншому краю. Ці лінійки використовуються для визначення орієнтації і щільності коду.

Існують два основних набору символів. Вони використовують згорткове кодування для корекції помилок, яке використовувалося в перших версіях коду *Datamatrix*, ці версії описані як ECC-000 .. ECC-140. Другий набір описаний як ECC-200 і використовує метод корекції помилок за допомогою клда *Ріда-Соломона (Reed-Solomon*). Символи ECC-000 .. 140 завжди мають непарну кількість модулів по кожній стороні квадрата. Символи ECC-200 завжди містять парне число елементів з кожної зі сторін. Максимальна ємність символу ECC-200 становить 3116 цифр або 2335 букв в символі, що складається з 144 модулів.

Найбільш популярними застосуваннями для Datamatrix є маркування невеликих предметів, таких як електронні елементи і друковані плати електронних приладів. Ці додатки використовують здатність Datamatrix розмістити приблизно 50 символів в коді розміром 3 мм і той факт, що код може бути прочитаний при 20-відсоткової контрастності друку.

Код читається ПЗС-камерою або ПЗС-сканером. Символи площею від 1/8 дюйма до 7 дюйма може бути прочитаний з відстані від контакту до 36 діймов. Звичайна швидкість читання складає 5 кодів в секунду.

Отже, основна перевага використання кодування *Data Matrix* - компактність при кодуванні невеликих обсягів інформації (до 10 символів). Ця перевага пояснює популярність символіки в таких сферах застосування як [3]:

- медична промисловість;
- поштові перевезення;
- електронна промисловість;
- автомобілебудування;
- харчова промисловість;
- авіакосмічна та оборонна промисловість;
- енергетичне машинобудування.

Штриховий код QR Code

При розробці двомірного матричного штрих-коду фірми *Denso* особливу увагу було

приділено швидкості зчитування / декодування. Представники компанії стверджують, що їм вдалося досягти на порядок вищого швидкодії - 30 етикеток в секунду (кожна ємністю 100 символів) проти максимум 3 етикеток в секунду (такий же ємності) в кодуванні *Data Matrix* або *PDF417*. Секрет полягає в застосуванні комбінованого методу: зчитування відбувається відразу в усіх напрямках, а прискорити процедуру декодування допомагають спеціальні детектори положення (вкладені квадрати, розташовані в трьох кутах етикетки). Завдяки цим піктограмам сканер легко і швидко розбирається як в розмірі коду, так і в орієнтації етикетки на площині [3].

Специфікація *QR Code* знаходиться в стані розвитку, але судити про основні характеристики коду можна, наприклад, за варіантом *QR Code Model 2*. Цей варіант припускає наступну максимальну ємність коду (в залежності від типу даних): 7089 цифр, 4296 букв і цифр, 2953 двійкових символів (8-бітних) або 1817 символів японської мови в кодуванні *Kanji-Kana*. Допускається кодування суміші даних різних типів. Дані в *QR Code* представляються сукупністю чорних і білих точок, кожна з яких трактується як одиниця даних, або модуль. Розмір коду варіюється від 21x21 до 177x177 модулів (крок збільшення кратний 4). Неважко оцінити, яка площа потрібна для етикетки тієї чи іншої ємності. Наприклад, якщо застосовується код 105x105 модулів, а розмір кожного модуля дорівнює 0,25 кв. мм, то площа області коду складе 105x0,25 кв. мм = 26,25 кв. мм. Сюди треба додати необхідні поля (шириною не менше чотирьох модулів). У підсумку отримуємо, що необхідна площа етикетки складе (105 + 8) x0,25 кв. мм = 28,25 кв. мм [2].

Основна перевага *QR-коду* - це легке розпізнавання скануючим обладнанням, що дає можливість використання в торгівлі, виробництві, логістиці.

Існує чотири основних кодування *QR-кодів*:

• Цифрова: 10 біт на три цифри, до 7089 цифр.

• Алфавітно-цифрова: підтримуються 10 цифр, літери від A до Z і кілька спецсимволов. 11 біт на два символу, до 4296 символів

• байтовими: дані в будь-якої зручної кодуванні (за замовчуванням ISO 8859-1), до 2953 байт.

• Кандзі: 13 біт на ієрогліф, до 1817 ієрогліфів.

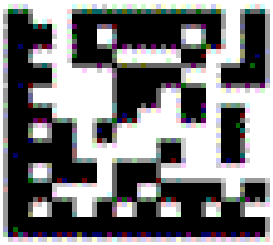
Microsoft Tag

У 2009 році компанія «Microsoft» ввела новий формат «*Microsoft Tag*», заснований на власній розробці - *High Capacity Color Barcode (HCCB)*. Штрих-коди цього формату відносяться до двовимірним, а сам формат вводився для бурхливого розвитку ринку мобільного маркування - для ідентифікації інформації зберігається на серверах компанії за допомогою фотокамер мобільних пристроїв [4]. Проблема «*Microsoft Tag*» в тому, що для їх зчитування потрібне особливе ПО, яке, втім, поки знаходиться у вільному доступі. З одних джерел випливає, що при декодуванні «Microsoft Tag» виникають труднощі сприйняття цього формату камерами мобільних пристроїв чи сканерами штрих-кодів, а також з'являються помилки зчитування - якість зображення цього штрих-коду має бути майже ідеальним і без спотворень, а пристрій декодування розташовуватися майже строго навпаки. Інші ж кажуть, що цей формат більш стійкий до виникнення проблем сканування при деякому пошкодженні, в порівнянні, наприклад, з *QR-кодом*. На відміну від тривимірного штрих-коду «*Color C Code*», кольорові «*Microsoft Tag*» не можуть зберігати багато інформації і здебільшого призначені для виведення її на мобільні пристрої з мережі інтернет.

ColorCode

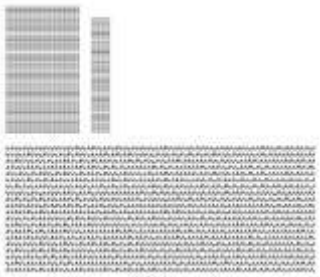
Розроблений вченими Університету *Yonsei (Корея), ColorCode* ™ являє собою фірмову двовимірну штрих-кодову систему, призначену для зберігання URL, яка може зчитуватися камерою мобільного телефону. З його допомогою камера визначає індексовані коди, які в свою чергу пов'язані з відповідною інформацією. Матриця, що складається з окремих блоків і аналогових даних, що стосуються числа квітів, оцифровується, а потім обробляється виділеним сервером з використанням зареєстрованих адрес цих кодів [5].

CPCode



CPCode - фірмовий код, розроблений *CP Tron, Inc*. Він складається з квадратних матричних символів з L-образної периферійної мішенню і прилеглих настановних міток. Візуально цей код нагадує *Data Matrix Code* [5].

DataGlyphs



DataGlyph - оригінальний код, розроблений *Xerox PARC*. Цей код складається з комбінації маленьких «/» і «/» на сірому тлі, що кодують двійкову інформацію, включаючи синхрогрупи і корекцію помилок. Кожен знак може мати в довжину 1/100 дюйма (0.25мм). Даний код забезпечує щільність 1000 байтів з 8 бітів на 1 квадратний дюйм. *DataGlyph* допускає наявність чорнильних міток, низька якість зображення і навіть наявність скріпок на символі, завдяки внутрішній програмі корекції помилок і випадкових елементів [6].

DataGlyphs розроблений таким чином, що він має здатність зливатися з дизайном продукції, на якому він надрукований. *DataGlyphs* може бути логотипом або фоном для тексту або зображення. Області застосування - опитувальні листи, бланки для відповіді при прямій розсилці і візитні картки. Символи можуть зчитуватися за допомогою програм сканування зображення. Це дає дивовижні можливості, яких не було в жодній з колишніх систем кодування. Наприклад, користуючись варіацією в товщині сусідніх гліфів та в їх кольорі, гліфами можна надрукувати чорно-біле або кольорове зображення, структура якого буде непомітна на око (як ми не бачимо точки різного діаметру при друку фотографій в газеті).

Datastrip Code

Datastrip Code спочатку називався *Softstrip* і був розроблений *Softstrip Systems*. Ця найраніша з двох двовимірних символік. Даний оригінальний код в даний час належить *Datastrip Inc.* Це запатентована система кодування і сканування, що дозволяє друкувати інформацію, зображення і навіть оцифрований звук на простому папері і дуже стислому форматі і безпомилково зчитувати їх за допомогою комп'ютера.

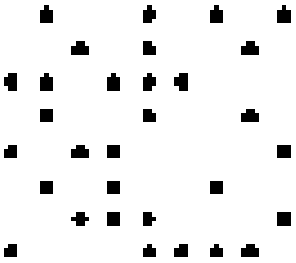
Основні компоненти *Datastrip* - надруковані графічні зображення (the *Datastrip*) і оптико-електронні зчитувальні пристрої. Код *Datastrip* є матричне зображення, що складається з дуже маленьких прямокутних чорних і білих областей (DiBits). Маркери з одного боку і по верхній смузі (покажчик початку рядка, шаховий шаблон і рамка) містять установчу інформацію для пристроїв, призначених для зчитування *Datastrip Code*, і

забезпечують неспотвореному даних. Інформація в заголовку містить подробиці про дані, що зберігаються в смузі: назва файлу, число байтів, щільність шару даних і т.д. Метод кодування *Datastrip,* що включає біти контролю парності в кожну кодованих рядок, забезпечує дуже високу надійність і можливість корекції помилок [7].

Смуги інформації зазвичай мають 5/8 дюймів в ширину і 9 дюймів в довжину. Щільність даних варіюється від 150 до 1 000 байтів на 1 квадратний дюйм в залежності від технології друку, що використовується при їх виробництві. *Datastrip Code* може успішно проводиться за допомогою більшості матричних лазерних принтерів (включаючи високошвидкісні лазерні принтери), а також струменевих або термографических друкованих пристроїв. Datastrip Code може відтворюватися на більшій частині видів паперу (включаючи газетний папір) і пластмасі, з використанням звичайних технологій друку - від офісних фотокопіювальних пристроїв (для смуг з меншою щільністю) до швидкісних рольових друкарських машин. Смугу з низькою щільністю (до 1 100 байта на 1 9-дюймову смугу) можуть виготовлятися на матричних принтерах. Смуги, що містять до 3 500 байтів, можуть виготовлятися за допомогою лазерних принтерів. Смуги з дуже високою щільністю (до 4 800 байтів) вимагають більш складних технологій виготовлення з використанням фотографічних технологій.

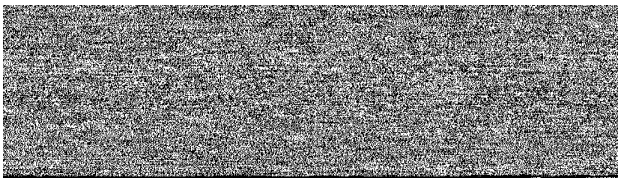
Datastrip Code може зчитуватися спеціальними пристроями, що виробляються *Datastrip, Inc.*, при цьому пристрій, що зчитує повинно знаходитися в контакті з кодом. Спочатку даний код просували як технологію, що дозволяє зчитувати програмне забезпечення, надруковане в книгах і журналах. В даний час цей код в основному використовується для друкування інформації на різних посвідченнях [5].

Dot Code A



Dot Code A (також відомий як *Philips Dot Code*) є одним з нечисленних точкових кодів. Ця символіка розроблялась для ідентифікації об'єктів на відносно малій площі, або ж для прямої маркування за допомогою технологій маркування, що відрізняються низькою точністю. Символ складається з певної послідовності точок - від 6 x 6 до 12 x 12, остання з яких дозволяє визначати більше 42 мільярдів окремих предметів. Області застосування - ідентифікація лабораторного скляного посуду та маркування білизни в пральні [5].

INTACTA.CODE



INTACTA.CODE ™ являє собою фірмовий код, розроблений *INTACTA Technologies, Inc.* Він може обробляти будь-яку двійкову інформацію, наприклад, виконуючі файли, відео, текстову інформацію, аудіофайли (або поєднання файлів) із застосуванням *INTACTA.CODE* ™ для стиснення, кодування і корекції помилок з метою створення оболонки, що дозволяє безпечно дістрібутувати дані, в той же час підтримуючи збереження формату і змісту.

9.3.Тривимірний штриховий код (рельєфний штриховой код (BumpyBarcode))

Тривимірний штриховий код - це насправді будь-який лінійний (одновимірний) код (наприклад, *Code 39* або *Code 128*), тиснення на поверхні. Цей код зчитується з урахуванням відмінностей висоти, а не контрасту, з метою розрізнення штрихів і проміжків між ними, за допомогою спеціального пристрою, що зчитує.

Такий штрих-код може використовуватися, коли віддруковані етикетки неможливо наклеїти на поверхню або коли вони можуть бути пошкоджені в агресивному або руйнівному середовищі. На них може бути нанесена фарба або покриття і, тим не менше, їх легко можна зчитати. Вони можуть бути постійної особливістю предмета, що виключає неправильне маркування [5].*Таблиця 9.2. Порівняння найбільш популярних двовимірних штрихових кодів* [8]

Характеристика	**PDF417**	**DataMatrix**	**QR-код**	**Aztec Code**
Оптимізація для існуючих технологій друку	Прямокутна матриця	Зображення будується з стандартних квадратних пікселів	Зображення будується з стандартних квадратних пікселів	Зображення будується з стандартних квадратних пікселів
Нанесення на різні матеріали	Достатньо контрастного двукольорового зображення	Достатньо контрастного двукольорового зображення	Достатньо контрастного двукольорового зображення	Достатньо контрастного двукольорового зображення
Максимальний обсяг даних (при максимальному рівні корекції помилок)	2–3 Кбайт	2-3 Кбайт	2-3 Кбайт	2 кбайта
Максимальний розмір	151x151 пікселі	144x144 пікселі	177x177 пікселі	151x151 пікселі
Коди корекції помиок	9 рівнів корекції помилок Виправляється до 64% пошкоджень	Виправляється до 30% пошкоджень	Виправляється до 30% пошкоджень (фіксовані рівні в 7, 15, 25 и 30%)	Виправляється до 95% пошкоджень (рівень від 5% до 95%, стандартно 23%)
Стійкість просторового распізнавання кода	Поворот на довільний кут	Поворот на довільний кут	Поворот на довільний кут, дзеркальне відображення	Поворот на довільний кут, дзеркальне відображення
Відкритість формата	Формат відкритий	Формат відкритий	Формат відкритий	Формат відкритий, хоча й захищений патентами переданий для вільного використання
Використання	Широке використання в документообертi, сфері транспорту, телекомунікацій	Широке використання, в тому числі в промисловості	Реклама та розваги, логотипи, що вміщують інформацію про фірму, визітівки, туризм, електронні квитки, маркування продуктів	Використовується в онлайнових квитках, багатьох авіа-та з/н компаній, а також в регістраційних документах
Створення кодів	безкоштовно	безкоштовно	безкоштовно	безкоштовно
Считування коду автономно	так	так	так	так

Контрольні питання до розділу

1. Особливості лінійних (одновимірних) штрихових кодів.
2. Особливості двовимірних штрихових кодів.
3. Особливості трьохвимірних штрихових кодів.
4. Особливості чотирьохвимірних штрихових кодів.
5. Наведіть основні критерії штрихових кодів.
6. Код PDF 417. Особливості побудови. Рівні коректування помилок.
7. Код micro PDF 417. Особливості побудови. Порівняння з кодом PDF 417.
8. Aztec Code. Особливості побудови та застосування.
9. Код Data Matrix. Особливості побудови та застосування.
10. QR Code. Особливості побудови та застосування.
11. Microsoft Tag. Особливості побудови та застосування.
12. ColorCode. Особливості побудови та застосування.
13. CPCode. Особливості побудови та застосування.
14. DataGlyphs. Особливості побудови та застосування.
15. Datastrip Code. Особливості побудови та застосування.
16. Dot Code A. Особливості побудови та застосування.
17. INTACTA.CODE. Особливості побудови та застосування.
18. Тривимірний штриховий код (рельєфний штриховой код (BumpyBarcode)). Особливості побудови та застосування.

Список рекомендованої літератури

1. Жураковський Б.Ю. Сфери застосування двовимірних штрихових кодів / Жураковський Б.Ю., Довженко Н.М. // Системи управління, навігації та зв'язку № 2(38), 2016. – С.83-87.

2. Жураковський Б.Ю. Особливості застосування QR-кодування в телекмунікаційній мережі України / Жураковський Б.Ю., Довженко Н.М. // Науково-технічна конференція «Актуальні проблеми розвитку науки і техніки», ДУТ, м. Київ. – 22.10.2015. с. 18-21.

3. QR-код та Data Matrix [електронний ресурс]. – режим доступу до матеріалів статті: https://mybiblioteka.su/tom2/3-80575.html

4. Виды и типы штрихкодов [електронний ресурс]. – режим доступу до матеріалів статті: https://kkm74.ru/articles/vidy_i_tipy_shtrih_kodov/.

5. Жураковський Б.Ю. Порівняльний аналіз формування та застосування двомірних штрих-кодів для передачі даних / Жураковський Б.Ю., Довженко Н.М. // Системи управління, навігації та зв'язку № 2(34), 2015. – С.68-70.

6. Астафьева Е. История появления и развития популярных 2D штрихкодов [електронний ресурс]. – режим доступу до матеріалів статті: https://idexpert.ru/reviews/13658/

7. Жураковський Б.Ю. Використання методів адаптивного кодування для каналів з параметрами, що змінюються / Жураковський Б.Ю. // Вісник ДУІКТ № 5(2), 2007. – С.199-202.

8. Жураковский Б. Ю. Багатовимірні штрихові коди. / Б. Ю. Жураковский, В. А. Дружинін. // Адаптивні системи автоматичного управління. – 2018. – №2. – С. 15–31. DOI: https://doi.org/10.20535/1560-8956.33.2018.164669

РОЗДІЛ 10. ПРОТОКОЛИ ІНТЕРНЕТ РЕЧЕЙ

10.1. Протоколи інфраструктури

Обсяг інформації, що формується одним сенсорним вузлом, порівняно невеликий, однак більшість сервісів Інтернету речей побудовано на принципі обробки інформації від безлічі вузлів, що принципово відрізняється від архітектур, прийнятих в класичних мережах, типу абонент - вузол зв'язку для телефонії, клієнт - сервер для передачі даних [1].

Таким чином, ми стикаємося з новою архітектурою: багато джерел - багато одержувачів, крім того, обсяг трафіку від сенсорного вузла може бути як дуже маленьким, так і дуже великим. Звичні прикладні протоколи для передачі повідомлень не розраховані на таке використання.

Рис. 10.1. Протоколи архітектури IoT

Протокол маршрутизації RPL

RPL означає протокол маршрутизації для мереж низької потужності та трат. Це протокол IPv6. Мережі з низьким рівнем втрат потужності включають в себе безпроводові локальні мережі (WPAN), мережі низьковольтних лінійних зв'язків (PLC) та мережі безпроводових датчиків (WSN).

Рис. 10.2. Категорії протоколів IoT

Ці мережі мають деякі характеристики:

- Можливість оптимізувати та заощадити енергію
- Можливість підтримувати схеми трафіку, відмінних від одноадресного спілкування
- Можливість запускати протоколи маршрутизації через шари каналів з обмеженими розмірами кадрів

RPL був розроблений, щоб підтримувати мінімальні потреби в маршрутизації шляхом створення високоточної топології над мережами з втратами. Цей протокол надає підтримку різноманітних типів моделей трафіку: багатоточкове, точка-багатоточка та точка-точка. Пристрої в мережі, що використовують цей протокол, підключаються один до одного таким чином, щоб у цьому з'єднання не було циклів. Для досягнення цього спочатку споруджується вузол, який називається цільовим орієнтованим ациклічним графіком *(destination oriented directed acyclic graph, DODAG)*, який перенаправляється на одне призначення. Специфікації *RPL* звертаються до *DODAG* як до основи *DODAG*. Кожний вузол, який входить до складу *DODAG*, знає свій головний вузол, але не має інформації про його дочірні вузли. *RPL* підтримує щонайменше один шлях від кожного вузла до кореневого і до бажаного батьківського [2].

Це зроблено для підвищення продуктивності пошуку швидшого шляху.

Топологія *DODAG*, що використовується в *RPL*, зображена на рис. 10.3.:

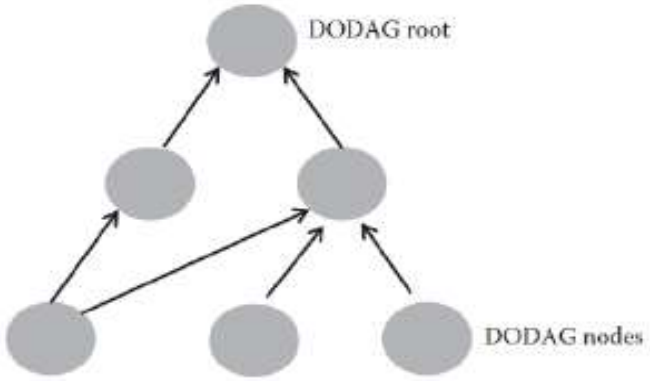


Рис. 10.3. Протоколи інфраструктури

Маршрутизатори *RPL* працюють в одному з двох режимів роботи (MOP): режим не зберігання або зберігання.

У режимі не зберігання повідомлення маршруту *RPL* рухаються у бік нижчих рівнів на основі маршрутизації джерела IP, тоді як у режимі зберігання маршрутизація вниз здійснюється на основі адресі призначення IPv6.

IEEE 802.15.4

Цей протокол був створений для того, щоб вказати підрівні для MAC та фізичного рівня, насамперед, для низькошвидкісних бездротових приватних мереж. Враховуючи різноманітні переваги, пропоновані цим протоколом, такі як низьке енергоспоживання, низька швидкість передачі даних, а також низька вартість та висока пропускна здатність повідомлень, вона дуже підходить для використання в системах IoT як протокол зв'язку. Цей протокол також забезпечує надійне з'єднання і може обробляти величезну кількість вузлів (приблизно близько 65K вузлів). Ідеально підходить для забезпечення зв'язку, оскільки забезпечує високий рівень безпеки, шифрування та служби автентифікації. Єдиною негативною стороною цього протоколу є те, що вона не забезпечує жодної з QoS(*quality of service*) гарантій.

Рис. 10.4. Архітектура IEEE 802.15.4

Цей протокол ґрунтується на *ZigBee* та інших протоколах, що використовуються в IoT-комунікації. IEEE 802.15.4 підтримує передачу у трьох частотних діапазонах, використовуючи метод *DSSS(direct sequence spread spectrum).*

На основі частотного каналу, передача даних відбувається в три рази швидкість передачі даних:

- 250 kbps at 2.4 GHz;
- 40 kbps at 915 MHz;
- 20 kbps at 868 MHz.

Цей протокол підтримує два типи вузлів мережі:

- Повнофункціональні пристрої (FFD);
- Знижено функціональні пристрої (RFD).

FFD можуть працювати як координатор персональної зони (PAN) або просто як звичайний вузол. Координатор має можливість створювати, керувати та підтримувати мережу. *FFDs* можуть зберігати таблицю маршрутизації у своїй пам'яті і можуть забезпечити *MAC*. Вони також можуть спілкуватися з іншими пристроями, використовуючи одну з наступних топологій:

- зірка;
- однорангова;
- кластерне дерево.

RFD - це дуже прості вузли, і вони мають обмежені ресурси. Вони можуть спілкуватися тільки з вузлом координатора, використовуючи тільки топологію зірки.

Топологія зірок: містить принаймні один FFD та кілька інших RFD. FFD, призначений для роботи в якості координатора PAN, повинен бути розташований у центрі мережі. Цей FFD несе відповідальність за управління та контроль усіх інших вузлів, які є частиною мережі (рис.).

Топологія однорангової мережі: вона містить координатора PAN, а інші вузли зв'язуються між собою в тій самій мережі або через проміжні вузли до інших мереж.

Топологія кластерного дерева: це особливий тип одноранговох топології. Він складається з координатора PAN, кластерної голови та нормальних вузлів.

IPv6 over Low-Power Wireless Personal Area Networks(6LoWPAN)

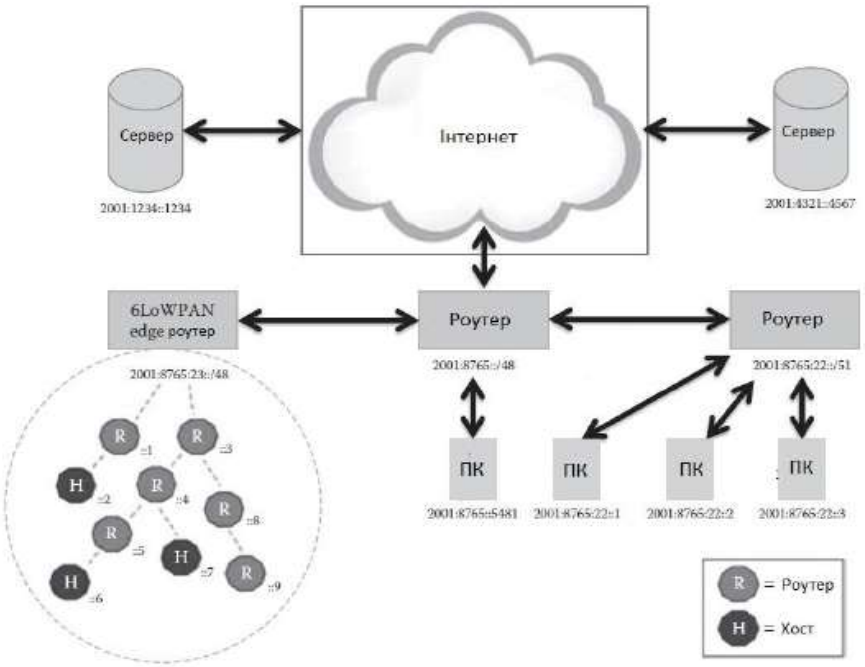


Рис. 10.5. Архітектура 6LoWPAN

Вихідна лінія до Інтернету забезпечується точкою доступу (*AP, access point*), яка в цьому випадку є маршрутизатором IPv6. Різні типи пристроїв, таких як ПК та сервери, можуть бути підключені до AP. Компоненти мережі 6LoWPAN підключаються до мережі IPv6 за допомогою маршрутизатора 6LoWPAN. Нижче наведено функції, які виконує «edge» маршрутизатор:

- Це дозволяє обмінюватися даними між пристроями 6LoWPAN та Інтернетом (або іншою IPv6 мережею).
- Це дозволяє обмінюватися даними між пристроями, що входять до мережі 6LoWPAN.
- Це допомагає генерувати та підтримувати мережу 6LoWPAN.

Оскільки мережі 6LoWPAN можуть спілкуватися з IP-мережами, вони підключаються до IP-мереж просто за допомогою IP-маршрутизаторів.

«Edge» маршрутизатори, які використовуються для підключення мереж 6LoWPAN до інших IP-мереж, передають IP-датаграми між різними носіями, що використовуються в IP-мережах. Медіа, що використовується в мережі IP, може бути Ethernet, Wi-Fi, 3G або 4G. Оскільки «edge» маршрутизатори, що використовуються в мережевих датаграмах мережі 6LoWPAN для інших IP- мереж із використанням мережевого рівня, вони не підтримують стан прикладного рівня. Це, в свою чергу, знижує робоче навантаження на «edge» маршрутизаторі з точки зору потужності обробки, що дозволяє використовувати дешеві вбудовані пристрої з простим програмним забезпеченням [1].

Bluetooth Low Energy

Bluetooth Low Energy (BLE) спочатку працював як частина базової специфікації Bluetooth 4.0.

BLE використовує радіоприймач малої дальності з мінімальною потужністю і працює довгий час. Його діапазон охоплення становить близько 100 метрів, що приблизно в 10 разів перевищує звичайний Bluetooth.

Затримка BLE в 15 разів менша за звичайну Bluetooth. BLE працює, використовуючи потужність від 0,01 мВт до 10 мВт. Ці характеристики роблять BLE ідеальним протоколом для використання пристроями IoT.

EPCglobal

RFID (радіочастотна ідентифікація) пристрої - безпроводові мікрочіпи, які використовуються для позначення об'єктів для автоматичної ідентифікації.

Електронний код продукту (EPC) - це унікальний ідентифікатор, що зберігається в тезі RFID, що допомагає ідентифікувати та відслідковувати елементи в сценарії керування ланцюжком постачання. *EPCglobal* – це організація, що розробила EPC, а *EPCglobal* також готує та підтримує стандарти, пов'язані з *RFID* та *EPC*. *RFID* може бути використана як ключова технологія для пристроїв IoT з наступних причин:

- Відкритість;
- Масштабованість;
- Надійність;
- Підтримка ідентифікаторів об'єктів та відкриття сервісів.

Тег RFID має дві основні компоненти: електронний мікросхеми для зберігання ідентичності об'єкта та антени, що дозволяє чіпу спілкуватися з системою читання тегів. Зв'язок між тегом і читачем тегів відбувається за допомогою радіохвиль. Два основних компоненти системи RFID:

- радіоприймач;
- читач тегів.

Z-Wave

Z-Wave - *це протокол бездротового зв'язку з малою потужністю, який використовується переважно для домашніх мереж (HAN, home area networks).*

Він має широке застосування в розробці програм дистанційного керування для розумних будинків, а також інших невеликих комерційних областей. Z-Wave була розроблена компанією ZenSys, а пізніше вдосконалена альянсом Z-Wave.

Z-Wave працює переважно в частотному діапазоні біля ГГц, що зазвичай становить близько 900 МГц [3].

Цей протокол використовує топологію мережевої сітки з малою потужністю. Кожен вузол або пристрій, що входить до складу мережі, має можливість надсилати та отримувати команди керування через стіни та поверхи будинку, і вони використовують проміжні вузли для маршрутизації даних навколо перешкод, які можуть бути присутніми в будинку. Складається мережа з контролерів та підпорядкованих пристроїв.

ZigBee

Протокол ***ZigBee*** був обрамлений альянсом ZigBee. Наступні особливості *ZigBee* роблять його дуже придатним для застосування IoT:

- Низьке енергоспоживання
- низька вартість
- Підтримка великої кількості вузлів мережі (<= 65K вузлів)

Крім особливостей, перерахованих вище, *ZigBee* має децентралізовану топологію мережі, яка дуже подібна до Інтернету. Цей протокол має можливість, яка дозволяє вузлам знаходити нові маршрути, якщо один маршрут не працює в мережі. Ця функція робить його дуже надійним бездротовим протоколом .

Специфікація *ZigBee* використовує нижні шари стека протоколу IEEE 802.15.4 і визначає власні верхні шари від мережі до програми.

10.2. Протоколи виявлення сервісів

Multicast Domain Name System (mDNS)

mDNS - це служба, яка може працювати як унікальний DNS-сервер. Цей підхід дуже гнучкий через те, що простір імен DNS можна використовувати локально без будь-якої додаткової конфігурації [2]. mDNS - це вигідний вибір для вбудованих пристроїв на базі Інтернету з наступних причин:

- Для керування пристроями не потрібна ручна настройка або адміністрування.
- Можна запустити без будь-якої додаткової інфраструктури.
- Високий рівень відмовостійкості через здатність функціонувати, навіть якщо відбудеться несправність інфраструктури.

DNS Service Discovery

Цей протокол допомагає клієнтам знаходити набір необхідних послуг, які присутні в мережі за допомогою стандартних *DNS*-повідомлень. Цей протокол також допомагає підключати пристрої без зовнішнього адміністрування або конфігурації. Виявлення служби *DNS (DNS-SD)* зазвичай використовує *mDNS* для надсилання пакетів *DNS* до певних адрес мультимовлення за допомогою *UDP*. Робота сервісу - це двоетапний процес:

1. Пошук назв вузлів необхідних служб.
2. Об'єднання IP-адреси з іменами хостів, використовуючи *mDNS.*

Universal Plug and Play (UPnP) - це набір мережевих протоколів, який був розроблений форумом *UPnP*. Основні особливості *UPnP*, що робить його придатним для сервісного виявлення пристроїв *IoT*, є наступні:

- Можливість підключення пристрою *UPnP* до мережі динамічно (автоматично) та отримання IP-адрес інших пристроїв і одночасно передавати свої можливості на інші пристрої.
- Конфігурація та адміністрування з нуля [6].

10.3. Протоколи рівня додатків

Представлена топологія на рис. 10.6 відповідає шаблоном проектування передачі повідомлень, який має назву "видавець-підписник“ (*Publisher-Subscriber, або pub/sub*). У такій схемі вводиться поняття видавця – джерела інформації та передплатника – одержувача інформації. Термін підписка пов'язаний з певною операцією, виконаною учасниками, з метою отримання інформації передплатником від конкретного видавця, а також упорядкування збору інформації – параметрів періодичності отримання та аналогічних (в залежності від реалізації) показників.

В даному випадку розглядається ситуація, коли сенсорний вузол (Node) об'єднує інформацію від багатьох датчиків (наприклад, дані вологості повітря) і направляє її згідно з параметрами передплати або за запитом, або самостійно через певний інтервал часу. Зазвичай самі датчики досить примітивні, їх завдання зводяться до постійної передачі інформації про контрольовані параметри. Тому з'являється необхідність об'єднувати датчики в вузли, оснащені мікроконтролерами, які будуть відповідати за зчитування вимірюваних даних і відправку їх за заздалегідь визначеними алгоритмами далі на сервер. Також найчастіше для взаємодії клієнта з системою необхідна ще клієнтська програма (Application), встановлена на персональному пристрої, яка необхідна для наочного представлення одержуваної від датчиків, або вже обробленої сервером інформації та управління системою. Така топологія також розрахована на включення брокера (Broker) [1].

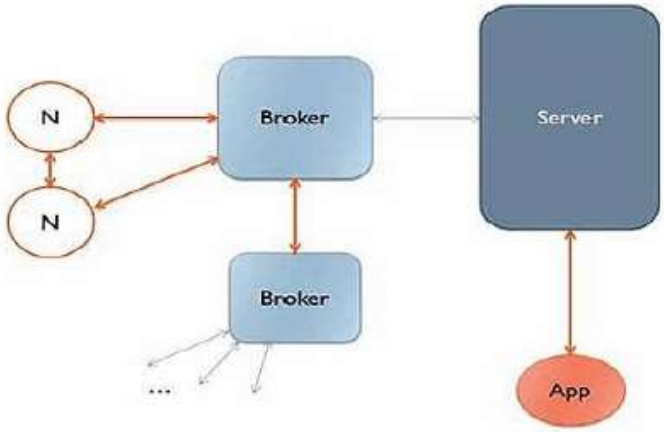


Рис. 10.6. Базова топологія, яка використовується для передачі повідомлень в IoT

Брокер – це сервер, який приймає інформацію від видавців і передає її відповідним передплатникам, в складних системах може виконувати, також різні операції, пов'язані з аналізом та обробкою даних, що надійшли на сервер. Брокер може встановлювати пріоритети сполученням і формувати черги для передачі повідомлень. Таким чином брокер організовує пересилання повідомлень, їх зберігання та фільтрацію. Під чергою повідомлень розуміється контейнер, або блок, в якому зберігаються повідомлення в процесі їх пересилання. При недостатньому ресурсі каналу зв'язку, або якщо одержувач недоступний під час того, як надсилається повідомлення, черга зберігає повідомлення до тих пір, поки воно не буде доправлено до відправника.

Протокол DDS

DDS (Data Distribution Service) - протокол прикладного рівня M2M для систем реального часу. Базується на моделі "видавець-передплатник".

Основна функція протоколу полягає в тому, щоб здійснити з’єднання пристроїв з іншими пристроями за допомогою шини обміну повідомленнями (див. рис.10.7). Протокол *DDS* може ефективно та синхронно доставляти мільйони повідомлень в секунду. Пристрої дають запит на дані інакше, ніж в IT мережах [5].

По-перше, пристрої працюють швидко. Масштаб реального часу часто вимірюється в долях мікросекунд. Пристроям потрібно здійснювати зв'язок з іншими пристроями, використовуючи складні шляхи, тому прості і надійні двоточкові TCP потоки даних обмежують можливості для такої передачі.

Натомість *DDS* забезпечує деталізований контроль якості обслуговування (QoS), багатоадресну передачу, переналаштовану надійність і всеосяжну надмірність. Крім того, сильною стороною *DDS* є розгалуження даних.

Протокол *DDS* забезпечує потужні способи фільтрації та відбору даних за адресами призначення, причому число синхронних одержувачів даних може обчислюватися тисячами. Деякі пристрої досить компактні, тому існують полегшені версії протоколу DDS, які працюють в умовах обмеженого обсягу.

Для використання даних від пристроїв зіркоподібна мережа зовсім не годиться. Замість цього *DDS* реалізує пряму шинний зв'язок між пристроями на базі реляційної моделі даних. ЇЇ називають шиною даних (DataBus), оскільки це мережевий аналог бази даних (database).

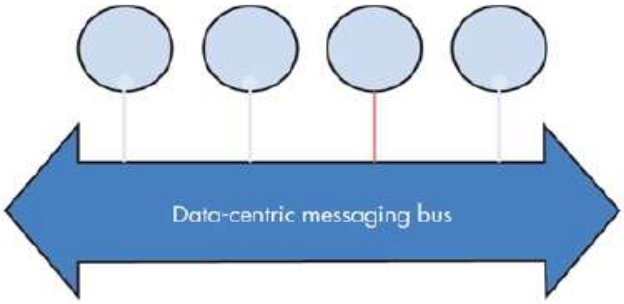


Рис.10.7. Принцип з’єднання пристроїв за допомогою протоколу DDS в IoT

Високопродуктивні системи інтегрованих пристроїв використовують протокол *DDS*. Це єдина технологія, яка забезпечує гнучкість, надійність та швидкість, необхідні для побудови складних додатків реального часу. Ці додатки містять в собі військові системи, вітроелектростанції, інтегровані системи лікарень, системи діагностичної візуалізації, системи супроводження ресурсів і автомобільні системи випробувань і забезпечення безпеки.

Протокол XMPP

XMPP (eXtensible Messaging and Presence Protocol) - відкритий, заснований на XML, вільний для використання протокол для миттєвого обміну повідомленнями та інформацією про присутність в режимі, близькому до режиму реального часу [6].

Спочатку спроектований легко розширюваним, протокол, крім передачі текстових повідомлень, підтримує передачу голосу, відео та файлів через мережу.

В протоколі *XMPP* використовується текстовий формат XML в якості вбудованого типу, забезпечуючи природний зв'язок між людьми. Протокол працює по TCP, або за допомогою HTTP поверх TCP. Його перевагою є метод адресування за допомогою ідентифікаторів *Jabber ID*, який містить в собі наступні, такі компоненти як вузол, домен та ресурс, причому два останні компоненти не є обов’язковими.

Адреса має такий вид *username@gmail.com*, який допомагає з'єднувати користувачів у величезному просторі Інтернету. *XMPP* підтримує різні комунікаційні моделі (запит-відповідь, публікація, підписка та інші)[6].

XMPP забезпечує простий спосіб адресуванні пристроїв. Це особливо зручно, коли дані передаються між віддаленими, найчастіше незалежними точками, як у випадку зв'язку між двома абонентами. Цей протокол не володіє високою швидкістю. Фактично, в більшості реалізацій цього протоколу використовується метод опитування або перевірки доповнень тільки на вимогу.

Сильними сторонами цього протоколу також є безпека, масштабованість, тому він ідеально підходить для невеликих мереж Інтернету речей.

Протокол CoAP

CoAP (Constrained Application Protocol) - це спеціалізований протокол передачі, розроблений робочою групою IETF-CORE, створений для мереж і пристроїв з обмеженими ресурсами, M2M додатків [2]. *CoAP* можна розглядати як доповнення до HTTP, але на відміну від HTTP *CoAP* націлений на використ*ання в пристроях з певними обмеженнями. CoAP використовує транспортний протокол* UDP.

Повідомлень, використовуваних протоколом *CoAP,* не так багато, більшість з них це запити відповіді: GET(отримати інформацію з приводу ресурсу), PUT(задати нове завдання над ресурсом), POST(зміна дій над ресурсом), DELETE(видалити активні можливості ресурсу), CONNECT(з’єднання). Клієнти (додатка користувача) використовують повідомлення для управління і спостереження за ресурсом. За запитом встановлюється

прапор спостереження, і сервер продовжує відповідати після того, як початкове повідомлення було передано. Це дозволяє серверам організовувати потокову передачу змін станів датчиків.

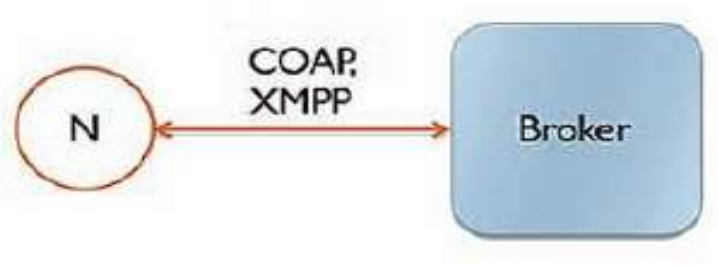


Рис. 10.8. Сегмент мережі де використовується протокол CoAP та XMPP

Таким чином, на ділянці мережі між сенсорним вузлом і брокером для забезпечення їх зв'язку, з метою реєстрації та конфігурації вузлів, а також для передачі інформації найчастіше застосовуються два протоколи - *XMPP* та *CoAP*. Фактичний протокол протоколу залежить від умов, які реалізується на мережі. Можна відзначити, що *XMPP* знайшов своє застосування в системах освітлення і клімату, а також використовується для адресування пристроїв в невеликих персональних мережах.

Очевидно, що *CoAP* призначений для пристроїв з обмеженими ресурсами й для мереж з низьким енергоспоживанням. Відомо застосування протоколу в системах датчиків температури та інших датчиків розумного будинку.

Протокол STOMP

STOMP - Simple (або Streaming) Text Oriented Message Protocol - простий протокол обміну повідомленнями, що передбачає широку взаємодію з багатьма мовами, платформами та брокерами [2]. Даний протокол підходить під шаблон "видавець-передплатник" і за допомогою повідомлень SEND (відправити), SUBSCRIBE (підписатися), UNSUBSCRIBE (відписатися), BEGIN (почати), ABORT (переривати), ACK (підтвердити), NACK(не підтвердити), ISCONNECT(відключити) організовує зв'язок з брокером за методом "запит-відповідь".

Цей протокол використовується в тих випадках, коли необхідно застосування простого протоколу передачі повідомлень в мережах, що мають обладнання різних платформ.

Протокол схожий на HTTP, використовує транспорт TCP, є простим текстовим протоколом, що дозволяє клієнтам STOMP спілкуватися з будь-яким брокером повідомлень, котрі підтримують цей протокол [3].

Таким чином, цей спосіб взаємодії, розроблений для обміну повідомленнями між платформою, описаною одною мовою програмування, і клієнтом, програмне забезпечення якого розроблене іншою мовою. Підтримує велику кількість сумісних клієнтських бібліотек.

Треба відзначити, що для забезпечення роботи брокера в мережі Інтернету речей можливе використання обох протоколів: MQTT і STOMP. Тільки протокол STOMP орієнтований тільки на взаємодію брокера з сервером, а протокол MQTT забезпечує "наскрізний“ зв'язок, як від брокера до сенсорних вузлів, так і від брокера до сервера.

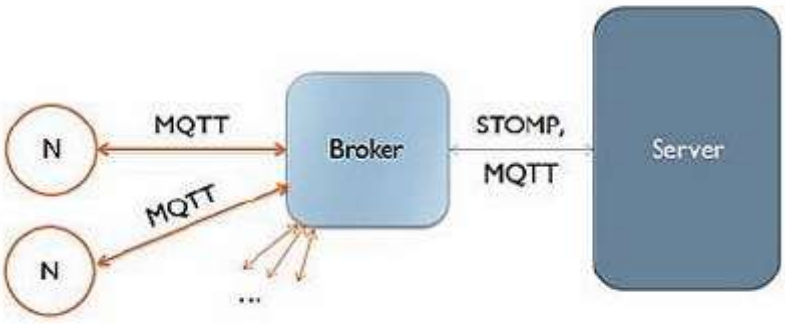


Рис. 10.9. Сегмент мережі де використовується протокол MQTT та STOMP

Протокол SOAP

SOAP (Simple Object Access Protocol) – протокол обміну сруктурованими та довільними повідомленнями формату XML в розподіленому обчислювальному середовищі [1]. SOAP використовує базову модель з'єднання, що забезпечує узгоджену передачу повідомлення від відправника до одержувача, потенційно допускає наявність посередників, які можуть обробляти частина повідомлення або додати до нього додаткові елементи [4].

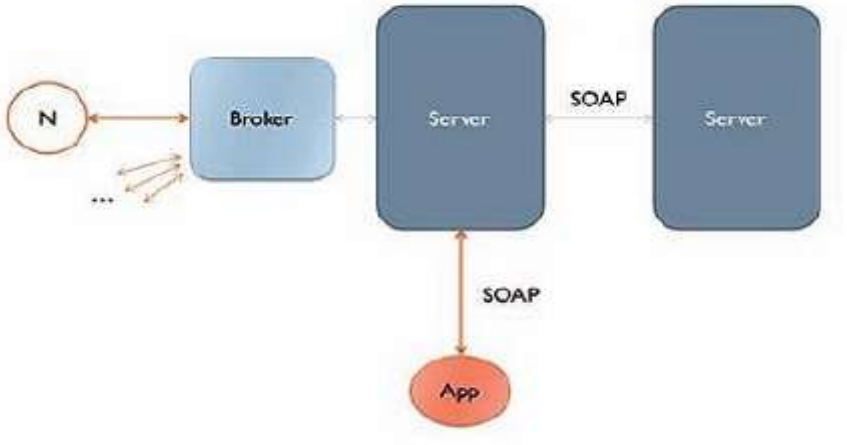


Рис. 10.10. Сегмент мережі де використовується протокол SOAP

SOAP підтримує два механізми доступу - SOAP MESSAGE та SOAP RPC [5].

SOAP MESSAGE - це протокол для відправлення та обробка SOAP повідомлень, заснованиа на об'єкті Message. Може використовуватися для асинхронних комунікацій та має на увазі негайну, або відкладену відповідь на запит.

SOAP RPC являє собою простий протокол "запит-відповідь", який базується на об'єкті Call. Цей об'єкт використовується для синхронного віддаленого виклику процедур за допомогою XML.

Завдяки декільком повідомленням (GET, SOAP ACTION–RESPONSE, SOAP ACTION), який передбачає запит-відповідь, протокол може використовуватися з будь-яким протоколом прикладного рівня: FTP, HTTPS, SMTP [6].

Протокол MQTT

MQTT (Message Queue Telemetry Transport) - це легкий, компактний і відкритий протокол обміну даними створений для передачі даних на віддалених локаціях, де потрібний невеликий розмір коду і є обмеження до пропускної здатності каналу [7]. Перераховані вище вимоги дозволяють застосовувати його в системах M2M (машина-машина).

MQTT був внутрішнім і пропрієтарним протоколом для *IBM* протягом багатьох років, поки не був випущений у версії 3.1 в 2010 р в якості безкоштовного продукту. У 2013 р *MQTT* був стандартизований і прийнятий в консорціум *OASIS*. У 2014 р *OASIS* опублікував його публічно як версію *MQTT 3.1.1*. *MQTT* також є стандартом *ISO (ISO / IECPRF 20922*). *MQTT* базується на стеці *TCP/IP* [8].

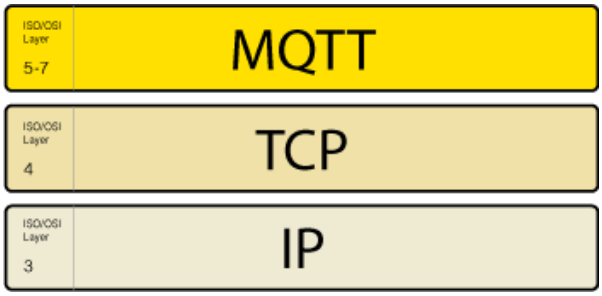


Рис. 10.11. Протокол *MQTT*

У той час як архітектури клієнт-сервер багато років є основою для сервісів центрів обробки, моделі публікація-підписка (*publish-subscribe*) представляють собою альтернативу, яка корисна для використання *IoT*. Публікація-підписка, також відома як *pub/sub*, є способом відокремити клієнта, що передає повідомлення, від іншого клієнта, який отримує повідомлення. На відміну від традиційної моделі клієнт-сервер, клієнти не обізнані про будь-які фізичні ідентифікатори інтерфейсів пристроїв/програм, на зразок *IP*-адреси або порту.

MQTT - це архітектура *pub/sub*, однак не є чергою повідомлень. Черги повідомлень по природі своїй зберігають повідомлення, а *MQTT* - ні. У *MQTT*, якщо ніхто не підписується (або не слухає) на тему (*topic*), повідомлення просто ігноруються і втрачаються. Черги повідомлень також підтримують топологію клієнт-сервер, де один споживач з'єднаний з одним виробником.

Клієнт, що передає повідомлення, називається **видавцем** (**publisher**); клієнт, який отримує повідомлення - **абонентом** (**subscriber**). У центрі знаходиться **MQTT-брокер** (**MQTT broker**), який несе відповідальність за обмін повідомленнями між клієнтами і фільтрацію даних. Такі фільтри забезпечують:

- **фільтрацію за темами** (**Topic Filters**) - за задумом, клієнти підписуються на **теми** (**topic**) і певні гілки тем і не отримують даних більше, ніж хочуть. Кожне опубліковане повідомлення повинно містити тему (topic), і брокер несе відповідальність за повторну передачу цього повідомлення абонентам або ігнорування його;
- **фільтрація по вмісту** - брокери мають можливість перевіряти і фільтрувати опубліковані дані. Таким чином, будь-які дані, які не зашифровані, можуть керуватися брокером до того, як зберегти їх або передати іншим клієнтам;
- **фільтрація за типом** - клієнт, що прослуховує потік даних, на які він підписаний, може також застосовувати свої власні фільтри. Вхідні дані можуть аналізуватися, і в залежності від цього потік даних обробляється далі або ігнорується.

Клієнти працюють на краю (*Edge*), публікують і/або підписуються на теми, керовані брокером *MQTT*. У прикладі розглянуті дві теми (topic): вологість і температура. Клієнт може підписатися на кілька тем. На рисунку представлені розумні датчики, що володіють достатніми ресурсами для управління власним клієнтом *MQTT*, а також прикордонні маршрутизатори (*Edge Routers*), які надають клієнтські послуги *MQTT* від імені датчиків або пристроїв, які не підтримують *MQTT*. Одне із особливостей моделі обчислень видавець/абонент полягає в тому, що як видавець, так і абонент повинні знати тему гілки і формат даних перед початком передачі [9].

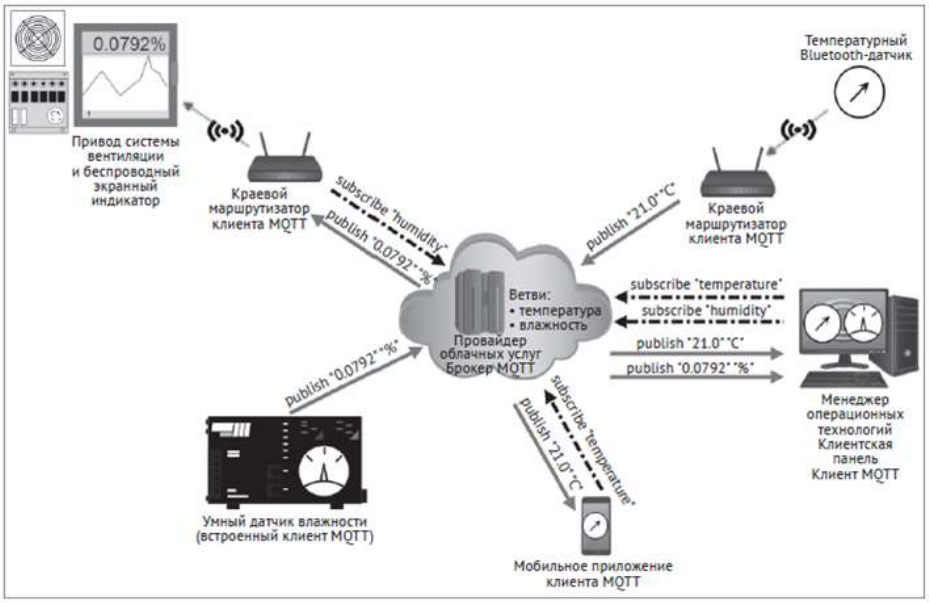


Рис. 10.12. Основні принципи взаємодії MQTT

MQTT успішно відокремлює видавців від абонентів. Оскільки брокер є керівним органом між видавцями і абонентами, немає необхідності безпосередньо ідентифікувати їх на основі фізичних даних (таких як *IP*-адреса). Це дуже корисно при розгортанні *IoT*, оскільки фізичний ідентифікатор може бути невідомим або загальним. *MQTT* і інші моделі *pub/sub* також є часово-незалежними. Це значить, що повідомлення, опубліковане одним клієнтом-видавцем, може бути прочитане абонентом в будь-який час. Абонент може перебувати в місці з дуже низьким енергоспоживанням/обмеженою пропускною здатністю і відповісти на повідомлення через кілька хвилин або годин. Через відсутність фізичних і часових залежностей моделі *pub/sub* дуже добре підходять для підвищення продуктивності.

MQTT не залежить від формату даних. Корисне навантаження (*payload*) може містити будь-який тип даних, тому і видавці, і абоненти повинні розуміти і погоджувати формат даних. У корисне навантаження можна надсилати текстові повідомлення, дані зображення, звукові дані, зашифровані дані, двійкові дані, об'єкти *JSON* або практично будь-яку іншу структуру. Однак текстові і двійкові дані *JSON* є найбільш поширеними типами даних корисного навантаження.

Максимально допустимий розмір пакета в *MQTT* становить 256 Мб, що дозволяє отримати надзвичайно велике корисне навантаження. Зверніть увагу, однак, що це також залежить від хмари і брокера. Наприклад, *IBM Watson* дозволяє обробляти дані розміром до 128 Кб, а *Google* підтримує 256 Кб. З іншого боку, опубліковане повідомлення може включати корисне навантаження нульової довжини. Поле корисного навантаження не є обов'язковим. Доцільно звірити відповідність розмірів корисного навантаження з вашим хмарним провайдером. Недотримання цієї вимоги призведе до помилок і відмови у доступі до хмарного брокера.

Деталі архітектури MQTT

MQTT може зберігати повідомлення в брокері необмежено довго. Цей режим роботи керується прапорцем. Збережене на брокері повідомлення відправляється будь-якому клієнту, який підписується на цю тематичну гілку *MQTT*. Повідомлення негайно відправляється цьому новому клієнту. Це дозволяє йому отримати статус або сигнал з теми, на яку він недавно підписався, без очікування. Як правило, клієнт, що підписується на тему, може очікувати годину або навіть дні, перш ніж інший клієнт-видавець опублікує нові дані.

MQTT означує додатковий об'єкт під назвою ***Остання воля і заповіт (LWT)***. *LWT* - це повідомлення, яке вказує клієнт під час етапу підключення. *LWT* містить тему «Остання воля», *QoS* і фактичне повідомлення. Якщо клієнт неправильно відключається від

брокерського з'єднання (наприклад, тайм-аут *keep-alive*, помилка введення-виведення або клієнт закриває сеанс без відключення), тоді брокер зобов'язаний транслювати повідомлення *LWT* всім іншим підписаним на цю тему клієнтам [9].

Незважаючи на те, що *MQTT* заснований на *TCP*, з'єднання все ще можуть обриватися, особливо в разі безпроводових датчиків. Пристрій може втратити живлення, зв'язок, або може бути просто польова поломка, і сеанс перейде в напіввідкритий стан (тобто з одного боку вважається що з'єднання є, а з іншого воно відсутнє). Тоді сервер буде вважати, що з'єднання як і раніше є надійним і очікувати дані. Щоб вийти з цього напіввідкритого стану, *MQTT* використовує систему ***keep-alive (утримування)***.

Використовуючи цю систему, як брокер *MQTT*, так і клієнт мають гарантію того, що з'єднання залишається працездатним, навіть якщо протягом деякого часу не було передачі. Після отримання чергового будь-якого пакету, таймери *keep-alive* скидаються на клієнті і сервері і починають відлік. Якщо протягом часу *keep-alive* клієнти не мають даних для відправки, вони повинні сформувати відправити пакет *PINGREQ* брокеру, який, в свою чергу, підтверджує повідомлення за допомогою *PINGRESP*. Якщо протягом півтора часу *keep-alive* пакет не буде отримано, брокер закриє з'єднання і відправить *LWT*-пакет всім клієнтам. Максимальний час *keep-alive* – 18 годин 12 хвилин 15 секунд.

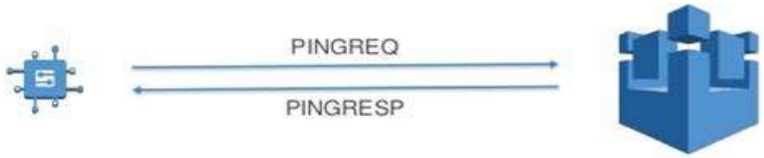


Рис. 10.13. Використання системи *keep-alive*

MQTT дозволяє також підтримувати постійні з'єднання. Постійні з'єднання зберігає на стороні брокера наступне:

- всі підписки клієнта
- всі повідомлення QoS, які не були підтверджені клієнтом
- всі нові повідомлення QoS, пропущені клієнтом

Параметр *client_id* посилається на цю інформацію для унікальної ідентифікації клієнтів. Клієнт може запитувати постійне з'єднання, проте брокер може відхилити запит і примусово перезапустити новий сеанс. При з'єднанні брокером використовується прапорець *cleanSession* для дозволу або заборони постійних з'єднань. Клієнт може визначити, чи збереглося постійне з'єднання за допомогою повідомлення *CONNACK*.

Постійні сеанси повинні використовуватися для клієнтів, які повинні отримувати всі повідомлення, навіть коли немає зв'язку. Вони не повинні використовуватися в ситуаціях, коли клієнт тільки публікує (записує) дані в теми.

Рівні якості обслуговування MQTT

У MQTT є три рівня якості обслуговування:

QoS-0 (незавірена передача) - це мінімальний рівень QoS. Це аналогічно моделі «спалити і забути», докладно описаної в деяких бездротових протоколах. Це найефективніший процес доставки без підтвердження одержувачем повідомлення і без повторної передачі повідомлення відправником;

QoS-1 (гарантована передача) - цей режим гарантує доставку повідомлення хоча б один раз одержувачу. Повідомлення може бути доставлено кілька разів, і одержувач відправить назад підтвердження з відповіддю PUBACK;

QoS-2 (гарантований сервіс для додатків) - це найвищий рівень QoS, який переконується в доставці і інформує відправника і одержувача, що повідомлення було передано правильно. Цей режим генерує більше трафіку через багатокрокове рукостискання між відправником і отримувачем.

Якщо одержувач отримує повідомлення з рівнем обслуговування *QoS-2*, він відповість відправнику повідомленням *PUBREC*. Це підтверджує повідомлення, і відправник відповість повідомленням *PUBREL*. *PUBREL* дозволяє одержувачеві безпечно відкинути будь-які повторні передачі цього повідомлення. Потім *PUBREL* підтверджується одержувачем за допомогою *PUBCOMP*. Поки повідомлення PUBCOMP передано не буде, приймач буде кешувати вихідне повідомлення для забезпечення безпеки.

QoS в *MQTT* визначається і контролюється відправником, і у кожного відправника може бути своя політика.

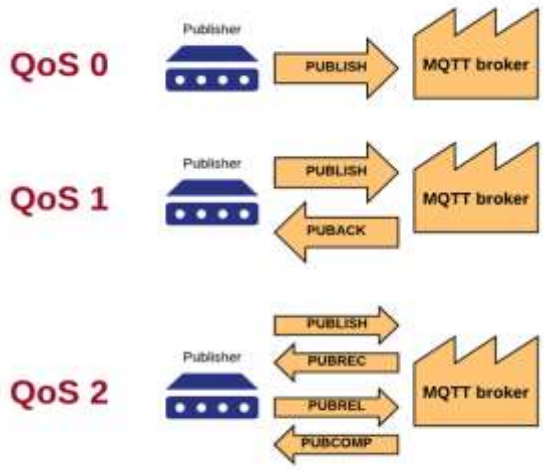


Рис. 10.14. Рівні якості обслуговування MQTT

Типові випадки використання [8]:

QoS-0 слід використовувати, коли повідомлення не потрібно зберігати в черзі. QoS-0 найкраще підходить для провідного підключення або коли система сильно обмежена в пропускної здатності;

Qos-1 слід використовувати за замовчуванням. QoS1 набагато швидше, ніж QoS2, і значно знижує вартість передачі;

QoS-2 - для критично важливих застосунків. Крім того, для випадків, коли повторна передача дубльованого повідомлення може привести до помилок.

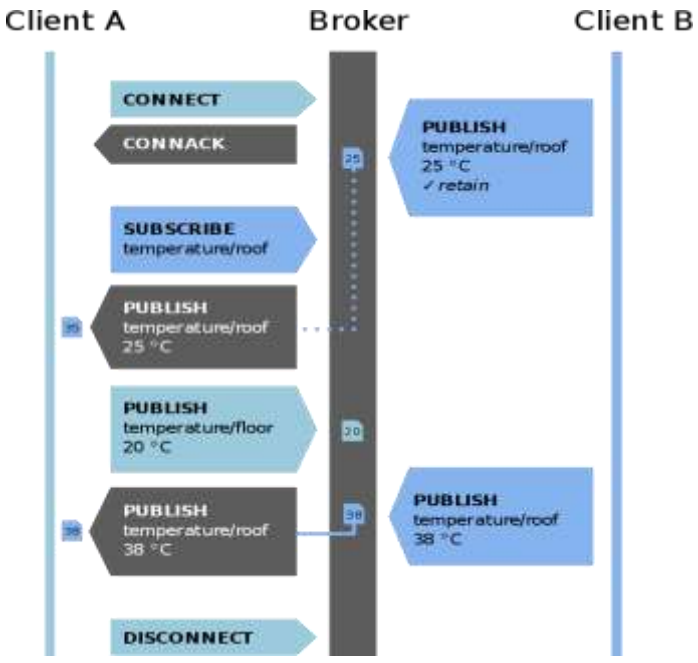


Рис. 10.15. Процедури та повідомлення, що використовуються в MQTT

Також існує версія протоколу *MQTT-SN* (MQTT для мереж датчиків), раніше відома як *MQTT-S*, яка призначена для вбудованих бездротових пристроїв без підтримки *TCP/IP* мереж.

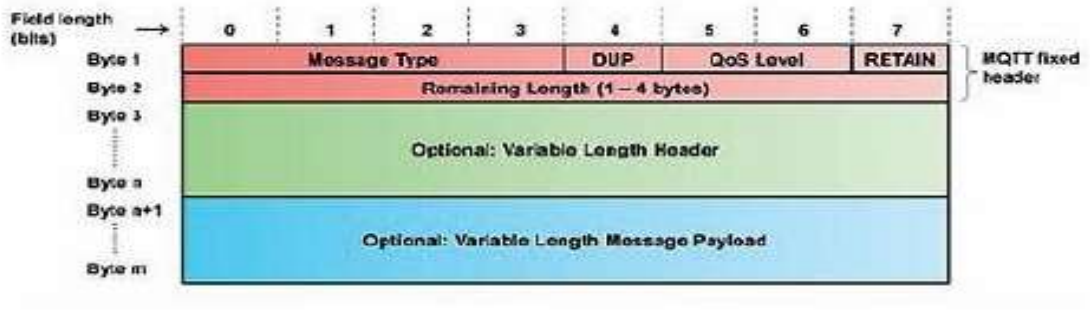


Рис. 10.16. Загальний формат повідомлення протоколу MQTT

На рисунку 10.16 представлений загальний формат повідомлень проколу MQTT. Повідомлення складається з двох заголовків:

- *MQTT Fixed Header* – заголовок фіксованої довжини;
- *Variable Length Header* – заголовок змінної довжини (в залежності від типу повідомлення);
- *Variable Length Message Payload* – поля корисного навантаження змінної довжини.

До заголовка фіксованої довжини входять такі поля:

- *Message Type* – тип повідомлення,
- *DUP* – прапор дублювання повідомлення,
- *QoS Level* – рівень якості обслуговування,
- *Retain* – спеціальний прапор збереження останнього прийнятого брокером повідомлення,
- *Remaining Length* – залишкова довжина,

Спрощений процес роботи протоколу MQTT:

Видавець передає повідомлення з певними даними (наприклад, інформація з датчиків вологості) на брокера, вказуючи при цьому тему (Topic), до якої ці дані відносяться (наприклад, "вологість").(див. рис. 10.17) [10].

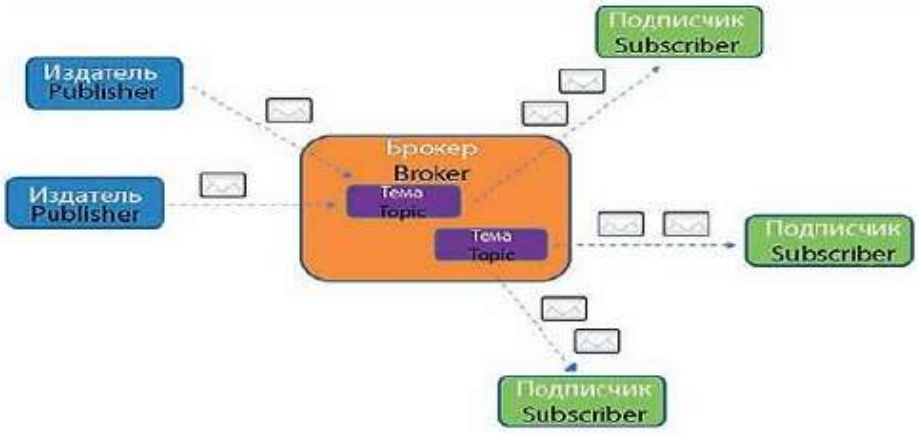


Рис. 10.17. Спрощений процес роботи протоколу MQTT

Брокер аналізує, які із передплатників мають підписку на певні теми, в даному випадку – на тему "вологість". Передплатникам, які підписані на тему "вологість", брокером буде відправлено повідомлення з інформацією від датчиків вологості. Таким чином, безліч

передплатників можуть бути підписані на різноманітні теми і в залежності від цих підписок отримувати необхідну їм інформацію, не спілкуючись з видавцем безпосередньо [11].

На рисунку 10.17. зображено схему передачі інформації за принципом "видавець-передплатник" [12].

Таблиця. 10.1. Порівняльна характеристика протоколів передачі повідомлень

Протокол	Транспорт	Призначення	Особливості
DDS	UDP	Для мереж, що потребують розподіленого навантаження	Реалізує прямий шинний зв'язок між пристроями на базі реляційної моделі даних
XMPP	TCP	Для адресації в невеликій персональній мережі	Для ідентифікації користувачів використовуються JID, по формату схожі на адреса електронної пошти (username@gmail.com)
COAP	UDP	Для мереж з обмеженими ресурсами, низьким Електроспоживанням	Враховує різні питання середовища реалізації в обмежених мережах
MQTT	TCP	Для завантажених мереж з великою кількістю пристроїв та Брокером	Використання механізму черг повідомлень
STOMP	TCP	Для мереж, в яких є можливість використання декількох комбінацій різних протоколів, що потребують простий протокол передачі повідомлень через брокера	Взаємодія з більшістю мов, платформ та Брокерами
SOAP	TCP	Для розподіленої обчислювальної мережі	Підтримує два механізми доступу: SOAP RPC та SOAP Message

Контрольні питання до розділу

1. Які протоколи і на яких рівнях архітектури IoT працюють?
2. Протокол маршрутизації RPL.
3. Наведіть категорії протоколів IoT.
4. Протокол IEEE 802.15.4. Архітектура IEEE 802.15.4. Типи вузлів мережі.
5. Протокол 6LoWPAN**.** Архітектура 6LoWPAN.
6. Bluetooth Low Energy.
7. Протокол EPCglobal. Компоненти RFID системи.
8. Протокол Z-Wave.
9. Протокол ZigBee.
10. Протоколи виявлення сервісів.
11. Протоколи рівня додатків**.** Базова топологія, яка використовується для передачі повідомлень в IoT.
12. Протокол DDS. Принцип з'єднання пристроїв за допомогою протоколу DDS в IoT
13. Протокол XMPP.
14. Протокол CoAP. Наведіть структуру сегменту мережі де використовується протокол CoAP та XMPP.
15. Протокол STOMP. Наведіть структуру сегменту мережі де використовується протокол MQTT та STOMP.
16. Протокол SOAP. Наведіть структуру сегменту мережі де використовується протокол SOAP.
17. Протокол MQTT. Основні принципи взаємодії MQTT.
18. Наведіть основні деталі архітектури MQTT.
19. Скільки існує рівнів якості обслуговування MQTT?
20 Наведіть загальний формат повідомлення протоколу MQTT.
21 В чому виражається спрощений процес роботи протоколу MQTT?

Список рекомендованої літератури

1. Аналитический обзор протоколов Интернета вещей // електрон. текст. дані URL: http://lib.tssonline.ru/articles2/reviews/analiticheskiy-obzor-protokolov-interneta-veschey
2. Протоколы «Интернета вещей»: основные сведения // електрон. текст. дані URL: http://old.rtsoft.ru/press/articles/detail.php?ID=2718
3. Z-Wave Technical Basics // електрон. текст. дані URL: https://www.domotiga.nl/attachments/download/1075/Z-Wave%20Technical%20Basics-small.pdf
4. Wi-Fi HaLow (IEEE 802.11ah) — дальнобойное беспроводное подключение с низким энергопотреблением для интернета вещей // електрон. текст. дані URL: https://www.ixbt.com/news/2016/01/05/wi-fi-halow-ieee-802-11ah.html
5. What's The Difference Between DDS And AMQP? // електрон. текст. дані URL: https://www.electronicdesign.com/embedded/what-s-difference-between-dds-and-amqp
6. XMPP // електрон. текст. Дані URL: https://ru.wikipedia.org/wiki/XMPP
7. Что такое MQTT и для чего он нужен в IIoT? Описание протокола MQTT // електрон. текст. дані URL: https://ipc2u.ru/articles/prostye-resheniya/chto-takoe-mqtt/
8. Протокол MQTT. Особенности, варианты применения, основные процедуры MQTT Protocol. // електрон. текст. Дані URL: http://www.mka.ru/categories/81/10416/
9. Что такое MQTT и для чего он нужен в IIoT? Описание протокола MQTT // електрон. текст. дані URL: https://ipc2u.ru/articles/prostye-resheniya/chto takoe-mqtt/
10. Протокол MQTT. Особенности, варианты применения, основные Процедуры MQTT Protocol. // електрон. текст. Дані URL: http://www.mka.ru/categories/81/10416/ (дата звернення: 01.06.2019)
11. Технологии для Web-сервисов // електрон. текст. дані URL: https://compress.ru/article.aspx?id=10975
12. Интернет вещей: В Украине построят сети для роботов и датчиков // електрон. текст. дані URL: https://biz.liga.net/all/telekom/article/oni-byli-kiborgi-v-ukraine-stoyat-seti-dlya-robotov-i-datchikov

РОЗДІЛ 11. РОЗУМНИЙ ТА БЕЗПЕЧНИЙ БУДИНОК

11.1.Елементи «розумного будинку»

Зростаюча різноманітність інтелектуальних датчиків, програмних рішень, підключених пристроїв, хмарних сервісів те що встановлено, щоб ми могли працювати в різних формах та форматах у наших живих та робочих середовищах.

Це квартири, офісні будівлі, виробничі поверхи та інші орієнтовані на дії, жваві та чудові місця, мають бути надзвичайно потужними та розширені технологіями. Звичайні і повсякденні об'єкти цифруються, з'єднуються один з одним локальної. Це - все, що в наших місцях, систематично наділяється відповідними та правильними інтелектуальними можливостями шляхом додавання функціональних модулів всередині, а також шляхом інтеграції з віддаленим програмним забезпеченням.

Навіть комунікаційні мережі наповнюються відповідними компетенціями та можливостями, щоб покращити роботу, випадкову та дешеву річ зробити розумною, будь-яку електроніку більш розумною, і в кінцевому підсумку люди - найрозумніші.

Всі види недоліків та залежностей усуваються за допомогою безлічі таких заходів, як стандартизація, адаптери, мости, проміжне програмне забезпечення, загальні інтерфейси API тощо. Можливості підключення і відтворення гарантуються. Пристрої виробляються належним чином та модернізуються, щоб об'єднувати та співпрацювати один з одним для реалізації завдань, орієнтованих на людей. Збирання інформації, агрегація, поширення, важелі впливу для полегшення розуміння інформації та концепцій візуалізації, що постійно посилюються до бачення більш інтелектуальних середовищ.

Пристрої виробляються з використанням дуже сильної фабричної моделі/індустріалізації. Всі високотехнологічні IT-сервери, сховища та мережеві рішення підлягають товарообігу. Це досягається шляхом виявлення та абстрагування всіх видів загальних функціональних можливостей, особливостей та засобів. Всі реалізовані через програмне забезпечення.

Важливі аспекти, такі як модифікованість, заміна, підставість, доступність, витратні можливості тощо легко інтегруються в програмне забезпечення.

Політика та бази знань у поєднанні з менеджером знань з'являються як механізм нового покоління для створення автономічної інфраструктури.

Програмний маршрут рекомендується для встановлення політики та виконання.

«Розумний будинок» призначений для максимально комфортного життя людей за допомогою використання сучасних високотехнологічних засобів [1].

Принцип роботи системи «розумний будинок» полягає в автоматизації всього, з чого складається житлова споруда: освітлення, кондиціонування, система безпеки, електроенергія, опалення, водопостачання та водовідведення і так далі.

Рис. 11.1. Складові «розумного будинку»

До основних підсистем «розумного будинку» відносяться: клімат-контроль, освітлення, мультимедіа (аудіо і відео), охоронні системи, зв'язок і інш.

В останньому випадку це датчики руху, світла, температури, тиску, вологості, вібрації і т.п.

Таким чином, «розумний будинок» складається з програмного і апаратного забезпечення, датчиків і проводової / безпроводової мережі.

У загальному випадку, «розумний будинок» надає його власнику такі переваги:

1) зниження споживання ресурсів (газ, вода, електроенергія);

2) високий рівень комфорту;

3) забезпечення необхідної взаємодії всіх систем об'єкта нерухомості, що автоматизуються, задання різних режимів роботи;

4) зниження ймовірності виникнення аварійних ситуацій;

5) підвищення оперативності, простоти і зручності управління.

Рис. 11.2. Компоненти «розумного будинку»

Більшість побутових пристроїв з категорії «розумних» речей можна поділити на дві групи за типом використання Інтернету.

До першої групи належить техніка, яка через *WWW* оновлює своє програмне забезпечення, отримує нові функції, приймає сигнали, коли знаходиться далеко господаря, і, відповідно, відправляє йому інформацію, яка підтверджує виконані дії та свій стан. Цей тип використання Інтернету побутовою технікою є найбільш розумним і здатний довести потенційному споживачеві свою корисність [2].

До другої групи входить техніка, в якій Інтернет є як би стороннім тілом. Сутність рішення в тому, що в абсолютно звичний побутовий прилад, типу мікрохвильовки або холодильника, вбудовується спрощений комп'ютер і дисплей, після чого з їх допомогою можна отримувати мультимедійні розваги там, де їх раніше не було, наприклад, на тій же кухні [2].

Одним з найперших прикладів побутової техніки, що має підключення до Інтернету, є звичайний тостер, оснащений інтерфейсом для віддаленого включення і повідомлення про готовність підсмаженого тосту. Так техножарт *Джона Ромки*, одного з перших фахівців в області *TCP/IP*-протоколу, породив в далекому 1988 році технотренд Інтернету речей, який в наші дні втілюється в життя.

Зростаючий список відомих домашніх мереж та рішень для автоматизації включає в себе наступне:

- *Елементи безпеки та спостереження*: датчики безпеки для вікон, дверей, руху, розбиття скла та диму можуть надавати найважливішу інформацію про безпеку наших будинків, коли ви знаходитесь вдома або в офісі. IP-захищені камери безпеки та спостереження дуже важливі для забезпечення тісної, нерозбитної та непроникної безпеки. Системи виявлення та попередження вторгнення є іншими відомими модулями безпеки.
- *Системи опалення, кондиціонування повітря, системи вентиляції, освітлення та системи відтінків*: Комфорт стає вирішальним чинником у будинках нового покоління. Нові машини оснащуються інструментами, щоб забезпечити різні умови навколишнього середовища. Забезпечується зв'язок між різними домашніми пристроями, включаючи світлові вимикачі, настінні сенсорні панелі тощо. Роботи оснащуються різними варіаціями для здійснення фізичних робіт для людей. Роботи, обладнані *Cloud*, будуть критично важливим для людей у той час, коли вони стануть розвинутими.
- *Обчислювальні та комунікаційні пристрої*. В даний час в домашніх умовах використовується широкий спектр обчислювальних машин, починаючи від персональних комп'ютерів (ПК), ноутбуків / ноутбуків / планшетів, маршрутизаторів *Wi-Fi* та шлюзів, носіїв та смартфонів.
- *Розваги, освіта та системи масової інформації*. Однією з найважливіших нововведень у медіа-технологіях та продуктах за останні роки.

Сьогодні ми можемо похвалитися фіксованими, портативними, мобільними пристроями для повсякденного навчання. Телевізори, що підтримують IP, виробляються в масових обсягах, різко збільшуючи наш вибір, зручність та комфорт. Веб, інформаційні та побутові прилади є достатніми та новаторськими. Технології для соціальних сайтів (веб 2.0) знаходяться на підйомі, що сприяє підвищенню продуктивності праці для людей та формуванню цифрових спільнот для обміну знаннями в режимі реального часу. Для домашнього кінотеатру, музичних систем *hi-fi*, *DVD-пристроїв*, ігрових консолей тощо [3].

- *Домашня мережа*: всі пасивні, онімілі предмети перетворюються на цифрові об'єкти. Вони підключаються до бездротової та розумної мережі з усіма видами побутової електроніки, щоб обмінюватися та спілкуватися (безпосередньо [однорангові] або опосередковано, через посередницькі пристрої). Кожного для підключається все більше і більше користувачів, до національної мережі. Домашня мережа також може з'єднуватися із зовнішнім світом через всеохоплюючий Інтернет. Що дозволяє дистанційно спостерігати, управляти та обслуговувати домашні пристрої. Автомобільні мультимедіа, навігаційні та інформаційно-розважальні системи, системи керування паркуванням тощо, також підключаються до домашніх систем безпосередньо або через проміжне програмне забезпечення на базі коробки для взаємодії та взаємодії в реальному часі.
- *Домашній контроль доступу:* Е-замки з'являються як найважливіша заходи безпеки для домашнього контролю доступу.
- *Розслабляючі та об'єкти настрою:* крім об'єктів у певних місцях, таких як тренажерні зали, санаторії, санвузли, гаражі автомобілів, предмети домашнього ужитку, такі як електричні лампи, ліжечка, стільці, шафи, віконні панелі, дивани, бігові доріжки, столи, дивани, автостоянки тощо з'єднуються між собою, щоб значно покращити настрій, стан користувачів.
- *Системи охорони здоров'я*: медичні кабінети, пігулки та таблетки, гумоїдних роботів і так далі займають перші слоти, що гарантують здорове життя для мешканців житла.
- *Кухонна техніка, вироби та посуд*. Модульна кухня, що включає в себе всі види електроніки, виявляється ключовим фактором для розумніших будинків. Кавоварки, хлібні тостерів, електронні печі, холодильники, мийки для посуду, кухонні комбайни тощо покращуються, щоб бути розумнішими в домашніх умовах.

- *Інтернет-холодильник* (*Internet refrigerator або Smart refrigerator*) – новий клас побутових холодильників, що з'явився на початку XXI століття. Як правило, він має вбудований комп'ютер з постійним підключенням до мережі інтернет і сенсорним екраном на фронтальній панелі

Рис. 11.3. Інтернет-холодильник

Такий холодильник не тільки зберігає продукти, а й дає можливість користуватися інтернетом, через який можна отримати доступ до різних сайтів (наприклад, з кулінарними рецептами для приготування страв) і навіть замовляти продукти в інтернет-магазинах з доставкою додому. Крім того, за допомогою інтернет-холодильника можна спілкуватися, використовуючи електронну і відеопошту.

Інтернет-холодильник може надавати цілий ряд сервісів: доступ в *Інтернет*, відеотелефон, *e-mail, TV, MP3*- музику, базу даних по улінарних рецептах і правилах харчування, електронне перо, щоб залишити повідомлення, голосові послання. Ряд моделей інтернет-холодильників обладнані телевізійним і радіоприймачем. Крім того, при використанні інтернет-холодильника з'являється можливість вивести на екран картинку з веб-камери зовнішнього відеоспостереження [2].

Це дозволяє бачити те, що відбувається у дворі приватного будинку, навіть не покидаючи кухні доглядати за своїм малюком, що знаходяться в дитячій кімнаті і т.д. Деякі пристрої даного типу також можуть стежити за вмістом холодильника, вибираючи оптимальні умови зберігання та заморозки продуктів. Крім цього, інтернет-холодильник відстежує продукти з терміном придатності. Інформація про все це надходить на смартфон користувача і останній, перебуваючи в магазині, може оцінити свої реальні потреби в продуктах.

Робот-пилосос може діяти автономно, програмуватися і управлятися через Інтернет, для чого є ряд сенсорів і інфрачервона вбудована камера. Система управління роботою пилососа робить кілька знімків в секунду створюючи, таким чином, карту всього будинку або окремих його кімнат. Пристрій також має можливість запам'ятовувати оптимальний шлях збирання і визначати своє місцезнаходження в будинку.

Рис. 11.4. Робот-пилосос

Акумулятора вистачає на певний час збирання (зазвичай до 1,5 годин), після закінчення якого робот сам відправляється на підзарядку. До пилососа є бездротовий доступ Wi-Fi за допомогою комп'ютера або смартфона. Через ці пристрої можна запустити його і в режимі реального часу спостерігати за тим, що відбувається в кімнаті. Більш того, можна поговорити з людьми, які знаходяться в будинку через систему голосового зв'язку. Вбудований джерело світла дозволяє бачити в повній темряві і перевірити приміщення навіть вночі.

Інтернет мікрохвильова піч має вбудований модем для виходу в інтернет, пам'ять для зберігання завантажувати інформацію і пульт управління. Вона виконує такі завдання:

- скачування рецептів з Інтернету і самопрограмування;
- зв'язок з компаніями - виробниками продуктів;
- дає доступ до системи замовлення продуктів по інтернету.

Інтернет-кондиціонер підключається до інтернету через проводову або безпроводову мережу *WiFi* і дає користувачеві доступ до управління кондиціонером з будь-якої точки земної кулі. Власник може дистанційно вмикати і вимикати систему, програмувати настройки, вибір між режимами, температуру, швидкість вентилятора, задавати параметри, словом здійснювати будь-які маніпуляції, доступні зі звичайного пульта. Керувати таким кондиціонером можна з будь-якого пристрою (комп'ютер, ноутбук, планшет, смартфон), в якому встановлена спеціальна програма і який має вихід в інтернет.

Рис. 11.5. Компоненти «розумного будинку»

Система по догляду за домашніми тваринами покликана забезпечити їм всі необхідні комфортні умови існування. Така система використовується в разі тривалої відсутності господарів будинку - це дозволяє не турбуватися про добробут своїх домашніх улюбленців. Основними завданнями системи по догляду за домашніми тваринами є автоматична подача їжі і пиття, а в разі виникнення непередбачених обставин - інформування господарів про них (по телефону, за допомогою SMS або по електронній пошті). За бажанням можна скласти повний звіт про поведінку домашніх улюбленців під час відсутності господарів - скільки разів і коли їли, коли ходили в туалет, пили воду і т.д.

Можна навіть супроводити цей звіт фотографіями (якщо встановлена камера спостереження) і передавати їх (по електронній пошті, за допомогою MMS) - словом, все, щоб господарі відчували себе комфортно і були впевнені в тому, що їх улюбленцям нічого не загрожує.

Отримані статистичні підрахунки та прогнози про те, що в вже з'являться сотні мікроконтролерів у будь-яких вдосконалених домашніх/офісних середовищах. Надзвичайно популярні технології, такі як картки, чіпи, наклейки, теги, інтелектуальні пил і т. д. дає початок потужному середовищу.

Наші повсякденні місця будуть наповнені і насичені зростаючою кількістю об'єктів, що виробляють та споживають події, екологічний моніторинг та вимірювальні рішення, системи контролю, активації та оповіщення, інтеграційні тканини, автобуси та дисплеї візуалізації та

інформаційні панелі, елементи мережевих та автоматичних пристроїв, десятки кишенькових комп'ютерів, портативних комп'ютерів, переносних приладів та ін., щоб зробити наше життя і місця приємним і придатним для життя.

Тобто розумний будинок – це система, яка забезпечує безпеку, ресурсозбереження та комфорт для всіх його користувачів. Як правило в розумному будинку є центральний процесор – так звані мізки будинку. Цей процесор розпізнає конкретні ситуації, що відбуваються в будинку і реагує на них: керує поведінкою інших систем за допомогою заданих алгоритмів (наприклад, включення світла в коридорі, коли відкривається вхідні двері). За рахунок цього в розумному будинку немає необхідності використовувати десятки різних пультів для кожного телевізора або кондиціонера, або постійно намацувати вимикачі світла в темряві [3].

Всю систему можна розділити на деякі компоненти: *автоматизація, ручне управління, мультимедіа, безпеку*.

Автоматизація – в нашому випадку це налаштування роботи системи в залежності від часу доби, рівня освітленості, руху, температури, макросів і сценаріїв.

Ручне управління всім зрозуміло, але не сказати про нього не можна. Це віддалене управління по телефону, комп'ютера, web додатком, бездротове управління електронікою, установка одного пульта для всіх пристроїв (завжди мріяв позбутися від нескінченної кількості пультів).

Мультимедіа – бездротове аудіо / відео, спостереження та інше.

Безпека – напевно, один з найбільш важливих аспектів при виборі розумного будинку.

Клієнт може встановити охоронну сигналізацію, світлову / звукову сигналізацію, створити імітацію присутності господарів, додати функцію «паніка» та інше.

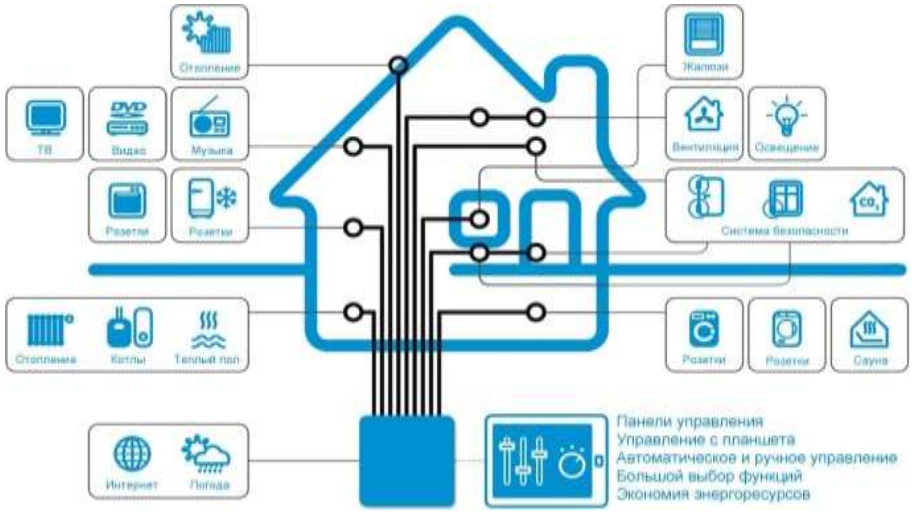


Рис. 11.6. Компоненти «розумного будинку»

«Розумний будинок» являє собою автоматизовану систему управління різними компонентами домашньої інфраструктури.

За допомогою спеціального обладнання, система може розпізнавати типові ситуації і реагувати на них, підключаючи ті чи інші компоненти. При цьому, «розумний дім» повністю контролює роботу кожного приладу і не допускає нераціонального їх використання.

Таким чином, за рахунок «синергетичного ефекту», розумний будинок дозволяє забезпечити оптимальний режим використання всієї сукупності приладів в будинку. А це дозволяє створити максимально комфортні умови проживання людей при максимально економному споживанні ресурсів [4].

Вся система «розумний будинок» складається з трьох основних підсистем:

Точка управління. Сучасні технології дозволяю забезпечити управління компонентами системи за допомогою самих різних пристроїв. Це може бути як простий вимикач, так і *Touch*-панель або *iPad*. Крім того, управління компонентами системи можна здійснювати за

допомогою голосу або бавовни долонями. Дистанційне керування забезпечується за допомогою мобільного телефону, SMS та інших подібних рішень.

Центральний контролер. Це, власне, головний мозок всієї системи. Саме сюди надходить вся інформація про роботу того чи іншого пристрою. Крім того, центральний контролер отримує і обробляє команди, одержувані від точок управління. Завдяки функціям центрального контролера став можливий ефективний контроль гармонійної роботи всіх приладів в будинку, починаючи від лампочки, до систем вентиляції або опалення.

Виконуючий пристрій. Під цим терміном розуміється вся сукупність приладів і систем в будинку. Це можуть бути, як прості прилади, на зразок мікрохвильової печі або музичного центру, так і вельми складні інтелектуальні системи, на зразок системи опалення або системи відеоспостереження.

Як правило, дана система забезпечує взаємодію кількох систем, інтегрованих в єдину систему управління всіма приладами і комунікаціями будинку. При цьому, найбільш частими компонентами системи «розумний будинок» є такі системи:

Електроживлення будинку. Розумний будинок контролює наявність електроживлення всіх інших систем в будинку. У разі необхідності, він самостійно задіє джерела безперебійного живлення і, в разі необхідності, додаткові генеруючі потужності.

Освітлення. Оптимальне використання освітлювальних приладів, з урахуванням рівня природного освітлення дозволяє забезпечити максимальну економію електричної енергії. Крім того, система забезпечує оптимальні умови для комфортного проживання людей.

Температура, вологість і своєчасне надходження свіжого повітря. Датчики, що вимірюють вищевказані параметри дають команду систем опалення, вентиляції та кондиціонування в автоматичному режимі. А це означає, що «розумний будинок» завжди підтримує оптимальні параметри повітря в приміщенні.

Управління побутовою технікою. Всі прилади, що працюють в будинку, можуть бути об’єднані в єдину мережу. Завдяки цьому, центральний контролер має можливість оптимально організувати роботу відеотехніки і кухонних приладів, систем підігріву ступенів і приводів автоматичних воріт.

Безпека. Сюди входять такі системи, як обмеження доступу в будинок небажаних осіб, контроль витоку газу, сигналізація і відеоспостереження та інші системи, що дозволяють контролювати рівень безпеки в будинку. Крім того, розумний будинок може забезпечити віддалене інформування про будь-якому інциденті в приміщенні, під час відсутності людей і навіть зімітувати їх присутність.

Слід зауважити, що в кожному конкретному випадку не обов’язкова наявність всіх вищевказаних систем. Технологія «розумний дім» відрізняється гнучкістю, і може бути оптимізована під конкретні вимоги певного клієнта.

Рис. 11.7. Система розумний будинок

"Розумний будинок" включає роботу з такими системами оснащення будівель:

1. Електротехнічні роботи

1.1. Освітлення

- Механічне керування
- Дистанційне керування
- Керування рівнем освітлення
- Розумні сценарії (реагування на природне освітлення, рух, тощо)

1.2. Силова проводка (Електрика, розетки звичайні та силові)

- Силові розетки (духовка, бойлер, мікрохвильовка тощо)
- Дистанційне керування
- Контроль розеток в дитячих кімнатах.

1.3. Електрощитова

- Блоки безперебійного живлення
- Стабілізація напруги
- Захист від пожежі
- Захист від ураження
- Захист від обриву нуля
- Контроль над споживанням

1.4. Слабовольтні мережі, датчики контролю

- Температури
- Вологості
- Руху
- Освітлення
- Гази/повітря

2. Контроль Опалення/Вентиляція

- Газ
- Котельна
- Твердопаливний котел

3. Безпека

4. Відеоспостереження

- Закритий/відкритий контур

5. Мультимедія/розваги

6. Керування шторами

7. Захист від протікання води

8. Керування голосом

9. Самонавчання

10. Інтеграції із сервісами (календар, будильник, знаходження по GPS)

11. Інтеграція із сучасною побутовою технікою

12. Підтримка сучасних стандартів і протоколів розумного будинку (KNX, ZigBee, і ін.)

13. Контроль на замками

14. Енергозбереження

15. Датчик шуму

16. Центральний порохотяг

11.2. Загрози «розумного будинку»

Експерти наполегливо заявляють про те, що постачальники послуг і пристроїв ринку IoT порушують принцип наскрізної інформаційної безпеки (ІБ), який рекомендований для всіх ІКТ-продуктів і послуг. Згідно з цим принципом, ІБ повинна закладатися на початковій стадії проектування продукту або послуги і підтримуватися аж до завершення їх життєвого циклу.

Але що ж ми маємо на практиці? Ось, наприклад, деякі дані досліджень корпорації HP (літо 2014 роки), метою яких було не виявити якісь конкретні небезпечні інтернет-пристрої і викрити їх виробників, але позначити проблему ІБ-ризиків в світі IoT в цілому [5].

Дослідники HPE звертають увагу на проблеми як на стороні власників пристроїв, так і на проблеми, над якими повинні подумати розробники. Так, на самому початку експлуатації користувачеві обов'язково потрібно замінити фабричний пароль, встановлений за замовчуванням, на свій особистий, оскільки фабричні паролі однакові на всіх пристроях і не відрізняються стійкістю. На жаль, роблять це далеко не всі. Оскільки не всі прилади мають вбудовані засоби ІБ-захисту, власникам також слід подбати про встановлення зовнішнього захисту, призначеної для домашнього використання, з тим щоб інтернет-пристрою не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди.

В ході проведеного HP дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротової трафік. Веб-інтрефейс 60% пристроїв експерти HP порахували небезпечним через небезпечну організацію доступу і високих ризиків міжсайтового скриптинга. У більшості пристроїв передбачені паролі недостатньою стійкості. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома.

Всього ж фахівці HP нарахували близько 25 різних вразливостей в кожному з досліджених пристроїв (телевізорів, дверних замків, побутових ваг, домашніх охоронних систем, електророзеток ...) і їх мобільних і хмарних компонентах.

Висновок експертів HP невтішний: безпечної екосистеми IoT на сьогоднішній день не існує. Особливу небезпеку речі Інтернету таять в собі в контексті поширення цільових атак (APT). Варто тільки зловмисникам проявити інтерес до будь-кого з нас, і наші вірні помічники зі світу IoT перетворюються в зрадників, нарозхрист відкривають доступ в світ своїх власників.

Слабкі місця IoT:

- *перехід на IPv6;*
- *живлення датчиків;*
- *стандартизація архітектури і протоколів, сертифікація пристроїв.*
- *інформаційна безпека;*
- *стандартні облікові записи від виробника, слабка аутентифікація;*
- *відсутність підтримки з боку виробника для усунення вразливостей*
- *важко або неможливо оновити ПЗ і ОС;*
- *використання текстових протоколів і непотрібних відкритих портів;*
- *використовуючи слабкість одного гаджета, хакеру легко потрапити у всю мережу;*
- *використання незахищених мобільних технологій;*
- *використання незахищеною хмарної інфраструктури;*
- *використання небезпечного ПЗ.*

Рис. 11.8. Загрози «розумного будинку»

Оскільки Інтернет речей продовжує інтегрувати, здавалося б, безглузді і незв'язані об'єкти, то повноцінна домашня операційна система виглядає цілком вірогідною. Хоча це перетворить Ваш будинок в оптимізований життєвий простір, повністю призначений для забезпечення Вашого комфорту, тим не менш, вона може також нести Вам серйозні ризики стати жертвою кібер-атаки в Вашому власному будинку.

Центральна ланка будь-якої системи безпеки розумного будинку майбутнього - це його замок. До речі, недавнє дослідження показало, що розумні замки лякаюче легко можна зламати, в результаті чого вони не можуть гарантувати виконання своєї основної функції, для якої, власне кажучи, вони й існують.

Існуючі системи досить прості для кібер-хакерів і не є перешкодою для того, щоб проникнути в Ваш будинок. А що якщо далі хакери в майбутньому зможуть використовувати це технологічне досягнення проти Вас? Якщо розумний замок можна зламати, щоб його відкрити, можливо, хакери знайдуть спосіб, як повністю його закрити, щоб Ви не могли його відкрити. В цьому випадку в майбутньому можна буде досить тихо проникати в чужий будинок: хакер зможе контролювати всі події віддалено. Більш того, він зможе вимагати у своїх жертв який-небудь розумний викуп за те, щоб вони могли потрапити в свої власні будинки. До речі, це може бути ідеєю для сценарію якого-небудь страшного фільму (Зовсім один вдома), але це жахлива думка. Якщо всі Ваші пристрої безпеки взаємопов'язані, то кібер-злочинці потенційно могли б отримати доступ також до Вашої домашньої сигналізації і навіть ключів від Вашого автомобіля.

Задимлений екран - тривога про пожежу. Одна функція безпеки, яка вже вбудована в деякі доступні на ринку детектори диму, - це можливість, що дозволяє розумному будинку отримувати інформацію (і використовувати її в подальшій роботі) від інших смарт-пристроїв, що дозволяє системі реагувати відповідним чином в разі небезпеки. Ця функція впроваджена для безпеки користувача, дозволяючи домашній системі, яка виявила пожежу, наприклад, розблокувати всі двері в будинку, щоб допомогти вибратися з нього якомога швидше. Це відмінний приклад того, як виробники IoT-рішень працюють над прозорою інтеграцією і взаємодією смарт-пристроїв всередині розумного будинку.

Однак є одне застереження: якщо ця технологія буде використовуватися кібер-злочинцями, то існує ймовірність створення небажаної ланцюгової реакції, яка в кінцевому підсумку може, навпаки, знизити рівень безпеки розумного будинку.

Ще один спосіб, коли хакер міг би потенційно здалеку нашкодити, - цестворення хибної тривоги про пожежу, яка відправляється в пожежні служби. Хаотична сцена може виглядати у вигляді задимленого екрану, що також в результаті може зробити Вас легкою здобиччю для інших потенційно шкідливих кібер-атак.

Чи можна використовувати IoT-пристрої для кібер-атаки? Легко. Зловмисники, як правило, працюють на маси: наприклад, розподілені атаки на відмову в обслуговуванні (DDOS), коли тисячі електронних листів або запитів відправляються на якийсь сервер, щоб уповільнити його роботу або взагалі вивести його з ладу. В цьому випадку в майбутньому ми можемо зіткнутися з ситуаціями, коли хакери спробують «завалити» якомога більше машин в надії на те, що якась їх частина буде працювати неправильно, що призведе до тяжких наслідків. Взагалі-то, лякає така перспектива. Можливо, саме з цієї причини урядові органи говорять про потенційні небезпеки Інтернету речей, пов'язаних з кібер-атаками.

Остерігайтеся холодильника. В мультсеріалі «Сімпсони» був епізод, коли Мардж нападає на домашню операційну систему з штучним інтелектом, яка готує їжу, але таємно планує «позбутися» від інших членів сім'ї. Звичайно, це кумедна пародія, але бентежить те, що нам буде потрібно всього кілька технологічних досягнень, щоб ці події вже перестали бути смішними, а опинилися жахливою дійсністю. Добре, припустимо, що Ваш холодильник поки не веде з Вами інтелектуальних бесід, і вже тим більше, не опрацьовує якісь вбивчі схеми щодо Вашої родини. Однак ще два роки тому ЦРУ відзначили загрозу з боку смарт-холодильників в розумних будинках. До чого б це? ЦРУ заметушилося від того, що холодильник використовувався як частина бот-мережі для виконання DDOS-атаки. І все це відбувалося зовсім непомітно для господаря цього холодильника, який навіть і гадки не мав про те, що його смарт-пристрій може виконувати якісь диявольські дії, крім як охолоджувати і зберігати їжу.

Сертифікація пристроїв IoT для захисту від хакерів. 11 жовтня 2016 року стало відомо про плани Єврокомісії - ввести обов'язкову сертифікацію або іншу аналогічну процедуру всіх приладів, що підключаються до інтернету речей. Передбачається вжити заходів на державному рівні, що повинно перешкодити хакерам використовувати інтернет речей для створення ботнетів. Як варіант, не виключається установка на пристрої мережі спеціальних уніфікованих чіпів, які убезпечать їх від атак хакерів. Ці заходи, на думку чиновників Єврокомісії, повинні підвищити рівень довіри до інтернету речей в суспільстві і перешкодити хакерам створювати ботнети з підключається техніки [4].

«Заходи щодо захисту інтернету речей від хакерів слід приймати саме на державному рівні, оскільки в контролі потребують не тільки самі прилади, а й мережі, до яких вони підключені, а також хмарні сховища. Схема сертифікації інтернету речей можна порівняти з європейською системою маркування енергоспоживаючих товарів, прийнятої в 1992 році.

Маркування є обов'язковою для автомобілів, побутової техніки та електричних ламп. Але виробники техніки вважають систему подібної маркування неефективною для захисту від хакерів. Замість цього вони вважали за краще б встановити в прилади стандартний чіп, який буде відповідати за безпеку підключення до інтернету.» - *Тібо Клейнер (Thibault Kleiner),* заступник європейського комісара з цифрової економіки та суспільству.

До групи приладів, що підключаються до інтернету, входять відеокамери, телевізори, принтери, холодильники та інша техніка. Велика частина цих пристроїв незадовільно захищена від хакерських атак. Самі по собі ці пристрої можуть не подавати інтересу для злочинців. Однак хакери зламують їх, щоб використовувати в якості роботів для створення ботнетів, за допомогою яких можна атакувати більш серйозні системи. Більшість власників зламаних пристроїв навіть не підозрюють, як використовується їхня техніка.

Як приклад наведена масштабна DDoS-атака на інтернет-ресурс *Krebs On Security*, в вересні 2016 року. «Інтенсивність запитів від ботнеті під час атаки досягла 700 Гб / с. У складі ботнету більш 1 млн камер, відорегістраторов та інших підключених до інтернету речей пристроїв. Це не перший резонансний випадок, коли подібні пристрої стають

частиною ботнету, проте вперше мережа складалася майже повністю з таких приладів.» - *Брайан Кребс (Brian Krebs),* власник ресурсу.

За даними Gartner, до інтернету речей підключено близько 6 млрд приладів, а до 2020 року їх число досягне 20 млрд, що створить хакерам ширші можливості для проведення масштабних атак за допомогою ботнетів.

У споживачів немає впевненості в безпеці пристроїв IoT. Компанія Gemalto оприлюднила в жовтні 2017 року статистику: виявляється, 90% споживачів не довіряють безпеці пристроїв Інтернету речей. Ось чому понад дві третини споживачів і майже 80% організацій підтримали уряди, що беруть заходи щодо забезпечення безпеки IoT.

Основні побоювання споживачів (згідно двом третинам респондентів) стосуються хакерів, які можуть встановити контроль над їх пристроєм.

Фактично, це викликає більше занепокоєння, ніж витік даних (60%) і доступ хакерів до особистої інформації (54%). Незважаючи на те, що пристроями IoT володіє більше половини (54%) споживачів (в середньому, по два пристрої на людину), тільки 14% вважають себе обізнаними про безпеку цих пристроїв. Така статистика показує, що як споживачам, так і підприємствам, необхідно додаткову освіту в даній сфері.

Фактично, майже кожна організація (96%) і кожен споживач (90%) відчувають необхідність в правилах щодо забезпечення безпеки Інтернету речей, прийнятих на рівні уряду.

Контроль над смарт-пристроями. Уразливість в мобільному і хмарному додатках *LG SmartThinkQ* дозволили дослідникам *Check Point* віддалено увійти в хмарний додаток *SmartThinQ*, і, заволодівши обліковим записом *LG,* отримати контроль над пилососом і вбудованої в нього відеокамерою.

Отримавши контроль над обліковим записом конкретного користувача *LG*, зловмисник може контролювати будь-який пристрій *LG* або пристрій, пов'язаний з цим обліковим записом, включаючи пилососи, холодильники, плити, посудомийні і пральні машини, фени та кондиціонери, розповіли в компанії. Уразливість HomeHack дає хакерам можливість стежити за сімейним життям користувачів за допомогою відеокамери робота-пилососа *Hom-Bot*, яка в режимі реального часу надсилає відео в додаток *LG SmartThinQ* в рамках функції *HomeGuard Security*. Залежно від моделей пристроїв *LG* зловмисники можуть також включати і відключати посудомийні або пральні машини. Наразі таку уразливість усунено.

11.3. Атаки на «розумний будинок»

Очевидно, що «розумний дім» знаходиться в небезпеці, оскільки, крім проводових загроз існують атаки по безпроводовим мережах і тому є більш уразливими, в наслідок використання відкритого середовища в якості носія даних і широкомовної природи безпроводових з'єднань.

Пасивні атаки

Аналіз трафіку і прослуховування комунікаційного каналу неавторизованими особами класифікується як пасивна атака. Атаки, націлені виключно на отримання передаються даних є пасивними по своїй натурі. Найбільш частими є наступні види атак спрямовані на порушення конфіденційності даних:

- *Моніторинг і прослуховування*. Даний вид атаки зустрічається найбільш часто. За допомогою підслуховування зловмисник може з легкістю отримати доступ до передається даними. При передачі контрольної інформації про конфігурацію мережі, дана техніка може становити найбільшу небезпеку для конфіденційності даних.
- *Аналіз трафіку.* Навіть коли інформація передається в зашифрованому вигляді, залишається ймовірність використання зловмисником техніки аналізу комунікаційних патернів. Активність сенсорів потенційно може розкрити досить інформації для нанесення зловмисником шкоди сенсорної мережі.

Рис. 11. 9. Класифікація атак

Активні атаки

Різні модифікації даних під час комунікації, здійснювані неавторизованими особами, класифікуються як активні атаки. Нижче надаються описи активних атак.

Атаки маршрутизації

Атаки, які здійснюються на мережевому рівні (network layer) моделі OSI називаються атаками маршрутизації. Наступні атаки маршрутизації зустрічаються найбільш часто:

Змінена маршрутна інформація. Найбільш схильні до даної атаки децентралізовані мережі, де кожен вузол є маршрутизатором і відповідно може змінювати маршрутну інформацію. Внаслідок даної атаки можуть відбуватися закільцьовування маршруту, збільшуватися час пакета даних в шляху до точки призначення і т. д.

Вибіркова розсилка. Скомпрометований вузол сенсорної мережі може вибірково видаляти певні пакети. Особливо ефективною дана атака може бути в комбінації з атаками, які збирають велику кількість трафіку на одному вузлі мережі. В результаті даної атаки серйозно страждає цілісність і доступність даних, що може істотно знизити рівень сервісу, що надається сенсорної мережею.

Атака «бездонна воронка» (*Sinkhole Attack*). Дана атака характерна тим, що скомпрометований вузол мережі починає діяти подібно воронці, використовуючи весь трафік сенсорної мережі. Особливо в мережах з протоколом маршрутизації, заснованому на широкомовній розсилці, зловмисник «слухає» запити на маршрути і відповідає сенсорним вузлам, що «знає» найкоротший маршрут до базової станції.

Як тільки скомпрометованому вузлу вдалося встати між сенсорним вузлом, що транслює і базовою станцією, він може виробляти будь-які дії з пакетами даних, що надходять.

«*Шаманська атака» (Sybil attack).* Під час даної атаки один скомпрометований вузол може використовувати кілька псевдо ідентифікаторів, видаючи себе відразу за кілька вузлів. Подібні атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі і т. д. По суті будь-яка мережа з рівноправними вузлами (особливо бездротові і децентралізовані мережі) є схильною до даної атаки [5].

Атака (Wormhole attack). Дана атака передбачає створення спеціального шляху між двома і більше скомпрометованими вузлами сенсорної мережі для передачі по ним перехоплених пакетів, доступних тільки для атакуючої системи. Подібні атаки представляють серйозну загрозу безпеці сенсорної мережі тому, що не вимагають компрометації вузла сенсорної мережі. Тоді коли вузол В (базова станція або звичайний

вузол) використовує широкомовну розсилку для запиту маршруту, зловмисник отримує даний запит і перенаправляє його до найближчого сусіда. Будь-який вузол, який отримав подібний перенаправлений запит розглядає себе як вузол, що знаходиться в зоні досяжності вузла В і запам'ятовує вузол В як свого «батька». Навіть якщо цей вузол знаходиться на великій відстані від вузла В і його відокремлюють від вузла В безліч сенсорних вузлів, він буде розглядати вузол В як наступний від себе [6].

Флуд атака (HELLO flood attack). Дана атака є широкомовною атакою, покликаною направити в сенсорну мережу масу необов'язкових повідомлень, які повинні позбавити мережу різноманітних ресурсів - канальної ємності, обчислювальної потужності, енергетичних ресурсів і т.д. Під час подібної атаки зловмисник за допомогою високочастотного радіопередавача з достатньою обчислювальною потужністю розсилає Hello пакети до безлічі вузлів сенсорної мережі. Вузли, які отримали Hello пакети, розглядають скомпрометований вузол як свого сусіда. Під час наступної передачі даних, вони будуть використовувати отриманий адресу з Hello пакетів для відправки. Таким чином, зловмисник отримає доступ до даних.

Інші атаки

Відмова в обслуговуванні.

Даний вид атаки може бути результатом ненавмисного виходу з ладу вузлів сенсорної мережі або ж результатом дій зловмисників. Найпростіша атака такого роду спрямована на витрату всіх ресурсів, доступних скомпрометованому вузлу за допомогою відправки непотрібних пакетів даних, таким чином перешкоджаючи легітимним користувачам мережі отримувати призначені їм сервіси і ресурси. Дана атака має на увазі не тільки спроби зловмисника зруйнувати мережу або розірвати з'єднання, але і будь-яка подія, що знижує здатність мережі надавати певні послуги і ресурси. Безліч типів подібних атак може бути здійснено на різних рівнях моделі OSI.

Захоплення вузла (node subversion)

Захоплення вузла зловмисником може спричинити розкриття важливої інформації, наприклад, криптографічних ключів, що в свою чергу може спричинити компрометацію всієї сенсорної мережі [5].

Несправність вузла (malfunction)

Несправний в результаті атаки вузол генерує невірні дані, що може порушити цілісність сенсорної мережі, особливо, якщо несправний вузол є вузлом, що агрегує дані, наприклад, головним вузлом кластера.

Простій вузла / вихід з ладу

Простій вузла або його вихід з ладу трапляється тоді коли вузол перестає функціонувати. У разі виходу з ладу головного вузла кластера, протокол сенсорної мережі повинен бути здатний надати альтернативний маршрут для пакетів даних.

Фізичні атаки

Вузли мережі часто встановлюються в середовищах із зовнішніми впливами. В таких середовищах маленький впливаючий фактор вузлів сенсорної мережі в поєднанні з відсутністю постійного нагляду за ними робить їх схильними до різних фізичних атак. На відміну від інших видів атак, фізичні атаки руйнують сенсори незворотньо.

Спотворення повідомлення

Будь-яка зміна контенту повідомлення зловмисником неминуче компрометує цілісність передачі даних.

Хибний вузол

Даний вид атак передбачає впровадження в мережу вузла, який посилає вузлів сенсорної мережі некоректні дані. Дана атака є однією з найбільш небезпечних атак, оскільки запроваджений вузол, який поширює зловмисний код, може привести до загибелі всю сенсорну мережу.

Копіювання вузла мережі

Концептуально дана атака полягає в наступному: зловмисник намагається впровадити заздалегідь підготовлені вузли в існуючу сенсорну мережу, використовуючи ідентифікатори вже існуючих вузлів в даній мережі. Для цього зловмисник фізично захоплює один вузол мережі з метою отримання його унікальних даних. Отримані дані згодом використовуються для конфігурації заздалегідь підготовлених вузлів, які згодом стають клонами захопленого вузла. За допомогою впровадження реплікованих вузлів в певні точки мережевий топології зловмисник може з легкістю управляти сегментом мережі [6].

Алгоритм надання захисту системи “Розумний будинок”

1. Стандартизація: мережа IoT в даний час є переважно бездротовою, це робить безпеку набагато складнішою, ніж традиційні дротові мережі через різноманіття нових протоколів і стандартів щодо радіочастот та радіозв'язку. Пристрої та система в цілому має відповідати стандартам, щоб забезпечити безпеку вашої системи та не зробити її уразливою для злочинців.
2. Сертифікація пристроїв/перевірка справжності: окрім відповідності стандартам, необхідно забезпечувати складові мережі сертифікатами, що видаються центрами сертифікації, для можливості перевірки пристроїв, що бажають проникнути в Вашу мережу та можуть їй зашкодити. Така перевірка допомагає проаналізувати певний пристрій на реєстрацію в своєрідній базі та надасть інформацію стосовно якості і можливості нанести збитки.
3. Аутентифікація: пристрої IoT повинні бути законними користувачами. Методи досягнення такого роду аутентифікації від статичних паролів до двофакторної аутентифікації, біометрії та цифрових сертифікатів. Унікальним для IoT є те, що пристрої(наприклад, вбудовані датчики) повинні розпізнати інші пристрої. Саме це зменшує ймовірність проникнення чужорідного тіла в системі.
4. Шифрування: необхідне для запобігання несанкціонованого доступу до даних. Це важко забезпечити через розмаїття пристроїв IoT та апаратних профілів. Проте шифрування має бути частиною повного процесу управління безпекою. На сьогоднішній день вчені сперечаються з приводу надійності того чи іншого варіанту та використання його в IoT, проте вже розроблений чіп для шифрування на еліптичних кривих, що може застосовуватися в пристроях Інтернету речей.
5. Захист інтерфейсу: більшість виробників обладнання та програмного забезпечення надають доступ до пристроїв через програмний інтерфейс(API). Їх забезпечення вимагає наявності аутентифікації та авторизації пристроїв, які потребують обміну даними. Тільки авторизовані пристрої, розробники та програми здатні здійснювати зв'язок між захищеними пристроями.
6. Механізми доставки: потрібні постійні оновлення та патчі, необхідні для подолання мінливої тактики кібератакерів. Це вимагатиме знань у патчах, що виправлятиме прогалини в критичному програмному забезпеченні на льоту.
7. Аналітика безпеки та прогнозування загроз: необхідно не лише стежити та контролювати дані пов'язані з безпекою, а також використовувати їх для прогнозування майбутніх загроз. Вони повинні доповнювати традиційні підходи, які шукають дії, що виходять за рамки встановленої політики.
8. Контроль доступу: якщо який-небудь компонент скомпрометовано, контроль гарантує, що вторгнення матиме мінімальний доступ до інших частин системи, наскільки це можливо [6]. Механізми контролю доступу на базі пристроїв аналогічні мережевим системам, навіть якщо хтось зможе вкрасти корпоративні облікові дані для входу в систему, скомпрометована інформація буде обмежуватися лише тими областями мережі, де вона авторизована.
9. Фізична безпека: окрім безпеки внутрішньої, мережі необхідний захист ззовні, тобто, наприклад, якщо це датчик, то він має бути розміщений таким чином, щоб зловмисник не мав до нього прямого фізичного доступу і був непомітний для нього.

Контрольні питання до розділу

1. Наведіть складові «розумного будинку».
2. У чому олягають переваги «розумного будинку»?
3. На які групи за типом використання Інтернету можливо поділити більшість побутових пристроїв з категорії «розумних» речей ?
4. На які компоненти можна розділити всю систему «розумного будинку»?
5. З кількох основних підсистем складається вся система «розумний будинок»? Назвіть та дайте характеристику кожній з них.
6. Які системи є найбільш частими компонентами системи «виконуючий пристрій» розумного будинку?
7. Які існують загрози «розумного будинку»?
8. Наведіть слабкі місця IoT, які можуть становити загорозу «розумному будинку».
9. Пасивні атаки на «розумний будинок». Дайте характеристику кожній з них.
10. Активні атаки на «розумний будинок». Дайте характеристику кожній з них.
11. Інші типи атак на розумний будинок.
12. Алгоритм надання захисту системи “розумний будинок”. В чому він полягає? Його особливості.

Список рекомендованої літератури

1. Информационная безопасность интернета вещей (Internet of Things) //електрон. текст. Дані URL:http://www.tadviser.ru/index.php/Статья:Информационная_безопасность интернет_вещей_(Internet_of_Things)
2. Богуслав А.М. Методи та моделі забезпечення захисту безпроводних сенсорних мереж// електрон. текст. Дані URL: http://er.nau.edu.ua/bitstream/NAU/22464/2/diser_ua_2.0.pdf
3. Орешкина Д. Эталонная архитектура безопасности интернета вещей // Часть 1. електрон. текст. Дані URL: https://www.anti- malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1
4. Орешкина Д. Эталонная архитектура безопасности интернета вещей //Часть 2. електрон. текст. Дані URL: https://www.anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2
5. John Blyler 8 Critical IoT Security Technologies // електрон. текст. Дані URL: https://www.electronicdesign.com/industrial-automation/8-critical-iot-security-technologies
6. Security in the internet of things // електрон. текст. дані URL: Sehttps://www.windriver.com/whitepapers/security-in-the-internet-of- things/wr_security-in-the-internet-of-things.pdf

РОЗДІЛ 12. SMART CITY

12.1. Класифікація Smart City

Smart City є предметом обговорення протягом багатьох років, і багато міст в усьому світі все активніше застосовують стратегічні підходи переходу до розумного статусу [1].

«Розумне місто» – це місто, в якому традиційні системи працюють більш ефективно за рахунок використання інформаційно-комунікаційних технологій [2].

Інформаційно-комунікаційні технології дозволяють використовувати менше енергетичних ресурсів, задовольняючи незмінний обсяг потреб, та зменшувати масштаби парникової емісії. Це означає запровадження «розумнішої» системи міського транспорту, оновленої системи водопостачання та утилізації відходів, а також створення ефективніших систем опалення та охолодження будинків [3].

При цьому, всі системи між собою мають бути взаємопов'язані та працювати як єдиний злагоджений механізм. До інформаційно-комунікаційних технологій додається людський та соціальній капітал, який відповідає за підвищення безпеки громадських місць та створення зручностей для жителів [4,5].

Таким чином, концепція «розумного міста» спрямована на надання реальних переваг для життя населення та функціонування бізнесу відповідно до принципів сталого розвитку [6].

Smart City складається із цілісної концепції розумної інтеграції інформаційних і комунікаційних технологій для моніторингу та управління міською інфраструктурою.

Мета таких заходів - поліпшити життя людей за допомогою підвищення рівня комфорту і безпеки, якості та ефективності обслуговування в різних сферах, оптимізації витрат на ряд високоексплуатованих ресурсів.

Інфраструктура Smart City має на увазі цілий спектр найрізноманітніших рішень, які реалізуються за допомогою впровадження розумних технологій.

Як правило, це альтернативні підходи до енергозабезпечення та водопостачання, можливість переробляти морську солону воду в прісну, впровадження сучасних систем із сортування та переробки сміття, введення в експлуатацію не моторизованих транспортних засобів, установка широкої мережі відеоспостереження та відеоаналітики, контроль чистоти повітря.

«Розумне місто» має шість основних складових, п'ять з яких полягають у наступному:

− *«розумна економіка» (smart economy)* – електронний бізнес та електронна торгівля, зростання продуктивності, інноваційно-технологічне виробництво товарів та доставка послуг тощо;

− *«розумне переміщення» (smart mobility)* – транспортні та логістичні системи, засновані на інформаційно-комунікаційних технологіях, які б дозволяли використовувати один чи два види транспорту для переміщення у будь-яку точку міста;

− *«розумні люди» (smart people)* – розвиток електронних навичок, підвищення рівня освіченості, підвищення кваліфікації, розвиток креативності та стимуляція інноваційних проривів;

− *«розумне життя» (smart living)* – запровадження способу життя, поведінки та моделі споживання за використанням інформаційно- комунікаційних технологій, покращення здоров'я та культурний розвиток;

− *«розумне врядування» (smart governance)* – інтерактивне місцеве правління, яке забезпечує ефективне всеохоплююче функціонування міста [7].

Шостою складовою концепції «розумне місто» є *«розумне довкілля» (smart environment)*, яка має тісний зв'язок із енергетикою. Адже основний наголос робиться на запровадженні принципів енергоефективності та зменшення викидів парникових газів. Тому у межах «розумного навколишнього середовища» передбачається створення «розумної енергетики» за рахунок запровадження замкнутих енергетичних мереж, систем контролю та

моніторингу рівня забруднення, реставрації та спорудження будинків, підвищення енергоефективності високим рівнем ефективності процесів когенерації [7].

Експерт у сфері урбаністики *Білл Хатчінсон* запропонував наступну Класифікацію Smart City :

- **Smart City 1.0.** У Smart City 1.0 немає загальної стратегії розвитку розумного міста, а впровадження розумних технологій та автоматизація впроваджена в окремі, не пов'язані між собою компоненти.

Прикладом може служити запровадження безготівкового розрахунку за проїзд в окремих видах комунального транспорту.

- **Smart City 2.0.** Smart City 2.0 передбачає об'єднання, злиття і взаємозв'язок раніше незалежних компонентів: максимально великого числа різноманітних датчиків, що є джерелами інформації, а також інших розумних технологій. У такому місті можливий безготівковий розрахунок в усіх видах комунального транспорту, але не приватному чи будь якому іншому.
- **Smart City 3.0.** У Smart City 3.0 передбачено об'єднання всіх технологічних датчиків та компонентів, уся інфраструктура та життєдіяльність міста буквально просякнута розумними технологіями. У такому місті повноцінно працює електронний квиток, де можливий абсолютно безготівковий розрахунок в усіх видах транспорту через різноманітні системи оплати. Варто зазначити, що абсолютного рівня розумного управління за категорією Smart City 3.0. не ще досягнуто жодним містом у світі.

Визначення *Smart City* Європейським Парламентом (2014 р.) засновано на тих же шести пунктах. Згідно з ним, розумне місто прагне вирішити суспільні проблеми, використовуючи ІТ-рішення в діяльності різних муніципальних суб'єктів і їх партнерства.

Разом з тим Європарламент вказує на проблемний контекст: розумні міста розглядаються як відповідь на виклики масштабної урбанізації (перенаселення, споживання енергії, розподіл ресурсів, захист навколишнього середовища). Міста перетворюються в стратегічні точки для вирішення проблем бідності та нерівності, безробіття і управління енергопотоками.

Система управління *Smart City* передбачає фокус на управлінні якістю функціонування та організації об’єктів міського середовища з використанням сучасних технологій для задоволення потреб населення. Така система управління великим містом дає змогу:

– задовольняти потреби мешканців міста за рахунок підтримання на високому рівні організації та функціонування об’єктів міського середовища;

– коригувати управлінські дії залежно від фактичного рівня задоволення потреб населення, який буде визначатись опитуванням, анкетуванням та результатами обробки інформації, отриманої з різноманітних документів;

– задіяти мешканців міста, як джерело об’єктивної інформації про рівень задоволення своїх потреб, для цього потрібно, щоб мешканці відчували довіру до органів влади, а це буде тоді, коли органи влади будуть частіше і чесніше інформувати мешканців про результати своєї діяльності, радитись з мешканцями щодо доцільності тих чи інших управлінських рішень.

Система *Smart City* дає можливість на високому рівні управляти містом з використанням електронних ресурсів, впроваджувати новітні технології для покращення функціонування міста та робити механізм органів місцевої влади прозорішим, а мешканцям більше впливати на прийняття рішень у місті [9].

Отже, система *Smart City* – є системою управління муніципалітетом, яка використовує інформаційні та комунікаційні технології для збору, обробки та обміну інформацією з громадськістю, підвищення оперативності та ефективності, управління ресурсами задля покращення якості надання державних послуг та підвищення добробуту населення.

Концепція розумного міста характеризується трьома базовими параметрами:

- технологічність;
- інтелектуалізація;

- фокусування на стилі життя: «Розумне місто» повинен бути екологічним, безпечним, енергоємним, що відкриває широкі можливості і забезпечує максимально комфортну життєдіяльність.

Серед першочергових галузей, які потребують інтелектуальної модернізації, є державне управління, інфраструктура міста і економіка.

12.2. Концепції розумного міста

Таблиця. 12.1. Найважливіші напрямки розвитку «розумного міста»

Інноваційна економіка	Міська інфраструктура	Державне управління
Інновації в промисловості, кластерах, районах міста	Транспорт	Адміністративні послуги громадянам
Розумна робоча сила: Освіта і зайнятість	Енергетика / Комунальні Послуги	Представницька і пряма демократія
Створення наукомістких компаній	Захист навколишнього середовища / безпека	Послуги для громадян: якість життя

Наприклад, концепція в цих напрямках може проявляється в наступних ознаках. Інноваційна економіка повинна бути самодостатньою і незалежною від природно-вуглецевих ресурсів.

У міській інфраструктурі необхідно впроваджувати економні і поновлювані джерела енергії. У державній гілки повинна вестися робота по підвищенню конкурентоспроможності капіталу, як фінансового, так і інтелектуального і людського.

Сьогодні людство становить близько 7,4 млрд осіб, майже половина – 3,6 млрд, вже проживає в містах, хоча ще 10 років тому частка міського населення становила близько 35%. При таких високих темпах урбанізації навантаження, створювана на міські служби, найчастіше виявляється непосильним.

Для вирішення цієї проблеми і були розроблені концепції розумних міст.

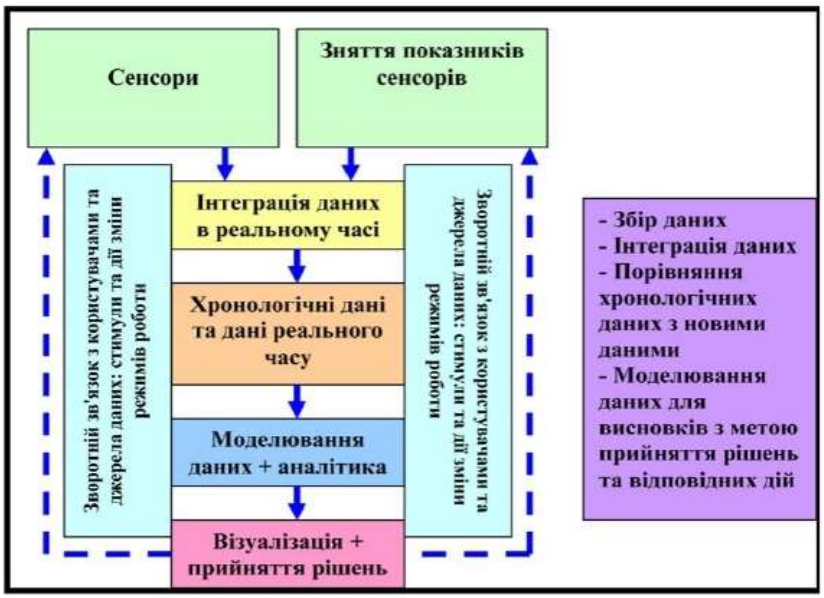


Рис. 12.1. Загальна схема розумного міста

Головне завдання проектів «Розумне місто» – підвищення ефективності всіх міських служб. Концепція отримала досить широке поширення, на разі Розумні технології в тому чи іншому обсязі реалізовані в 2500 містах по всьому світу.

Концепція розумного міста ґрунтується на шести його характеристиках:

- розумна економіка, розумна мобільність, розумне навколишнє середовище, розумні люди, розумне проживання, «розумне управління.

- Розумна Економіка має на увазі економіку, засновану на високотехнологічних галузях промисловості, які включають ІКТ та ті галузі промисловості, які використовують ІКТ на різних стадіях виробничого циклу.
- Розумна мобільність передбачає стійкі, інноваційні та безпечні транспортні системи на основі ІКТ-інфраструктури, які покращують міський рух і мобільність міських жителів у повсякденному міському житті.
- Розумні люди – це жителі міста, які володіють високим рівнем освіти і кваліфікації та активно інтегровані в громадське життя міста.
- Розумне навколишнє середовище включає в себе привабливі для життя природні умови, а також реалізацію заходів щодо охорони навколишнього середовища.
- Розумне проживання означає високий рівень розвитку різних складових феномена якості життя (культура, охорона здоров'я, безпека, житло, туризм).
- Розумне управління – це управління диверсифіковане. Делегування функцій і диверсифікація влади є основою соціальної взаємодії соціальних інститутів у розумному місті. В практичному аспекті концепція розумного міста повинна бути розглянута, насамперед, з управлінської точки зору у мегаполісах, що володіють великими соціальними, економічними, технологічними, інфраструктурними можливостями та мають перспективу розвитку як розумне місто.

12.3. Основні складові Розумного міста

Основні складові Розумного міста:

- інтелектуальна транспортна система (ІТС). Яка оптимізує рух транспорту шляхом відображення дорожньої ситуації на вуличних інформаційних панелях і смартфонах користувачів, підказує їм оптимальний маршрут і несе в собі безліч інших корисних функцій:

- *геоінформаційна (ГІС).* Служить загально географічною підкладкою для всіх підсистем Розумного міста.

- *електронна поліція (ePolice).* Працює в такий спосіб: при будь-якому дзвінку на пульт «електронної поліції» на карті ГІС відображається місце розташування абонента, а на моніторі чергового відкривається вікно для реєстрації повідомлення, його подальшої обробки і прийняття оперативних заходів.

- *електронна освіта (eEducation).* Вона дозволяє студенту бути присутнім на лекції, сидячи за власним комп'ютером у зручному для себе місці. Учень буде точно також слухати лекцію, бачити викладача і стежити за його записами на електронній дошці в аудиторії. Студент навіть може віртуально «підняти руку» і задати питання викладачеві. Всі записані лекції зберігаються для подальшого перегляду і закріплення матеріалу.

- *електронна охорона здоров'я (eHealth)*. Ця функція спростить процес електронного запису до лікаря. Основою системи є єдина електронна база пацієнтів. У цій базі відразу може ознайомитися з тим, які аналізи робилися, яке лікування призначалося в інших клініках. Система відеоконференцзв'язку з ефектом присутності (Telepresence) допоможе провести консиліум фахівців, розглянути в деталях результати МРТ і рентгенографії, а також зробити операцію під віддаленим керівництвом хірурга.

В архітектурі розумного міста можна виділити кілька рівнів і принципів, пов'язаних з ефективним управлінням, оптимальним використанням ресурсів, інформаційною підтримкою і комплексним використанням інформаційних ресурсів, аналізом і моніторингом середовища та програм розвитку, візуалізацією даних і проектів, прогнозуванням.

Концепція *Розумного міста* нерозривно пов'язана з екологічною сертифікацією будівель і споруд міста. Останні два десятиліття в усьому світі відзначається підвищення попиту на екологічне житло, офісні будівлі і промислові об'єкти.

Відповідно існують і екологічні нормативи, які формулюють умови створення та експлуатації екологічних будівель. Методи сертифікації будівель, в яких досить широко використовуються і засоби ГІС, дозволяють швидко й наочно дати оцінку еко-ефективності об'єкта. А в цілому гео-інформаційні системи та системи «*Facility Management*» (FM –

управління заданими бізнес властивостями активів; управління інфраструктурою об’єкта або організації) на базі ГІС відіграють провідну роль при реалізації концепції розумного міста.

До того ж, під «містом» у широкому сенсі можуть розумітися як власне населені пункти, так і інші великі територіально розподілені структури та інфраструктурні об’єкти. Так, яскравим прикладом практичного втілення концепції розумне місто може служити реалізація аеропорту Пекіна, як складного об’єкта, багато в чому схожого з цілим містом і виконує багато сучасних бізнес функцій, наприклад такі, як: реалізація потреб бізнесу працювати швидше, зручніше і дешевше на основі розвиненої логістичної інфраструктури з яскраво вираженим зонуванням території, надання можливостей проживання, покупок, проведення ділових зустрічей, організації виставок. ГІС є однією з технологій практичного застосування концепції *Розумне місто*. Це технологічна платформа корпоративного класу, що дозволяє зрозуміти просторові взаємозв’язки і вирішувати складні питання адміністративно-господарського управління.

Крім того, сучасна ГІС, така, наприклад, як повнофункціональна система Esri ArcGIS, є унікальним сховищем різнорідної інформації. Вона дозволяє створювати детальні 3D-моделі об’єктів і місцевості, отримувати точні геометричні параметри даних моделей, у наочній формі відобразити стан, поведінку і взаємозв’язок об’єктів нерухомості. Крім цього, вона дозволяє виконувати просторові запити, оптимально визначати розташування об’єктів інфраструктури (парковок, входів-виходів, в’їздів, систем безпеки, інженерних і комунікаційних систем), виявляти існуючі критичні відхилення від вимог, спрогнозувати розвиток надзвичайної ситуації. ГІС і FM-технології в рамках концепції Розумного міста забезпечують комплексний підхід до вирішення містобудівних завдань за рахунок інтеграції просторової і тимчасової інформації, містобудівних регламентів, об’єктивних та актуальних даних про об’єкти містобудівної діяльності, знань і досвіду. Також ГІС і FM технології широко використовуються в оперативно-технологічному управлінні міським господарством на основі зібраних об’єктивних даних.

Розумне місто також має такі визначення, як місто знань, цифрове місто, кібермісто та екомісто – в залежності від цілей міського планування. Розумні міста в економічному і соціальному аспектах спрямовані в майбутнє. Вони ведуть постійний моніторинг найважливіших об'єктів інфраструктури – автомобільних доріг, мостів, тунелів, залізниць, метро, аеропортів, морських портів, систем зв'язку, водопостачання, енергопостачання, навіть найважливіших будівель – в цілях оптимального розподілу ресурсів і забезпечення безпеки. Вони постійно нарощують число надаваних населенню послуг, забезпечуючи стійке середовище, яка сприяє благополуччю і збереженню здоров'я городян. Основу цих послуг становить інфраструктура інформаційно-комунікаційних технологій.

Рис. 12.2. Інфраструктура розумного міста

Розумне місто повинне містити у собі такі елементи:

- розумний будинок;
- енергозбереження та безпеку;
- розумні послуги – муніципальні послуги, перекладені в електронний вигляд;

- розумна парковка – моніторинг вільних паркувальних місць в місті;
- стан конструкцій – моніторинг технічного стану конструкцій;
- розумне освітлення – інтелектуальне і адаптоване під погоду вуличне освітлення;
- управління вивезенням і переробкою відходів – спостереження за наповнюваністю сміттєвих контейнерів, сортування та утилізація відходів;
- розумні дороги – управління рухом на основі оповіщення про погодні умови, непередбачених подіях.

12.4. Технології розумних міст

Розумне місто повинне відрізнятися своєю інформаційно-технологічною спроможністю, у даній частині наведено основні інноваційні технології розумного міста:

- *Збір інформації.*

Система новітніх сенсорів і технологія відеоавтентифікації. Бездротові сенсори, що діють на суші, воді, повітрі та в космосі, роблять можливим збір широкого спектра даних, що охоплюють всі сфери міського життя. Ці дані можна ефективно візуалізувати, збирати і використовувати в самих різних ситуаціях. Наприклад, для ранньої діагностики землетрусів або для спостереження за протяжними магістралями, або для біометричного розпізнавання.

- *Автентифікація.*

Дані, отримані в ході збору інформації, автентифіковані за місцезнаходженням і терміну давності. Оскільки обсяг міських даних для автентифікації величезний, для високошвидкісної і точної обробки даних необхідно застосування найсучасніших технологій.

Тільки так можливо забезпечити високий рівень автентифікації в режимі реального часу.

- *Моніторинг*. При виявленні в ході моніторингу будь-яких відхилень, інформація відправляється в певні відомства в режимі реального часу.

Наприклад, в разі виникнення будь-якого події, дані про нього разом з відео передаються у відповідне відомство в режимі реального часу. Таким чином, система сприяє запобіганню злочину, аварії або катастроф.

- *Контроль*. Дані, отримані в ході моніторингу, аналізуються в реальному часі, а найбільш важлива інформація для контролю відбирається і передається далі. Наприклад, кондиціювання повітря в будівлях можна налаштовувати більш точно за допомогою інформації про місцезнаходження, що дозволить створити більш сприятливу атмосферу для людей, які в них працюють.

- *Хмарні обчислення*. Надійна система резервного копіювання, здатна перенести локальні катастрофи, може надавати необхідну для аналізу інформацію. Більш того, для служб, зміст яких змінюється зі зміною ситуації і ходом часу, можлива організація оперативного зворотного зв'язку.

- *Віртуальний світ*. Можливість виходу у цифрову “матрицю”, абсолютно безпечний огляд міста з допомогою віртуальних окуляр.

- *Квантовий комп'ютер*. Квантовий комп'ютер – машина, яка об'єднає в собі досягнення комп'ютерної науки і квантової фізики – найскладнішого розділу сучасної науки, що вивчає елементарні частинки менше атома. Фізика цих частинок часто вступає в колізію з накопиченим академічним знанням (наприклад, суперечить теорії відносності Альберта Ейнштейна). Квантова частка може одночасно перебувати в різних місцях і в різних станах. Цей взаємовиключний з точки зору логіки принцип називається принципом суперпозиції.

У Розумних містах технології будуть проникати практично в усі сфери державного і суспільного життя, дозволяючи городянам ефективно управляти середовищем існування, починаючи від «розумних» будинків, які автоматично контролюють подачу тепла і електроенергії, температуру і вологість повітря, і закінчуючи взаємодією з бізнесом і міськими службами.

Місто стає «системою систем», заснованої на даних, оптимізованої і інтегрованою на кожному з рівнів - від індивідуальних пристроїв до будівель, міст і цілих регіонів.

12.5. Стандарти розумного міста

Стандарти відіграють дуже важливу роль у нашому житті, однак історія цього явища досить молода. Насправді, організації стандартів трохи більше, а ніж 100 років. Власне кажучи, найстарішим в світі установою подібного роду є Британський інститут стандартів (BSI), утворений в 1901 році, проте перший національний стандарт з'явився в тому ж BSI тільки в 1903 році, або точніше, був офіційно опубліковано. Народження світової системи стандартизації вже зовсім недавня історія – в 1946 році був створена Міжнародна організація по стандартизації або ISO. Власне технологічні міжнародні комітети типу IEEE ще молодше. Однак, не дивлячись на свою відносну молодість, сьогодні стандарти і сам процес стандартизації стали одним з основних факторів, що сприяють світовому розвитку, глобалізації ринків і виробництв, багато в чому визначаючи успіхи тих чи інших починань в бізнесі і навіть у політиці.

Для того щоб розглянути загальні стандарти розумного міста потрібно розглянути наступні компанії котрі розробляють ці стандарти:

- *W3C або Консорціум Всесвітньої павутини (World Wide Web Consortium, W3C)* – організація, розробляє і впроваджує технологічні стандарти для Всесвітньої павутини. Консорціум очолює *Тімоті Джон Бернерс-Лі*, автор багатьох розробок в області інформаційних технологій.
- *OGC (Open Geospatial Consortium: відкритий геоінформаційний консорціум)* – це міжнародна організація по розробці стандартів в області геоінформаційних сервісів.
- *DICOM (Digital Imaging and Communications in Medicine)* – галузевий стандарт створення, зберігання, передачі і візуалізації медичних зображень і документів обстежених пацієнтів.
- *CDISC (The Clinical Data Interchange Standards Consortium)* – це організація, що займається розробкою стандартів в галузі медичної інформації.

Цілі цілком зрозумілі – електронна карта пацієнта, яка при необхідності може бути прочитана в лобом лікувальному закладі світу.

- *OASIS (Organization for the Advancement of Structured Information Standards)* – глобальний консорціум, який управляє розробкою, конвергенцією і прийняттям промислових стандартів електронної комерції в рамках міжнародного інформаційного співтовариства. даний консорціум є лідером за кількістю випущених стандартів, що відносяться до Веб-службам.

Крім цього він займається стандартизацією в області безпеки, електронної комерції; також зачіпається громадський сектор і ринки вузькоспеціальною продукції. У OASIS входить понад 5000 учасників, що представляють понад 600 різних організацій з 100 країн світу.

- *OMG (Object Management Group)* – консорціум (Робоча група), що займається розробкою і просуванням об'єктно-орієнтованих технологій і стандартів. Це некомерційне об'єднання, розробляє стандарти для створення інтероперабельних, тобто від платформи незалежних, додатків на рівні підприємства. З консорціумом співпрацює близько 800 організацій – найбільших виробників програмного забезпечення.

Іспанські фахівці зі стандартизації також прийняли у себе стандарт ISO підномером UNE-ISO 37120 і доповнили його двома своїми стандартами UNE 178301 і UNE 178303. Однак це стандарти на тему управління міськимиактивами. 75 міст світу приєдналися до ініціативи Open & Agile Smart Cities, яка покликана стандартизувати роботу з даними в розумних містах.

Власне, з широкого трактування застосування IoT, складно його стандартизувати. Не давно IEEE спробувала випустити матеріал «До питання про визначення інтернету речей», але він звівся до викладу позицій різних організацій. Так, W3C розглядає IoT з точки зору інтернету речей (Web of Things), а NIST в руслі кібер-фізичних систем

Але інститут інженерів електротехніки і електроніки (IEEE), міжнародна некомерційна асоціація спеціалістів в області техніки, світові лідери в області розробки стандартів по

радіоелектроніці, електротехніці та апаратному забезпечені обчислювальних систем і мереж, підготовила набір стандартів, які можуть використовуватися при впроваджені технологій для розумних міст.

Вони виділили десять основних категорій, по впровадженню технологій і відповідно до них розробили наступні стандарти:

- Smart grid (Розумна мережа)

IEEE 1547 Series DER
IEEE 1815 Distributed Network Protocol
IEEE 2030 Series Interoperability
IEEE C37 Series Grid Critical Infrastructure

- Learning technologies (Навчальні технології)

IEEE 1484 Series eLearning Technologies
IEEE 1278 Series Distributed Interactive Simulation
IEEE 1516 Series Modeling and Simulation
IEEE 1730 Series Distributed Simulation Engineering and Execution Process

- Smart home (Розумний будинок)

IEEE 802 LAN/MAN
IEEE 1901 Series PLC
IEEE 1905.1 Home Network for Heterogeneous Technologies
IEEE 2030.5 Smart Energy Profile

- eGovernance (Електронне управління)

IEEE P7002 Data Privacy Process
IEEE P7004 Child and Student Data Governance
IEEE P7005 Transparent Employer Data Governance
IEEE P7006 Personal Data Artifical Intelligence (AI) Agent

-Cyber security (Кібербезпека)

IEEE P802E ePrivacy
IEEE 1363 Series Encryption
IEEE 1402 Physical Security
IEEE 1686 Intelligent Electronic Devices (IEDs)

- 5G (Мобільний зв'язок п'ятого покоління)

IEEE P1914.1 Fronthaul
IEEE P1918.1 Tactile Internet
IEEE 802 LAN/MAN
IEEE P1915 – IEEE 1921.1 Series Software Defined Networks

- Internet of things (IoT) (Інтернет речей)

IEEE P2413 IoT Architecture
IEEE 1588 Precision Time Stamp
IEEE 1451 Series Sensor Networks
IEEE P1451-99 Harmonization of IoT Devices and Systems

- Energy efficiency (Енергоефективність)

IEEE 1801 Low Power, Energy Aware Electronic System
IEEE P1889 Electrical Performance of Energy Saving Devices
IEEE P1823 Universal Power Adapter for Mobile Devices
IEEE P1922.1 – IEEE P1929.1 Series for Energy Efficient Systems

- eHealth (Електронне здоров'я)

IEEE 11073 Series Medical Devices
IEEE 139 RF Emission from ISM Equipment
IEEE 602 Healthcare Facilities

- Intelligent transportation (Інтелектуальне транспортування)

IEEE 1609 Series Wireless Access Vehicle Environment
IEEE 1901 Series Power Line Communications (PLC)
IEEE 802.15.4p WPAN Rail Communications and Control
IEEE 1512 Emergency Management System

Рис. 12. 3. Стандарти IEEE розумного міста

12.6. Інформаційні технології та інформаційно-технологічні платформи

Платформи розділені на п'ять категорій відповідно до технологій, що використовуються кожною з платформ. На рис. 12.4 представлено огляд платформ проаналізованих розумних міст. На цьому рисунку представлено більшість платформ, що використовують *Cloud Computing* [8].

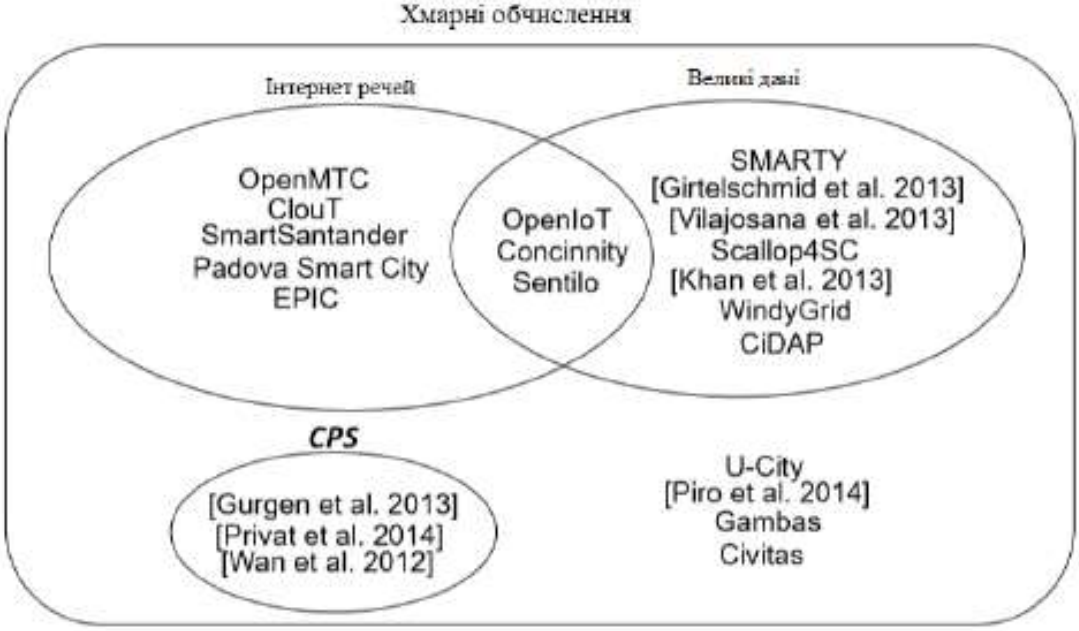


Рис. 12.4. Платформи розумних міст

SmartSantander – це експериментальна інфраструктура для підтримки, розробки та розгортання додатків та послуг у *Smart City* [9]. Проект зосереджений в Сантандері, Іспанія, крім того використовується і в інших європейських містах.

Платформа обробляє велику кількість різноманітної інформації, включаючи дані про стан дорожнього руху, температуру, викиди CO2, вологість.

В даний час в місті впроваджено понад 20 тисяч давачів.

Розумне місто Падуя [11] використовує IoT для створення сенсорної мережі в місті Падуя, Італія. Використовуючи більше трьохсот давачів, платформа збирає дані про навколишнє середовище, такі як викиди CO2, температуру повітря, і контролює вуличні ліхтарі. Особливістю цієї платформи є використання загальних протоколів і форматів даних для забезпечення взаємодії між кількома міськими системами.

Проект Європейської платформи інтелектуальних міст (EPIC) [11] пропонує повне Middleware для IoT для полегшення використання і управління бездротовою мережею з давачами (WSN). Це проміжне програмне забезпечення має на меті боротися з проблемами неоднорідності, сумісності, масштабованості, розширюваності та конфігурації в WSN.

ClouT [12] пропонує двошарову архітектуру для збору даних з WSN і управління давачами та приводами в міській мережі [13]. Першим шаром є давач та привід, який обробляє дані з WSN. Другий шар, шар ядра IoT, керує і контролює мережу давачів та приводів.

OpenMTC [14] (Відкрита комунікація за типом комп'ютерів) – це платформа для інтелектуальних міст, заснована на комп'ютеризації (M2M). Його мета полягає в тому, щоб забезпечити ефективне спілкування між великою кількістю пристроїв, пов'язуючи їх з багатьма службами.

Для досягнення цієї мети платформа підтримує стандартні інтерфейси для різних типів пристроїв, способи обробки даних / подій для досягнення продуктивності в реальному часі, а також легку розробку додатків, що надає комплект для розробки програмного забезпечення.

Аналіз вищезазначених платформ призвів до виявлення чотирьох основних функціональних вимог: управління WSN, управління даними, зібраними з міста, управління послугами та додатками, а також інфраструктури, щоб зробити дані з платформи доступними для міських програм. Цей аналіз також призвів до виявлення п'яти не функціональних вимог: адаптації, сумісності, масштабованості, розширюваності та конфігурації.

Можна виділити дві слабкі сторони цих платформ: відсутність компонентів попередньої обробки для перевірки цілісності даних, зібраних з міста, і малих перетворень даних, таких як агрегація.

OpenIoT3 є відкритим вихідним кодом для розробки додатків на основі IoT. Він має API для керування *WSN*, а також службу каталогів для динамічного виявлення давачів, розгорнутих у місті; крім того має шар для визначення послуг і доступу.

Проект *Concinnity* надає платформу для управління даними та додатками за моделлю ***PaaS*** [16], з якою її автори отримали великі об'єми даних. Однак, ця платформа зосереджена на кількох джерелах даних, таких як *WSN,* соціальні мережі та дані користувачів цієї платформи. Вона також містить каталог служб, де розробники можуть знаходити та публікувати свої розробки, що полегшують використання даної платформи.

Sentilo [17] – це платформа, яка займається управлінням давачами та приводами, призначеним для інтелектуальних міст, які шукають відкритості та сумісності. *Sentilo* використовує поняття IoT для керування *WSN* та *Cloud Computing* для обміну даними з додатками.

Інструменти *Big Data* використовуються в основному для збору та зберігання даних з давачів, що забезпечує масштабованість платформи. Проект *Sentilo* спочатку був розроблений для розміщення в місті Барселона; після його розгортання місто випустило код за ліцензіями LGPL та EUPL з відкритим вихідним кодом.

Основними функціональними вимогами, визначеними для цієї групи платформ, були: керування *WSN*, управління життєвим циклом даних (збір, зберігання, обробка), надання даних з загальнодоступною платформою, сервісний каталог для розробників додатків і

інструменти для впровадження розвитку даних платформ. Як нефункціональні вимоги відносять: сумісність і масштабованість.

Слабким місцем цих платформ є відсутність засобів обробки потоків для аналізу даних у реальному часі з міста, що є важливою вимогою для багатьох додатків Smart City. Інша проблема полягає в тому, що більшість платформ не підтримують налаштування послуг, для роботи з даними громадян. Також незважаючи на проблеми з конфіденційною інформацією, залишається бажання надання індивідуальних послуг для громадян.

Платформи, які використовують хмарні обчислення та великі об'єми даних

Vilajosana та. ін. [18] представляють платформу для розумних міст на основі хмарних обчислень і великих даних, основними компонентами яких є управління даними та хостинг послуг. Вона включає в себе API відкритих даних, що дозволяє стороннім програмам отримувати доступ до даних, що зберігаються у платформі. Інструменти великих даних використовуються для збору потоків даних та їх аналізу, а саме прогнозування та висновки.

Scallop4SC *(платформа SCALable LOgging для розумного міста)* [19, 20] використовує великі дані для обробки великого обсягу даних, зібраних зі смарт-будівель. Платформа використовує інформацію про будівлю, наприклад, споживання води та енергії, температуру, вологість повітря та кількість сміття.

Періодично будівлі передають дані на платформу для обробки. Метою є аналіз розумних даних будівлі, для яких він використовує алгоритм *MapReduce.*

CiDAP [21] – це велика платформа для аналітики даних, яка розгорнута в тестовому полі SmartSantander. Платформа використовує дані, зібрані з SmartSantander, і аналізує їх, щоб зрозуміти поведінку міста. Основними компонентами цієї платформи є: агенти, які збирають дані з платформи

SmartSantander **-** сховище даних для зберігання даних; обробка великих даних для інтенсивної обробки даних та аналітики; і сервер *CityModel*, відповідальний за взаємодію з зовнішніми додатками. Ця платформа використовує *Apache Spark* [22] для обробки даних.

Khan та. ін. [23] пропонують архітектуру *Smart City*, що базується на даних *Big Data*, для досягнення необхідної доступності та масштабованості, необхідної для платформи *Smart Cities.* Архітектура має три шари: один для збору, аналізу та фільтрації даних; інший для зіставлення та агрегування даних, щоб зробити його семантично доречним; і третій рівень, де користувачі можуть переглядати та відновлювати дані, оброблені з двох інших шарів. Реалізація архітектури використовує тільки проекти з відкритим кодом, і автори представили засоби для всіх шарів [24].

WindyGrid [25], є ініціативою міста Чикаго, це платформа для інтелектуальних міст, метою якої є представлення даних як в реальному так і в минулому часі з єдиним поглядом на усі міські операції. Для розробки даної платформи використовувалися технології Big Data, такі як база даних *MongoDB NoSQL* і паралельні процесори даних.

SMARTY [26] – проект, спрямований на надання інструментів і послуг для мобільності та гнучкості систем міського транспорту. Його програмна платформа збирає дані з декількох джерел, таких як транспортний потік, місцезнаходження користувача, затримки транспортних послуг та доступність паркування. Мережа недорогих давачів збирає дані з міста, а соціальні мережі постійно контролюються для отримання даних від громадян. Платформа обробляє величезну кількість даних, що генеруються містом, з використанням методів інтелектуального аналізу даних, таких як класифікація, регресія та кластеризація.

Платформа, запропонована ***Girtelschmid*** та. ін. [27] використовує семантичні технології для створення платформи для інтелектуальних міст, додаючи гнучкість в конфігурації та адаптації системи. Однак, щоб подолати вузькі місця, які зазвичай пов'язані з репозиторіями онтологій та інструментами міркувань, автори поєднують свої семантичні методи з методами обробки даних Big.

Основними функціональними вимогами, визначеними для цієї групи платформ, були: управління даними, такі як збір, аналіз та візуалізація даних; обробка великомасштабних даних, таких як пакетна обробка та обробка в реальному часі; використання семантичних

методів у поєднанні з *Big Data*. Як нефункціональні вимоги відносять: масштабованість і адаптацію.

Більшість платформ у цьому розділі не мають рівня IoT і не вказують, як збираються дані з міста; винятком є *CiDAP*, який використовує тест *SmartSantander* як проміжне програмне забезпечення IoT. Іншим недоліком є те, що більшість платформ не включають обговорення проблем безпеки.

Платформи, які використовують лише технологію Cloud Computing

Piro та. ін. [28] представляють дворівневу сервісну платформу для створення програм *Smart City*. Перший, це низький рівень, який контролює зв'язок між пристроями міста *WSN*. Другий рівень збирає дані з пристроїв і надає послуги з розробки додатків, які використовують дані з міста.

U-City [29] – це платформа для створення розумних повсюдних міст. Платформа пропонує кілька функцій управління послугами, такі як автономне виявлення сервісу, розгортання сервісу та виконання контекстно-орієнтованого сервісу. Вона також пропонує заздалегідь визначені послуги, такі як механізм виводу, контекстно-орієнтована послуга передачі даних і портал для управління платформою.

Gambas, проміжне програмне забезпечення для розробки додатків *Smart City* [30], підтримує збір, розподіл та інтеграцію даних. Платформа також надає середовище виконання програми для полегшення розробки та розгортання служб за допомогою даних міста та реєстру служб. Проміжне програмне забезпечення підтримує контекстну обізнаність, так що послуги *Smart City* можуть адаптуватися до ситуації, поведінки та намірів громадян. Вся комунікація на платформі зашифрована для забезпечення конфіденційності та безпеки громадян.

Civitas [31] є проміжним програмним забезпеченням для підтримки розвитку послуг *Smart Cities*. Вона використовується для полегшення розробки та розгортання додатків *Smart City,* а також для уникнення появи «інформаційних островів» [32], тобто відключені програми, які не поділяють відповідної інформації.

Громадяни підключаються до проміжного програмного забезпечення через спеціальний пристрій під назвою *Civitas Plug*, який забезпечує конфіденційність і безпеку. Проміжне програмне забезпечення має два основні принципи дизайну для полегшення інтеграції додатків: все це програмний об'єкт, який сприяє послідовності розробки програмного забезпечення та повторного використання проміжного програмного забезпечення; і незалежність міського плану, а це означає, що міські служби не повинні працювати лише з одним містом.

Основними функціональними вимогами, визначеними для цієї групи платформ, були: управління послугами та управління даними. Як не функціональні вимоги, визначають: безпеку, конфіденційність і контекстну обізнаність.

Недоліком платформ, представлених у цьому розділі, є те, що жоден з них не використовує відомі рамки для реалізації компонентів, таких як механізм виводу і інструменти обробки, які можуть ускладнити обслуговування.

Платформи, які використовують Хмарні обчислення та Кібер-Фізичні Системи (CPS) як технологічні засоби

Gurgen та. ін. [33] представили проміжне програмне забезпечення для автономних послуг *Smart Cities*, яке включає багато власних властивостей, такі як самоорганізація, самооптимізація, самоконфігурація, самозахист, самовідновлення, Самовідкриття і самооцінка.

Вони виправдовують використання хмарних обчислень для забезпечення масштабованості, надійності та еластичності платформи. Ця платформа надає розробникам додатків контексти окремих користувачів і міста.

Privat та. ін. [34] пропонують іншу платформу на основі *CPS*, основною характеристикою якої є можливості самостійної конфігурації та самоадаптації в розумних середовищах, включаючи розумні міста. Ця платформа надає спільну розподілену програмну інфраструктуру, яка збирає дані та реагує на зміни у середовищі.

Wan та. ін. [35] пропонують платформу *CPS*, яка використовує менеджер подій для управління та створення співпраці між компонентами *M2M*. Ця платформа надає дані та послуги стороннім додаткам через модуль публікації / підписки. Платформа також дозволяє створювати потоки подій для керування і обробки критично важливих повідомлень.

Основними функціональними вимогами, визначеними для цієї групи платформ, були: автономна реакція на зміни в міському середовищі, комунікація між пристроями міста, а також механізм публікації / підписки на додатки для зв'язку з платформою. Як нефункціональні вимоги, визначено: конфігурацію, адаптацію та усвідомлення контексту.

Платформи зосереджені на розгортанні, налаштуванні та роботі *CPS*- пристроїв у місті, але їм не вистачає важливих вимог, таких як моніторинг та публікація даних з пристроїв. Вони також не описують жодного механізму перевірки даних, зібраних з міста, відкидаючи невідповідності.

Платформа CiDAP

Платформа міських даних та аналітики (*CiDAP*) – це платформа на основі великих даних, яка спрямована на використанні даних, зібраних у місті, для забезпечення контекстної обізнаності та інтелекту в програмах і службах. Ця платформа обробляє великі набори даних, зібрані *з Middleware IoT*.

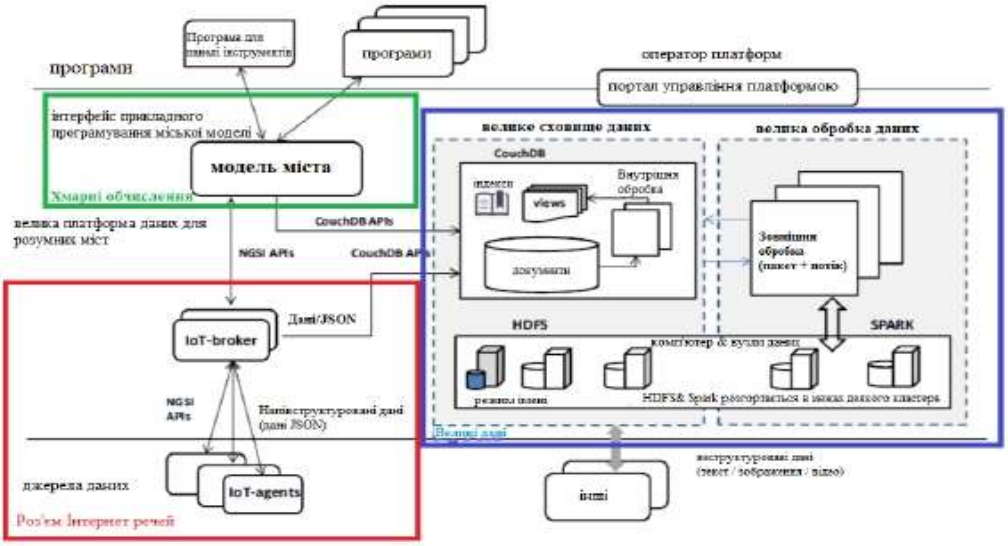


Рис.12.5. Платформа CiDAP

Представлена архітектура платформи має наступні п'ять основних компонентів:

- *IoT-агенти* підключаються до прошивки IoT і служать шлюзом для пристроїв, доступних для платформи. Кожне джерело даних проміжного програмного забезпечення IoT відображається у агенті IoT;
- IoT-Brokers діють як уніфікований інтерфейс для агентів IoT, полегшуючи доступ до даних проміжного програмного забезпечення. Цей компонент зв'язується з великим сховищем даних для передачі даних, що зберігаються, і з сервером *CityModel* для передачі даних, які будуть використовуватися безпосередньо за допомогою програм;
- *Big Data Repository* зберігає необроблені дані, зібрані з міста, і обробляє дані з компонента обробки великих даних. Платформа використовує базу даних *CouchDB4 NoSQL*, яка зберігає дані як документи *JSON*. Цей компонент також має внутрішній інструмент обробки, який робить обробку простою, наприклад, перетворення даних у

нові формати або створення нових структурованих переглядів та таблиць для індексування даних;

- велика обробка даних відповідає за складну або інтенсивну обробку з використанням даних, що зберігаються у великому сховищі даних, таких як агрегація даних або інтелектуальний аналіз даних. Крім того, він обробляє історичні дані, використовуючи пакетні процеси, або дані реального часу, використовуючи потоки даних. Цей компонент використовує *Apache Spa*rk для цієї обробки;
- *City Model Server* – це інтерфейс платформи для зовнішніх додатків.

*API City*Model дозволяє програмам виконувати прості та складні запити, і підписуватись на певні фрагменти даних з платформи. Прості запити запитують останні дані з пристроїв, складні запити запитують сукупні історичні дані, а підписка – це механізм, з якого програми періодично отримують дані з пристроїв [36].

Червоні, зелені та сині поля на рисунку висвітлюють поняття, що використовуються для реалізації кожного шару платформи. Коробка з'єднувача IoT має компоненти для полегшення доступу до пристроїв IoT в платформі. Поле великих даних містить компоненти для зберігання та аналізу даних, зібраних з різних джерел. Нарешті, вікно *Cloud Computing* вказує інтерфейс платформи з зовнішніми додатками, який реалізований за допомогою хмарних сервісів.

CiDAP в основному стосується зберігання та обробки великої кількості даних на платформі, що важливо через величезну кількість даних, зібраних у місті. Сильними сторонами його архітектури є зберігання та обробка даних, модулі обробки в реальному часі та пакетної обробки, а також те, що пов'язана з ним платформа вже тестувалася в тестовому полі SmartSantander.

Важливим обмеженням *CiDAP* є те, що платформа не передбачає конкретних сервісів і інструментів для розробників додатків, а також не дозволяє розгортати нові сервіси в платформі, що ускладнює її розширення.

Червоні, зелені та сині поля на рисунку підкреслюють поняття, що використовуються для реалізації кожного шару платформи. Коробка з'єднувача IoT має компоненти для полегшення доступу до пристроїв IoT, та до платформи.

Поле великих даних містить компоненти для зберігання та аналізу даних, зібраних з різних джерел. Вікно *Cloud Computing* вказує на інтерфейс платформи з зовнішніми додатками, яка реалізована за допомогою хмарних сервісів.

CiDAP в основному стосується зберігання і обробки великої кількості даних у платформі. Це є важливим через величезну кількість даних, зібраних у місті. Сильними сторонами цієї архітектури є зберігання та обробка даних, модулі які працюють у реальному часі, пакетної обробки, а також те, що асоційована платформа вже тестувалася на тестовому полі *SmartSantander*.

Важливим обмеженням *CiDA*P є те, що платформа не передбачає конкретних послуг та інструментів для розробників додатків і не дозволяє розгортати нові послуги.

OpenIoT

Архітектура платформи, складається з трьох шарів: фізичної площини, віртуалізованої площини і площини утиліти (рис.12.6).

Фізичний площина – це проміжне програмне забезпечення, відповідальне за збір, фільтрацію, об'єднання та очищення даних від давачів, приводів і пристроїв.

Ця площина виступає в ролі інтерфейсу між фізичним світом і платформою *OpenIoT*. Поточна версія *OpenIo*T використовує проміжне програмне забезпечення *X-GSN* [37], проміжне програмне забезпечення з відкритим кодом для управління, моніторингу та контролю пристроїв IoT.

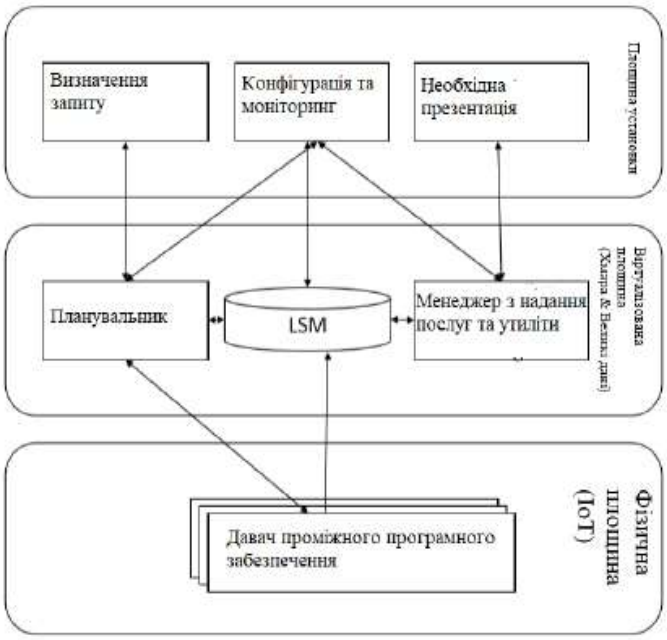


Рис. 12.6. Архітектура платформи OpenIoT

Віртуалізована площина має на меті зберігання даних, виконування послуг і планування виконаних послуг. Основними компонентами віртуальної площини є:

1. планувальник приймає запити на послуги і забезпечує доступ до ресурсів, які потрібні сервісу, а саме потоки даних. Також цей компонент відповідає за виявлення сенсорів, необхідних для виконання служби;
2. зберігання хмарних даних, зберігає всі дані з платформи, наприклад, потоки даних, зібрані з давачів, і дані, створені в рамках платформи, такі як профілі користувачів, визначення служб і зареєстровані програми. Для зберігання даних, зібраних з проміжного програмного забезпечення IoT, *OpenIoT* використовується *Middleware (LSM)* [38];
3. менеджер з надання послуг та утиліт має три основні функції: обробку та комбінацію даних, зібраних з інтерфейсу IoT, надання дозволів послугам, та надання результатів запитів платформі або до додаткам третіхсторін. Також цей компонент відстежує використання послуг, визначених у платформі для обліку та виставлення рахунків.

Площина *Utility-App*, це користувальницький інтерфейс платформи, який має три основні компоненти:

1. визначення запитів, дозволяє користувачам визначати нові програми, використовуючи служби, розгорнуті на певній платформі;
2. презентація запиту, виконує програми створені в компоненті *Definition Request*. Коли користувач використовує додаток, він зв'язується з диспетчером процесів та утилітою, щоб отримати результати виконання служб;
3. конфігурація і моніторинг дозволяє конфігурувати параметри платформи, такі як періодичність зчитування даних з давачів і моніторинг стану всіх платформних пристроїв і компонентів.

OpenIoT є повноцінною платформою, яка відповідає майже всім основним вимогам смарт сіті. Сильними сторонами цієї платформи є використання проміжного ПО IoT для налаштування та збору даних з пристроїв, проміжного програмного забезпечення для зберігання даних, зібраних з давачів, інструментів розробки, і того факту, що платформа є відкритим джерелом.

Однак його архітектура не розглядає інші джерела даних, такі як соціальні мережі, і не надає підтримку для послуг попередньої обробки, що стосуються великих даних.

Найнижчою складовою еталонної архітектури є *Cloud* and *Networking*, яка відповідає за управління та зв'язок вузлів міської мережі. Цей компонент має ідентифікувати всі пристрої,

підключені до платформи, включаючи сервери, давачі, приводи та пристрої користувача. Використання концепцій хмарних обчислень важливо для забезпечення деяких фундаментальних нефункціональних вимог, включаючи масштабованість і розширюваність.

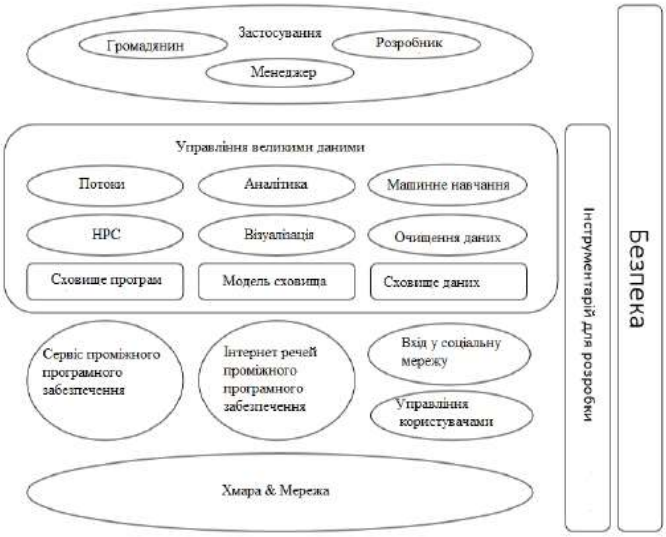


Рис. 12.7. Єдина архітектура

У верхній частині інфраструктури *Cloud* і *Networking*, еталонна архітектура включає в себе *Middleware* програмного забезпечення IoT і службу *Middleware.* Перший повинен управляти міською мережею IoT і забезпечувати ефективну комунікацію платформи з пристроями користувача, давачами міста та приводами. Служба *Middlewar*e повинна керувати послугами, які платформа надаватиме додаткам, виконуючи такі операції, як публікація, втілення, моніторинг, складання та хореографування цих послуг.

Проміжне програмне забезпечення *X-GSN* можна використовувати для реалізації *Middleware IoT*, який вже використовується в проекті *OpenIoT*. Іншим варіантом є використання компонентів платформи *Sentilo*, яка також є з відкритим вихідним кодом, і реалізація повного програмного інтерфейсу IoT.

Для забезпечення кращих послуг громадянам важливо, щоб платформа зберігала деякі дані користувача, що є роллю компонента «*Управління користувачами*». Але, щоб забезпечити конфіденційність користувачів, ці дані повинні бути належним чином захищені, а дозвіл на їх зберігання має бути отримано від користувача. Більш того, оскільки міська платформа буде мати багато додатків, може бути корисно запропонувати єдиний механізм входу.

Контрольні питання до розділу

1. Основні складові розумного міста. Наведіть характеристики кожного.
2. Наведіть класифікацію Smart City.
3. Система управління *Smart City.*
4. Найважливіші напрямки розвитку «розумного міста»
5. Концепції розумного міста
6. На яких характеристиках ґрунтується концепція розумного міста?
7. Наведіть загальну схему розумного міста.
8. Основні складові Розумного міста.
9. Які елементи місто повинне містити у собі Розумне місто?
10. Які існують технології розумних міст?
11. Стандарти розумного міста.
12. Інформаційно-технологічні платформи розумних міст.

13. Платформи, які використовують хмарні обчислення та великі об’єми даних.
14. Платформи, які використовують лише технологію Cloud Computing.
15. Платформи, які використовують Хмарні обчислення та Кібер-Фізичні Системи (CPS) як технологічні засоби.
16. Платформа CiDAP. Основні компоненти платформи.
17. Платформа OpenIoT. Архітектура OpenIoT.
18. Які існують основні компоненти віртуальної площини архітектури OpenIoT.
19. Як основні компоненти має площина Utility-App архітектури OpenIoT.

Список рекомендованої літератури

1. Li D, Yao Y, Shao Z, et al. From digital earth to smart earth. Chin Sci Bull, 2014, 59: 722-733.
2. Van den Besselaar P, Melis I, Beckers D. Digital cities: organization, content, and use. In: Ishida T, Isbister K, eds.
3. Widmayer P. Building digital metropolis: Chicago's future networks. IT Prof, 1999, 1: 40-46.
4. Malek J A. Informative global community development index of informative smart city. In: Proceedings of 8th WSEAS International Conference on Education and Educational Technology, Athens, 2009. 17-19.
5. Moser M A. What is smart about the smart communities movement.EJournal, 10, 2001: 11.
6. Komninos N, Sefertzi E. Intelligent cities: R&D offshoring, Web 2.0 product development and globalization of innovation.
7. Nam T, Pardo T A. Conceptualizing smart city with dimensions of technology, people, and institutions. In: Proceedings of 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times. New York: ACM, 2011. 282–291.
8. Wolfgang Apolinarski, Umer Iqbal, and Josiane Xavier Parreira. 2014. The GAMBAS mid-dleware and SDK for smart city applications. In Pervasive Computing and Communica-tions Mas - sive IoT Data. In Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. 324-327.DOI [Електронний ресурс] – http://dx.doi.org/10.1109/SOCA.2014.47 – (дата звертання 17.02.2019).
9. Luis Sanchez, Luis Muoz, Jose Antonio Galache, Pablo Sotres, Juan R. Santana, Veronica Gutierrez, Ra-jiv Ramdhany, Alex Gluhak, Srdjan Krco, Evangelos Theodoridis, and Dennis Pfisterer. 2014. Smart-Santander: IoT experimentation over a smart city testbed. Computer Networks 61 (2014), 217 – 238. DOI [Електронний ресурс] – http://dx.doi.org/10.1016/j.bjp.2013.12.020 - Special issue on Future Internet Testbeds Part I – (дата звертання 17.02.2019).
10. Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. 2014. Internet of Things for Smart Cities. Internet of Things Journal, IEEE 1, 1 (Feb 2014), 22–32. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/JIOT.2014.2306328 – (дата звертання 18.02.2019).
11. Pieter Ballon, Julia Glidden, Pavlos Kranas, Andreas Menychtas, Susie Ruston, and Shenja Van Der Graaf. 2011. Is there a Need for a Cloud Platform for European Smart Cities?. In eChallenges e-2011 Conference Proceedings, IIMC International Information Management Corporation.
12. Kenji Tei and Levent Gurgen. 2014. ClouT: Cloud of things for empowering the citizen clout in smart cities. In Internet of Things (WF-IoT), 2014 IEEE World Forum on. IEEE, 369–370.
13. Jose Antonio Galache, Takuro Yonezawa, Levent Gurgen, Daniele Pavia, Marco Grella, and Hiroyuki Maeomichi. 2014. ClouT: Leveraging Cloud Computing Techniques for Improving Management of Massive IoT Data. In Service- Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. 324–327. DOI

[Електронний ресурс] –http://dx.doi.org/10.1109/SOCA.2014.47 – (дата звертання 26.02.2019).
14. A. Elmangoush, H. Coskun, S. Wahle, and T. Magedanz. 2013. Design aspects for a reference M2M communication platform for Smart Cities. In Innovations in Information Technology (IIT), 2013 9th International Conference on. 204–209. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/Innovations.2013.6544419 – (дата звертання 01.03.2019).
15. Riccardo Petrolo, Valeria Loscri, and Nathalie Mitton. 2014. Towards a Cloud of Things Smart City. IEEE COMSOC MMTC E-Letter 9, 5 (Sept. 2014), 44–48. [Електронний ресурс] – https://hal.inria.fr/hal-01080273 – (дата звертання 01.03.2019).
16. Chao Wu, David Birch, Dilshan Silva, Chun-Hsiang Lee, Orestis Tsinalis, and Yike Guo. 2014. Concinnity: A Generic Platform for Big Sensor Data Applications. Cloud Computing, IEEE 1, 2 (July 2014), 42–50. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/MCC.2014.33 – (дата звертання 7.03.2019).
17. Malcolm Bain. 2014. Sentilo – Sensor and Actuator Platform for smart Cities. (March 2014). Retrieved February 20, 2015 from [Електронний ресурс] – https://joinup.ec.europa.eu/community/eupl/document/ sentilosensor and- actuator-platform- smart cities – (дата звертання 7.03.2019).
18. Ignasi Vilajosana, Jordi Llosa, Borja Martinez, Marc Domingo-Prieto, Albert Angles, and Xavier Vilajosana. 2013. Bootstrapping smart cities through a self-sustainable model based on big data flows. Communi- cations Magazine, IEEE 51, 6 (2013), 128–134.
19. Kohei Takahashi, Shintaro Yamamoto, Akihiro Okushi, Shinsuke Matsumoto, and Masahide Nakamura. 2012. Design and implementation of service API for large-scale house log in smart city cloud. In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. 815–820. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/ CloudCom.2012.6427590 – (дата звертання 10.03.2019).
20. Kohei Takahashi, Shinsuke Matsumoto, and Masahide Nakamura. 2014. Smart Cities Data Streams Integration: Ex- perimenting with Internet of Things and Social Data Flows. In Proceedings of the 4th International Conference on Web Intelligence, Mining and Semantics (WIMS14) (WIMS '14). ACM, New York, NY, USA, Article 60, 5 pages. DOI [Електронний ресурс]– http://dx.doi.org/10.1145/2611040.2611094 – (дата звертання 15.03.2019).
21. Bin Cheng, Salvatore Longo, Flavio Cirillo, Martin Bauer, and Ernoe Kovacs. 2015. Building a Big Data Plat-form for Smart Cities: Experience and Lessons from Santander. In Big Data (BigData Congress), 2015 IEEE International Congress on. 592–599. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/BigDataCong ress.2015.91 – (дата звертання 19.03.2019).
22. Matei Zaharia, Mosharaf Chowdhury, Michael J Franklin, Scott Shenker, and Ion Stoica. 2010. Spark: cluster computing with working sets. In Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, Vol. 10. 10.
23. Zaheer Khan, Ashiq Anjum, Kamran Soomro, and Muhammad Atif Tahir. 2015. Towards cloud based big data analytics for smart future cities. Journal of Cloud Computing 4, 1 (2015), 1–11. DOI [Електронний ресурс] – http://dx.doi.org/10.1186/s13677- 015- 0026-8.
24. Zaheer Khan, Ashiq Anjum, and Saad Liaquat Kiani. 2013. Cloud Based Big Data Analytics for Smart Future Cities. In Utility and Cloud Computing (UCC), 2013 IEEE/ACM 6th International Conference on. 381–386. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/UCC.2013.77 – (дата звертання 14.02.2019).
25. Sean Thornton. 2013. Chicagos WindyGrid: Taking Situational Awareness to a New Level. (March 2013). Retrieved February 20, 2015 from [Електронний ресурс] – http://datasmart.ash.harvard.edu/news/article/chicagos-windygrid- taking-situational-awareness-to-a-new-level-259 – (дата звертання 18.03.2019).
26. Giuseppe Anastasi, Maximiliano Antonelli, Alessio Bechini, Simone Brienza, Eleonora D'Andrea, Domenico De Guglielmo, Pietro Ducange, Beatrice Lazzerini, Francesco

Marcelloni, and Armando Segatori. 2013. Urban and social sensing for sustainable mobility in smart cities. In Sustainable Internet and ICT for Sustainability (SustainIT), 2013. IEEE, 1–4.
27. Sylva Girtelschmid, Matthias Steinbauer, Vikash Kumar, Anna Fensel, and Gabriele Kotsis. 2013. Big Data in Large Scale Intelligent Smart City Installations.In Proceedings of International Conference on Infor- mation Integration and Web-based Applications & Services (IIWAS '13). ACM, New York, NY, USA, Article428, 5 pages. DOI [Електронний ресурс] – http://dx.doi.org/10.1145/2539150.2539224 – (дата звертання 18.03.2019).
28. Giseppe Piro, Ilaria Cianci, Luigi A. Grieco, Gennaro Boggia, and Pietro Camarda. 2014. Informa- tion centric services in Smart Cities. Journal of Systems and Software 88, 0 (2014), 169 – 188. DOI [Електронний ресурс] – http://dx.doi.org/10.1016/j.jss.2013.10.029 – (дата звертання 22.03.2019).
29. Yong Woo Lee and Seungwoo Rho. 2010. U-city portal for smart ubiquitous middleware. In Advanced Com- munication Technology (ICACT), 2010 The 12th International Conference on, Vol. 1. 609–613.
30. Wolfgang Apolinarski, Umer Iqbal, and Josiane Xavier Parreira. 2014. The GAMBAS middleware and SDK for smart city applications. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on. 117–122. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/PerComW.201 4.6815176 – (дата звертання 27.03.2019).
31. Flix J. Villanueva, Maria J. Santofimia, David Villa, Jess Barba, and Juan Carlos Lopez. 2013. Civ- itas: The Smart City Middleware, from Sensors to Big Data. In Innovative Mobile and Inter- net Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on. 445–450. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/IMIS.2013.80 – (дата звертання 01.04.2019).
32. Junping Qiu, Yanhui Song, and Siluo Yang. 2010. Digital Integrated Model of Government Resources under E-Government Environment. In Internet Technology and Applications, 2010 International Conference on. 1–4. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/ITAPP.2010.5566315 – (дата звертання 01.04.2019).
33. Levent Gurgen, Ozan Gunalp, Yazid Benazzouz, and Mathieu Gallissot. 2013. Self-aware cyber-physical systems and applications in smart buildings and cities. In Design, Automation Test in Europe Conference Exhibition (DATE), 2013. 1149–1154. DOI [Електронний ресурс] – http://dx.doi.org/10.7873/ DATE.2013.240 – (дата звертання 04.04.2019).
34. Gilles Privat, Mengxuan Zhao, and Laurent Lemke. 2014. Towards a Shared Software Infrastructure for Smart Homes, Smart Buildings and Smart Cities. In International Workshop on Emerging Trends in the Engineering of Cyber-Physical Systems, Berlin.
35. Jiafu Wan, Di Li, Caifeng Zou, and Keliang Zhou. 2012. M2M Communications for Smart City: An Event- Based Architecture. In Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on. 895–900. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/CIT.2012.188 – (дата звертання 07.04.2019).
36. Riccardo Petrolo, Valeria Loscri, and Nathalie. Automation Test in Europe Conference Exhibition (DATE), 2013. 1149–1154. DOI [Електронний ресурс] – http://dx.doi.org/10.7873/DATE.2013.240 – (дата звертання 07.04.2019).
37. Jean-Paul Calbimonte, Sofiane Sarni, Julien Eberle, and Karl Aberer. 2014. XGSN: An Open-source Semantic Sensing Middleware for the Web of Things. In 7th International Workshop on Semantic Sensor Networks.
38. Danh Le-Phuoc, Hoan Quoc Nguyen-Mau, Josiane Xavier Parreira, and Manfred Hauswirth. 2012. A mid- dleware framework for scalable management of linked streams. Web Semantics: Science, Services and Agents on the World Wide Web 16 (2012), 42–51.

РОЗДІЛ 13. ТЕХНОЛОГІЇ ОБРОБКИ ВЕЛИКИХ ДАНИХ (BIG DATA)

13.1. Огляд технологій

Великі дані (Big Data) – позначення структурованих и неструктурованих даних величезних обсягів і значного розмаїття, що піддаються ефективній обробці програмних інструментів, які горизонтально масштабуються та з'явились у кінці 2000-х років, і альтернативних традиційних систем управління базами даних і рішенням класу рішень *Business Intelligence* [1].

Аналітики компанії IBS «весь світовий обсяг даних» оцінили такими величинами [2]:

- 2003 г. — 5 ексабайтів даних (1 ЭБ = 1 млрд гігабайтів)
- 2008 г. — 0,18 зеттабайта (1 ЗБ = 1024 ексабайта)
- 2015 г. — более 6,5 зеттабайтів
- 2021 г. — 44–48 зеттабайта (прогноз)
- 2025 г. — цей об'єм збільшується ще у 10 разів.

Великі дані – це сукупність технологій, покликаних здійснювати три операції [3]:

- Обробляти більші, у порівнянні зі «стандартними» сценаріями, об'єми даних.
- Уміти працювати з даними, що швидко надходять у дуже великих об'ємах. Тобто даних не просто багато, а їх постійно стає все більше й більше.
- Вміти працювати зі структурованими і мало стуктурованими даними паралельно і у різних аспектах.

Вважається, що ці «вміння» дозволяють виявляти приховані закономірності, що вислизають від обмеженого людського сприйняття [4].

Це дає безпрецедентні можливості оптимізації багатьох сфер нашого життя: державного управління, медицини, телекомунікацій, фінансів, транспорту, виробництва і так далі [5]. Не дивно, що журналісти і маркетологи так часто використовували словосполучення *Big Data*, що багато експертів вважають цей термін дикредитованим і пропонують від нього відмовитись [6].

Більш того, у жовтні 2015 року компанія *Gartner* виключила *Big Data* з числа популярных трендів. Своє рішення аналітики компанії пояснили тим, що до складу поняття «великі дані» входить значна кількість технологій, які вже активно застосовуються на підприємствах, вони частково стосуються інших популярних сфер і тенденцій і стали повсякденним робочим інструментом.

13.2. Три принципи роботи з великими даними

Визначальними характеристиками для великих даних є, окрім їх фізичного об'єму, й інші, які підкреслюють складність задачі обробки і аналізу цих даних. Набір даних *VVV* (*volume, velocity, variety* — фізичний об'єм, швидкість приросту даних і необхідність їх швидкої обробки, здатність обробляти дані різних типів) був розроблений компанією *Meta Group* у 2001 році з метою вказати на рівну значимість управління даними по всім трьом аспектам.

У подальшому з'явилась інтерпретація з чотирьома V (додалась *veracity – достовірність*), п'ятою V (*viability – життєздатність і value – цінність*), семи V (*variability – змінність та visualization – візуалізація*). Але компанія IDC, наприклад, інтерпретує саме четверте V як value (цінність), пікреслюючи економічну доцільність обробки великих об'ємів даних у відповідних умовах [7].

Виходячи з вищеназваних визначень, основні принципи роботи з великими даними такі:

Горизонтальна масштабованість. Це — базовий принцип обробки великих данных. Як вже було зазначено, великих даних з кожним днем стає все більше. Відповідно, необхідно збільшувати кількість обчислювальних вузлів, за якими розподіляються ці дані, при чому обробка має відбуватись без погіршення продуктивності

Відмовостійкість. Цей принцип витікає з попереднього. Оскільки обчислювальних вузлів у кластері може бути багато (іноді десятки тисяч) та їх кількість, не виключено, буде збільшуватись, зростає ймовірність виходу машин з ладу. Методи роботи з великими даними мають враховувати ймовірність таких ситуацій і передбачати превентивні заходи

Локальність даних. Оскільки дані розподілені по великій кількості обчислювальних вузлів, то, якщо вони фізично знаходяться на одному сервері, а обробляються на іншому, витрати на передачу даних можуть бути невиправдано великими. Тому обробку даних бажано проводити на тій же машині, на якій вони зберігаються

Ці принципи відрізняються від тих, які характерні для традиційних, централізованих, вертикальних моделей зберігання добре структурованих даних. Власне, для роботи з великими даними розробляються підходи і технології.

13.3. Технології і тенденції роботи з Big Data

Початково у сукупність підходів і технологій включались засоби масово-паралельної обробки невизначено-структурованих даних, такі як *СУБД NoSQL*, алгоритми *MapReduce* і засоби проекту *Hadoop*. У подальшому до технологій великих даних почали відносити й інші рішення, що забезпечують схожі за характеристиками можливості обробки надвеликих масивів даних, а також деякі апаратні засоби.

MapReduce — модель розподілених обчислювань у комп'ютерних кластерах, представлена компанією Google. Згідно з цією моделлю, додаток розділяється на значну кількість однакових елементарних завдань, що виконуються на вузлах кластера і потім, природнім шляхом зводяться у кінцевий результат.

SQL - мова структурованих запитів, що дозволяє працювати з базами даних. За допомогою SQL можна створювати і модифікувати дані, а управлінням масиву даних займається відповідна система управління базами даних.

NoSQL *(Not Only SQL, не лише SQL*) — загальний термін для різних нереляційних баз даних і сховищ, не означає якусь конкретну технологію чи продукт. Звичайні реляційні бази даних добре підходять для досить швидких і однотипних запитів, а на складних і гнучко побудованих запитах, характерних для великих даних, навантаження перевищує розумні межі і використання СУБД стає неефективним.

Основні риси:

- базова доступність - запити гарантовано завершується (успішно чи безуспішно);
- гнучкий стан - стан системи може змінюватися з часом, навіть без введення нових даних, для досягнення узгодження даних;
- узгодженість в кінцевому рахунку - дані можуть бути деякий час неузгодженими, але приходять до узгодження через деякий час.

Hadoop — проект фонду *Apache Software Foundation,* набір утилітів, бібліотек і фреймворків, що вільно розповсюджується, для розробки і виконання розподілених програм, які працюють на кластерах із сотень і тисяч вузлів. Вважається однією з основоположних технологій більшості даних.

Використовується для реалізації пошукових і контекстних механізмів багатьох високонавантажених веб-сайтів, у тому числі, для *Yahoo!* та *Facebook*. Розроблено на *Java* в рамках обчислювальної парадигми *MapReduce*, згідно з якою додаток розділяється на велику кількість однакових елементарних завдань, здійсненних на вузлах кластера і природним чином приводяться в кінцевий результат.

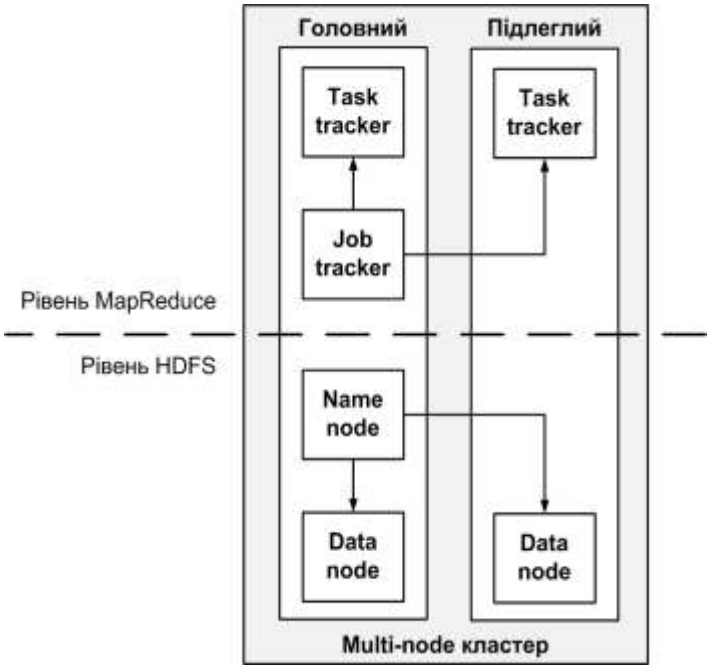


Рис. 13.1. Обчислювальна парадигма *MapReduce*

R — мова програмування для статистичної обробки даних і роботи з графікою. Широко використовується для аналізу даних і фактично став стандартом для статистичних програм.

Апаратні рішення. Корпорації *Teradata, EMC* та ін. др. пропонують апаратно-програмні комплекси, призначені для обробки великих даних. Ці комплекси поставляються як готові до установки телекомунікаційні шафи, що містять кластер серверів і керівне програмне забезпечення для масово-паралельної обробки. Сюди іноді відносять апаратні рішення для аналітичної обробки в оперативній пам'яті, зокрема, апаратно-програмні комплекси Hana компанії *SAP* і комплекс *Exalytics* компанії *Oracle*, незважаючи на те, що така обробка початково не є масово-паралельною, а об'єми оперативної пам'яті одного вузла обмежуються кількома терабайтами [8].

13.4. Методи і техніка анализу великих даних

Міжнародна консалтингова компанія *McKinsey*, що спеціалізується на розв'язанні задач, пов'язаних зі стратегічним управлінням, виділяє 11 методів і технік аналізу, що застосовуються до великих даних.

Методи классу Data Mining (видобуток даних, інтелектуальний аналіз даних, глибинний аналіз данних) — сукупність методів виявлення у даних раніше невідомих, нетривіальних, практично корисних знань, необхідних для прийняття рішень. До таких методів, зокрема, належать: навчання асоціативним правилам (association rule learning), класифікація (разгалуження на категорії), кластерний аналіз, регресійний аналіз, виявлення і аналіз відхилень тощо.

Краудсорсінг — класифікація і збагачення даних силами широкого, неозначеного кола особистостей, що виконують цю роботу без вступу у трудові стосунки.

Змішання та інтеграція даних (data fusion and integration) — набір технік, що дозволяють інтегрувати різнорідні дані з розмаїття джерел з метою проведення глибинного аналізу (наприклад, цифрова обробка сигналів, обробка природньої мови, включно з тональним аналізом).

Машинне навчання, включаючи навчання з учителем і без учителя – використання моделей, побудованих на базі статистичного аналізучи машинного навчання для отримання комплексних прогнозів на основі базових моделей.

Штучні нейронні мережі, мережевий аналіз, оптимізація, у тому числі генетичні алгоритми (*genetic algorithm* — евристичні алгоритми пошуку, що використовуються для

розв’язання задач оптимізації і моделювання шляхом випадкового підбору, комбінування і варіації потрібних параметрів з використанням механізмів, аналогічних натуральному відбору у природі)

Розпізнавання образів

Прогнозна аналітика

Імітаційне моделювання (*simulation*) — метод, що дозволяє будувати моделі, що описують процеси так, як вони би проходили у дійсності. Імітаційне моделювання модна розглядати як різновид експериментальних випробувань.

Просторовий аналіз (*spatial analysis*) — клас методів, що використовують топологічну, геометричну і географічну інформацію, що вилучається із даних.

Статистичний аналіз — аналіз часових рядів, A/B-тестування (*A/B testing, split testing* — метод маркетингового дослідження; при його використанні контрольна група елементів порівнюється із набором тестових груп, у яких один чи кілька показників були змінені, щоб з’ясувати, які зі змін покращують цільовий показник.

Візуалізація аналітичних даних — подання інформації у вигляді малюнків, діаграм, з використанням інтерактивних можливостей і анімації, як для отримання результатів, так і для використання у якості вихідних даних для подальшого аналізу. Дуже важливий етап аналізу великих даних, що дозволяє показати найважливіші результати аналізу у найбільш зручному для сприйняття вигляді [9].

13.5. Великі дані у промисловості

Згідно звіту компанії *McKinsey «Global Institute, Big data: The next frontier for innovation, competition, and productivity»*, дані стали таким само важливим фактором виробництва, як трудові ресурси чи виробничі активи. За рахунок використання великих даних, компанії можуть отримувати відчутні конкурентні переваги. Технології *Big Data* можуть бути корисними при вирішенні наступних задач:

- прогнозування ринкової ситуації
- маркетинг і оптимізація продажів
- вдосконалення продукції
- ухвалення управлінських рішень
- підвищення продуктивності праці
- ефективна логістика
- моніторинг стану основних фондів [10,11].

На виробничих підприємствах великі дані генеруються також внаслідок впровадження підприємства, великі дані генеруються також внаслідок впровадження технологій Промислового інтернету речей. У ході цього процесу основні вузли і деталі станків і машин оснащуються датчиками, виконавчими пристроями, контролерами та, іноді, недорогими процесорами, здатними виробляти граничні (туманні) обчислення. В процесі виробничого процесу здійснюється постійний збір даних і, можливо, їх попередня обробка (наприклад, фільтрація). Аналітичні платформи обробляють результати у найбільш зручному для сприйняття вигляді і зберігають для подальшого використання. На основі аналізу отриманих даних робляться висновки про стан обладнання, ефективність внесених змін у технологічні процеси і т.д..

Завдяки моніторингу інформації у режимі реального часу персонал підприємства має змогу:

- *скорочувати кількість простоїв*
- *підвищувати продуктивність обладнання*
- *зменшувати витрати на експлуатацію обладнання*
- *запобігати нещасним випадкам*.

Останній пункт особливо важливий. Наприклад, оператори, що працюють на підприємствах нафтопереробної промисловості, отримують у середньому біля 1500 аварійних повідомлень на день, тобто більше одного повідомлення у хвилину. Це призводить

до підвищеної втоми операторів, яким доводиться постійно приймати миттєві рішення про те, як реагує платформа на той чи інший сигнал.

Проте зміна класу досліджень – від оперативного до аналітичного, поява нових типів даних, необхідність швидкого доступу до них, зумовила збільшення інтересу до проблеми інтеграції та опрацювання даних з метою підвищення якості управлінських рішень. Найвищий пік активності дослідженьу сфері інтеграції припадає на 90-ті рр. XX ст. та на наш час [12] у зв'язку збурхливим розвитком методів *Business Intelligence* та збільшенням можливостей сховищ даних (збільшення обсягів збережених даних, наявністьпроцедур аналітичного опрацювання даних – *OLAP*).

Особливістю сучасних досліджень є аналіз не лише типів даних (описів), але й семантики. Особливо активний розвиток засобів для оперативного збору різнотипних даних, завантаження їх у сховище даних, аналізу та прогнозування спостерігається в сферах енергетики та адміністративного керування,нафтогазовому секторі [13].

Проблема швидкого отримання різнотипових даних (сенсорних числових, текстових документів, графіків тощо) з метою формування на їх основіоперативних рішень постала ще у роки 2-ї світової війни і активно розвивалась для застосування в атомних проектах, управлінні ракетами, навігації, управлінні бойовими діями.

Опрацювання та аналіз таких різнотипових даних використовується для моделювання розвитку подій та ситуацій, а також в системах підтримки прийняття рішень. Започаткували вивчення цієї проблеми *фон Нейман*, розробки компанії IBM, науковці школи Лєбєдєва С.О. (спеціалізована ЕОМ), *Глушкова В.М*. (системний аналіз, теорія конфліктних ігор, проблемно орієнтовані системи моделювання та опрацювання даних) [13] що призвело до розвитку мов блокового програмування, систем підтримки прийняття рішень.

Схема отримання інформації органами керування регіоном передбачає створення статистичних звітів іншими об'єктами галузі за наперед визначеноюформою з покроковим агрегуванням інформації від одного об'єкту до іншого

Це приводить до того, що особа, яка отримує інформацію, бачить її лише в агреговану вигляді за жорстко визначеними критеріями групування, а деталізована інформація потрапляє зі значним запізненням. Тому рішення, які можуть бути прийняті у такому випадку, недостатньо враховують усі особливості перебігу процесів розвитку регіону. Процес консолідації даних (на рисунку) для аналізу та прогнозування розвитку регіону генерує наступні задачі:

- підвищення оперативності отримання, аналізу та використання інформації, необхідної для підтримання прийняття рішень щодо керування регіоном.
- підвищення якості та дієвості керуючих рішень завдяки оперуванню достовірною інформацією, отриманою безпосередньо з відповідногоджерела;
- визначення нових аспектів діяльності регіону завдяки аналізу даних, які не потрапляли у традиційні звіти, і тому не враховувалися приприйнятті рішень;
- своєчасного виявлення негативних тенденцій розвитку з метою їх подальшого усунення.

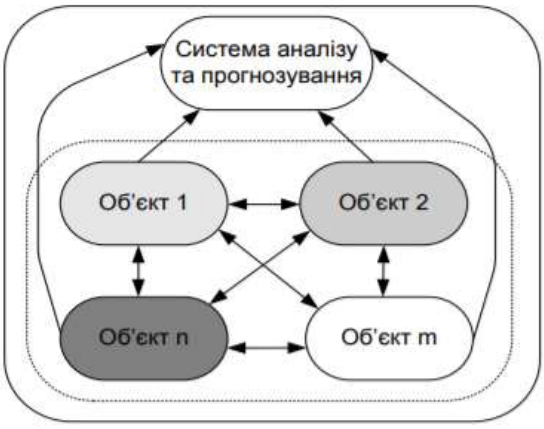


Рис. 13.2. Схема рівноправного обміну данними

Інформаційний бум призвів до збільшення кількості даних, накопичених у багатьох предметних галузях у сотні та тисячі разів. До таких областей відноситься і сфера державного управління. Кількість зібраної інформації зростає експоненційно. Так, за дослідженням *IDC Digital Universe Study* [14], проведеним на замовлення компанії EMC, сумарний обсяг світових даних у2005 році складав 130 ексабайт, до 2011 року він зріс до 1227 EB, а за останній рік знову подвоївся, досягши 3 ZB (зетабайт). Прогноз, здійснений тим же дослідженням, показує, що до 2021 року обсяг цифрових даних зросте до 7.9ZB. Розмір окремих баз даних зростає так само швидко і подолав петабайтний бар'єр. Більшість зібраних даних на даний час не аналізується, або ж проходить лише поверхневий аналіз [15].

Видобування даних є процесом виявлення нових нетривіальних закономірностей з великих масивів інформації. Необхідно зазначити, що прикметник «великий» у застосуванні до даних має тенденцію до постійного зростання значення. Наприклад, за даними *Тіма Суонсона* кількість операцій,що здійснюється щодня в криптовалюті *Bitcoin*, перевищила 100 000 операцій(оригінал у «Щоденний обсяг транзакцій в *Bitcoin* подолав 100-тисячнийбар'єр»: [Режим доступу] http://vkurse.ua/ua/business/ezhednevnyy-obemtranzakciy-v-bitcoin.html).

Основними проблемами, які виникають при обробці даних, є відсутність методів аналізу, придатних до застосування через їх різнотипність (для регіону – це і числові дані, і геодані, слабоструктуровані звіти тощо), потреба у значних людських ресурсах для підтримки процесу аналізу даних, висока обчислювальна складність наявних алгоритмів аналізу та стрімке зростання обсягу зібраних даних. Це в свою чергу призводить до постійного зростання часу, що витрачається на аналіз даних навіть при регулярному оновленні комп'ютерних засобів, а також – необхідність роботи із розподіленими базами даних, можливості яких більшість існуючих методів аналізу даних не використовують ефективно.

13.6. Визначення Великих даних

Концепція Великих даних не нова, вона виникла за часів мейнфреймів і пов'язаних з ними наукових обчислень [16, 18]. Як добре відомо, наукомісткість обчислень завжди було складним завданням. Як правило, вона нерозривно пов'язана з обробкою великих обсягів інформації.

Проте, безпосередньо термін «*Великі дані» (Big Data)* з'явився порівняно недавно. Він є одним з небагатьох, що має відомий день народження – 3вересня 2008 р. Тоді було випущено спеціальний випуск найстарішого британського наукового журналу *Nature*. Журнал присвячений пошукам відповіді на питання: «Як технології можуть вплинути на наукове майбутнє, що відкриває можливості для роботи з Великими даними» [15]. Згідно зі звітом *McKinsey* інституту під назвою «*Великі дані: Наступний рубіж для інновацій, конкуренції і продуктивності*», термін «*Великі дані*» відноситься до наборів даних, розмір яких перевищує ємність звичайної бази даних (БД) для видобування, зберігання, управління і аналізу інформації [15].

EWeek подає визначення, запропоноване дослідницькою компанією *Gartner*: «*Великі дані характеризуються обсягом, різноманітністю і швидкою плинністю структурованих і неструктурованих даних в процесорах і пристроях зберігання даних, а також перетворення даних для задач бізнес-консалтингу для підприємств*» [17].

Великі дані (Big Data) в інформаційних технологіях (за визначенням К. Лінча) – набір методів та засобів опрацювання структурованих і неструктурованих різнотипних динамічних даних великих обсягів з метою їх аналізу та використання для підтримки прийняття рішень [18].

Є альтернативою традиційним системам управління базами даних і рішенням класу *Business Intelligence*. До цього класу відносять засоби паралельного опрацювання даних (No*SQL, алгоритми MapReduce, Hadoop*) [5, 6, 17, 18].

На думку компанії *DCA (Data-Centric Alliance)* під *Big Data* розуміють не якийсь конкретний об'єм даних і навіть не дані, а методи їх обробки, які дозволяють розподілено

обробляти інформацію [11]. Ці методи можна застосовувати як до великих масивів даних (таких як дані всіх сторінок в мережі Інтерет), так і до малих масивів (інформація про денні поступлення товару в магазин).

Визначальними характеристиками для Великих даних є [17] обсяг (*volume*, в сенсі величини фізичного обсягу), швидкість (*velocity* в сенсах якшвидкості приросту, так і необхідності високошвидкісної обробки таотримання результатів), різноманіття (*variety*, в сенсі можливості одночасної обробки різних типів структурованих і слабоструктурованих даних).

Хмарні технології підтримують інфраструктуру віртуалізації та її профілювання для конкретних структур даних або для підтримки конкретних наукових робочих процесів [16].

Розмаїття (Variety) визначається за допомогою [16]:

- реляційних даних (таблиці / транзакції);
- текстових даних (Web), напівструктурованих даних (XML);
- даних на основі графових моделей (соціальна мережа, Semantic Web,RDF);
- потокових даних;
- великих публічних даних (онлайн, погода, фінанси і т.д.).

Є такі види вартості (*Value*) у Великих даних як статистичні дані, події, метадані тощо.

Швидкість *(Velocity) (Speed)* Великих даних подана як:

- дані генеруються швидко і повинні бути опрацьовані швидко,
- он-лайн аналіз даних,
- підтримка прийняття рішень з неповними даними.

Достовірність (Veracity) – поняття, зворотне до невизначеності, яка виникає через невідповідність даних, їх неповноту, латентність [18]. Аналіз даних в системах територіального управління зводиться до вирішення трьох конкретних завдань:

- соціально-економічна оцінка стану природного середовища в регіоні вданий час і перспективі, розроблення на її основі системи заходів по повному запобіганню чи максимальному пом'якшенню негативного впливу господарської діяльності на навколишнє середовище;
- визначення й врахування можливих наслідків змін у природному середовищі в результаті господарської діяльності і техногенних процесів, їх вплив на спеціалізацію і комплексний розвиток господарства регіону;
- врахування прогнозів еколого-економічних процесів у контексті загального комплексного прогнозу соціально-економічного розвитку регіону шляхом формування ряду критеріїв і обмежень як по ресурсах,так і за допомогою показників якісного стану навколишнього середовища.

Незважаючи на те, що термін був введений в академічному середовищі,первинною була проблема зростання кількості і різноманітності наукових даних. Станом на 2009 рік термін став широко поширений у діловій пресі, а до 2010 року з'явилася перша низка інформаційно-технологічних продуктів і рішень, що стосуються виключно проблем обробки великих обсягів даних. З 2011 року більшість найбільших постачальників інформаційних технологій для організацій в їх бізнес-стратегії використовують концепцію Великих даних,у тому числі *IBM, Oracle, Microsoft, Hewlett-Packard , EMC* [5, 10].

Завдання, що виникають під час опрацювання, обробки, інтерпретації,збору та організації Великих даних, з'явилися в численних секторах,включаючи бізнес, промисловість, некомерційні організації. Обсяги даних, такі як операції замовника у роздрібній торгівлі, моніторинг погоди, бізнес-аналіз,можуть швидко випереджувати потужність традиційних методів та інструментів аналізу даних. З'явилися нові методи та інструменти, включаючи бази даних *NoSQL, MapReduce*, обробка природної мови, машинне навчання,візуалізація, придбання, і серіалізація. Усе це стає необхідним, щоб повною мірою усвідомити, що відбувається, коли зростають Великі дані, як вони застосовуються і де починають відігравати вирішальну роль. Також необхідно знати вимоги до існуючих методів розроблення систем і аналізу даних.

Великі дані є терміном, який використовується для ідентифікації наборів даних, з якими ми не можемо впоратися з використанням існуючих методологій та програмних

засобів через їх великий розмір і складність. Багато дослідників намагаються розробити методики і програмні засоби для передачі даних або видобування інформаційних гранул з *Великих даних* [7, 14].

Особливості Великих даних, а саме:

- *робота з неструктурованою та структурованою інформацією,*
- *орієнтація на швидке опрацювання даних, призводять до того, що традиційні мови запитів виявляються малоефективними для роботи з даними* [14].

Концепція «Великі дані» досі не дуже добре окреслена, хоча активно використовується для бізнесу та технологій. Аналіз згаданих вище джерел, науково-популярних журналів, і блогів дають змогу виділити наступні фокуси обговорення [18]:

- джерела Великих даних,
- апаратне забезпечення та інфраструктура,
- програмне забезпечення і зберігання,
- інформаційні технології (методи і засоби обробки даних).
- використання Великих даних, бізнес-аналіз.

В якості джерел Великих даних можна виділити пристрої та людей. Приклади перших джерел: національні та міжнародні проекти, такі як Великийадронний коллайдер (LHC) в ЦЕРН, Лабораторія фізики елементарнихчастинок в Європі, Великий синоптичний оглядовий телескоп на півночі Чилі; промисловість (SCADA, фінанси і т.д.) [11].

Приклади другого типу джерел на рисунку: соціальні мережі, охорона здоров’я, роздрібна торгівля, особисті дані про місцезнаходження, управління громадським сектором і т.д. Для збору і обробки Великих даних доцільно використовувати технології хмарних обчислень. Хмарні обчислення – це нова парадигма для розміщення кластерів даних і надання різних послуг локальною мережею або через Інтернет.

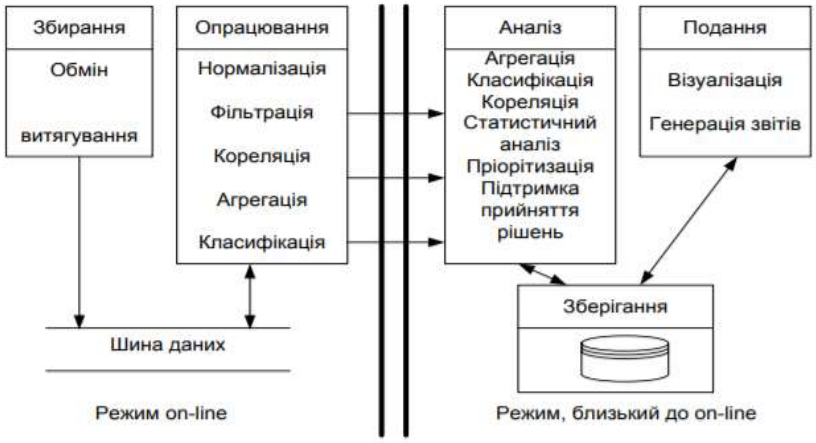


Рис. 13.3. Порівняльна характеристика OLAP та BigData

Хостинг кластерів даних дає змогу клієнтам зберігати та обчислювати величезну кількість даних у хмарі. Оскільки розмір окремих баз даних зростає швидко і подолав петабайтний бар’єр (наприклад, бази даних соціальних мереж),то онлайн опрацювання в режимі *OLAP* таких обсягів практично неможливе.

В таблиці подано відомості щодо ряду інструментів опрацювання Великих даних з відкритим вихідним кодом, які надаються через інфраструктури хмарних обчислень. Більшість інструментів забезпечується *Apache* і випущені під ліцензією *Apache* [19]. Усі ці продукти згруповано за типами задач, що виникають в процесах опрацювання Великих даних.

Засоби роботи з Великими даними [129]

Засоби для Великих даних	Опис
Засоби аналізу	
Ambari http://ambari.apache.org	Інструмент веб для надання послуг, управління та мониторингу Apache Hadoop кластерів
Avro http://avro.apache.org	Система серіалізації даних
Chukwa http://incubator.apache.org/chukwa	Система колекціонування даних для керування великими розподіленими системами
Hive http://hive.apache.org/	Інфраструктура сховища даних, яка забезпечує агрегацію даних
Pig http://pig.apache.org	Високорівнева мова потоків даних і виконуваний framework для паралельних обчислень
Spark http://spark.incubator.apache.org	Швидкий і генеральний обчислювач для даних Hadoop. Забезпечує просту і виразну модель програмування, яка підтримує широкий спектр додатків, у тому числі ETL, машинного навчання, опрацювання потоків
ZooKeeper http://zookeeper.apache.org	Високопродуктивна служба координації для розподілених застосунків
Actian http://www.actian.com/about-us/#overview	Забезпечує зберігання сирих даних і готує дані для подальшого аналіза
HPCC http://hpccsystems.com	Забезпечує швидке перетворення, паралельне опрацювання для застосувань з Великими даними
Засоби Data Mining	
Orange http://orange.biolab.si	Візуалізація та аналіз даних для новачка і експертів
Mahout http:// mahout/apache.org	Бібліотека засобів машинного навчання та випробування данних
KEEL http://keel.es	Еволюційний алгоритм для проблем видобування даних
Засоби соціальних мереж	
Apsche Kafka	Платформа з високою пропускною здатністю для опрацювання даних в режимі реального часу
Засоби BI	
Talend http://www. talend.com	Інтеграція даних, управління, інтеграція застосувань, засоби і сервіси для великих даних
Jedox http://www. jedox.com/en	Функції аналізу, звітності, планування
Pentaho http://www. pentaho.com	Інтеграція даних, бізнес-аналіз, візуілізація даних, прогнозування
Rasdsman http://rasdaman.eecs.jacobs-university.de/	Багатовимірні расторові дані (масив) без обмежень на розмір, наявність мови запитів
Засоби пошуку	
Apache Lucene http://lucene.apache.org	Застосування для повнотекстового індексування і пошуку
Apache Solr http://lucene.apache.org/solr	Повнотестовий пошук, фасетний пошук, динамічна кластеризація, формати документів типу Word, PDF, просторовий пошук
Elasticsearch http://www. Elasticsearch.org	Засіб розподіленого повнотекстового пошуку з веб-інтерфейсом і JSON документами
MarkLogic http://developer.marklogic.apache.com	NoSQL і XML база даних
mongoDB http:// mongodb.apache.org	Крос-платформа документно-орієнтована система управління базами даних з підтримкою JSON та динамічних схем
Cassandra http:// Cassandra.apache.org	Маштабована мульти-майстерня база даних без єдиної точки відмови
HBase http://hbase.apache.org	Маштабована розподілена база даних з підтримкою структурованого зберігання даних великого обсягу
InfiniteGraph http://www.objectivity.com	Розподіленя графована база даних

13.7. Обробка і методи аналізу Big Data

З точки зору обробки в основу технологій *Big Data* покладені два основних принципи:

- розподіленого зберігання даних;
- розподіленої обробки, з урахуванням локальності даних.

Розподілене зберігання вирішує проблему великого обсягу даних, дозволяючи організовувати сховище з довільного числа окремих простих носіїв. Зберігання може бути організовано з різним ступенем надмірності, забезпечуючи стійкість до збоїв окремих носіїв.

Розподілена обробка з урахуванням локальності даних означає, що програма обробки доставляється на обчислювач, що знаходиться якомога ближче до оброблюваних даних. Це принципово відрізняється від традиційного підходу, коли обчислювальні потужності і підсистема зберігання розділені і дані повинні бути доставлені на обчислювач. Таким чином, технології *Big Data* спираються на обчислювальні кластери з безлічі обчислювачів, забезпечених локальної підсистемою зберігання.

Доступ до даних і їх обробка здійснюються спеціальним програмним забезпеченням. Найбільш відомим і інтенсивно розвиваються проектом в області *Big Data* є *Apache Hadoop* [6,7]. В даний час на ринку інформаційних систем і програмного забезпечення синонімом Big Data є технологія Hadoop, яка представляє собою програмний фреймворк, що дозволяє зберігати і обробляти дані за допомогою комп'ютерних кластерів, використовуючи парадигму *MapReduce*. Основними складовими платформи *Hadoop* є:

- відмовостійка розподілена файлова система *Hadoop Distributed File System (HDFS)*, за допомогою якої здійснюється зберігання;
- програмний інтерфейс *Map Reduce*, який є основою для створення програмного забезпечення, що обробляють великі обсяги структурованих і неструктурованих даних паралельно на кластері, що складається з тисяч машин;
- *Apache Hadoop YARN*, що виконує функцію управління даними.

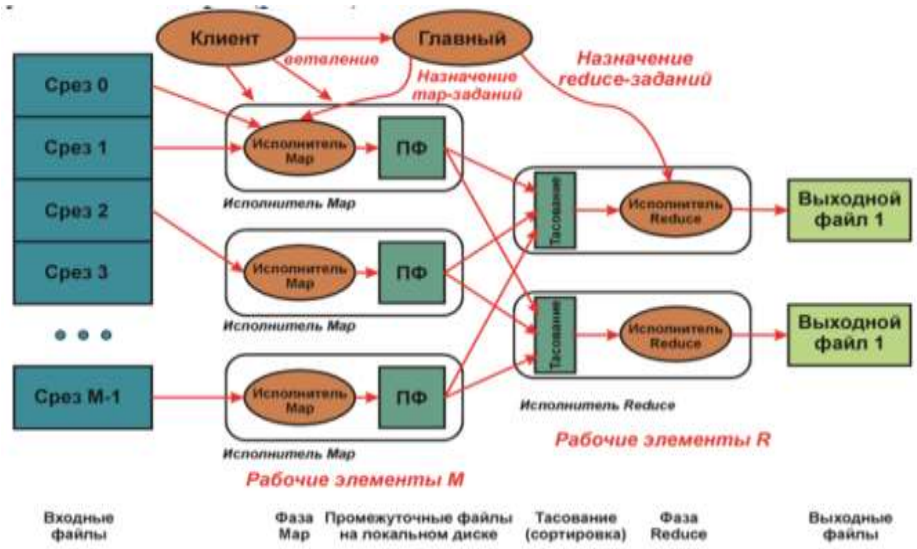


Рис. 13.4. Концептуальна модель MapReduce

Відповідно до підходу *MapReduce* обробка даних складається з двох кроків: *Map і Reduce*. На кроці *Map* виконується попередня обробка даних, яка здійснюється паралельно на різних вузлах кластера.

На кроці *Reduce* відбувається зведення попередньо оброблених даних в єдиний результат.

В основі моделі роботи *Apache Hadoop* лежать три основних принципи.

По-перше, дані рівномірно розподіляються на внутрішніх дисках безлічі серверів, об'єднаних *HDFS*.

По-друге, не дані передаються програмі обробки, а програма - до даних.

Третій принцип - дані обробляються паралельно, причому ця можливість закладена архітектурно в програмному інтерфейсі *Map Reduce*. Таким чином, замість звичної концепції «база даних + сервер» у нас є кластер з безлічі недорогих вузлів, кожен з яких є і сховищем, і обробником даних, а саме поняття «база даних» відсутня.

Платформа *Hadoop* дозволяє скоротити час на обробку і підготовку даних, розширює можливості по аналізу, дозволяє оперувати новою інформацією та неструктурованими даними.

Компанія *Oracle* розбиває життєвий цикл обробки інформації на три етапи і використовує для кожного з них власне рішення:

1) Збір, обробка та структурування даних.

В якості вирішення застосовується *Oracle Big Data Appliance* - це встановлений *Hadoop*-кластер, *Oracle NoSQL Database* і засоби інтеграції з іншими сховищами даних. Завдання *Oracle Big Data Appliance* полягає в зберіганні та первинній обробці неструктурованою або частково структурованої інформації, тобто як раз в тому, що у систем на базі *Hadoop* виходить найкраще.

2) Агрегація і аналіз даних.

Для роботи зі структурованими даними використовується комплекс *Oracle Exadata*. Модулі інтеграції *Oracle Big Data Appliance* дозволяють оперативно завантажувати дані в *Oracle Exadata*, а також отримувати доступ до даних «на льоту» з *Oracle Exadata*.

3) Аналітика даних в реальному часі.

Для максимально оперативного аналізу отриманих даних використовується *Oracle Exalytics Database Machine*, яка дозволяє вирішувати аналітичні завдання фактично в режимі «online». Існує безліч різноманітних методів аналізу масивів даних, в основі яких лежить приблизно однаковий набір інструментів аналізу даних [3]: багатовимірний аналіз (*OLAP*), регресія, класифікація, кластеризація і пошук закономірностей. Деякі з перерахованих методик зовсім не обов'язково можуть бути застосовані виключно до великих даними і можуть з успіхом використовуватися для менших за обсягом масивів (наприклад, A / B-тестування, регресійний аналіз).

Багатовимірний аналіз - суть методу полягає в побудові багатовимірного куба і отриманні його різних зрізів. Результатом аналізу, як правило, є таблиця, в осередках якої містяться агреговані показники (кількість, середнє, мінімальне або максимальне значення і так далі). Залежно від реалізації, існують три типи системи багатовимірного аналізу (*OLAP*): багатовимірна *OLAP* (*Multidimensional OLAP - MOLAP*); реляційна *OLAP* (*Relational OLAP - ROLAP*); гібридна *OLAP (Hybrid OLAP - HOLAP*). Серед них *ROLAP*-системи є найбільш прозорими і вивченими, оскільки ґрунтуються на широко поширених реляційних *СУБД*, в той час як внутрішній устрій *MOLAP* і *HOLAP* зазвичай більш закрита і відноситься до області «ноу-хау» конкретних комерційних продуктів.

MOLAP представляє інформацію у вигляді «чесної» багатовимірної моделі, але всередині використовуються ті ж підходи, що і в *ROLAP*: схеми «зірка» та «сніжинка». З точки зору СУБД база даних *ROLAP* - це звичайна реляційна база, і для неї необхідно підтримувати весь перелік операцій. Однак це не дозволяє, по-перше, жорстко контролювати етапи введення даних. По-друге, збирати статистику і підбирати оптимальні структури для зберігання індексів. По-третє, оптимізувати розміщення даних на диску для забезпечення високої швидкості введення / виводу. По-четверте, при виконанні аналітичних запитів через високі вимоги до швидкодії немає можливості провести глибокий статистичний аналіз і виробити оптимальний план виконання. У *ROLAP* використовуються «рідні» реляційні оптимізатори запиту, які ніяк не враховують «багатовимірність» бази даних. Технології *MOLAP* позбавлені перелічених недоліків і завдяки цьому дозволяють домогтися більшої швидкості аналізу.

Вибір технології *MOLAP / ROLAP / HOLAP* при аналізі Big Data залежить від частоти оновлення бази даних. З точки зору розпаралелювання обробки, на перший погляд, все просто - будь-який багатовимірний куб може бути «розрізаний *MOLAP* представляє інформацію у вигляді «чесної» багатовимірної моделі, але всередині використовуються ті ж підходи, що і в *ROLAP*: схеми «зірка» та «сніжинка». З точки зору СУБД база даних *ROLAP* -

це звичайна реляційна база, і для неї необхідно підтримувати весь перелік операцій. Однак це не дозволяє, по-перше, жорстко контролювати етапи введення даних. По-друге, збирати статистику і підбирати оптимальні структури для зберігання індексів. По-третє, оптимізувати розміщення даних на диску для забезпечення високої швидкості введення / виводу.

По-четверте, при виконанні аналітичних запитів через високі вимоги до швидкодії немає можливості провести глибокий статистичний аналіз і виробити оптимальний план виконання. У *ROLAP* використовуються «рідні» реляційні оптимізатори запиту, які ніяк не враховують «багатовимірність» бази даних. Технології *MOLAP* позбавлені перелічених недоліків і завдяки цьому дозволяють домогтися більшої швидкості аналізу.

Наприклад, якщо користувач запитує статистику продажів по країні за вказаний проміжок часу, а дані розподілені за кількома регіональним ОЛР-серверів, то кожен сервер повертає свою власну відповідь, які потім збираються воєдино. Якщо ж дані будуть розподілені по тимчасовому критерію, то при виконанні даного прикладу запиту все навантаження ляже на один сервер.

Проблема в тому, що, по-перше, дуже важко заздалегідь визначити оптимальний розподіл даних по серверах, а по-друге, для частини аналітичних запитів може бути заздалегідь невідомо, які дані і з яких серверів знадобляться.Стосовно до Великих Даним це означає, що існуючі підходи для багатовимірного аналізу можуть добре масштабироваться і що вони допускають розподілений збір інформації - кожен сервер може самостійно збирати інформацію, здійснювати її очищення і завантаження в локальну базу.

Регресія - під регресією розуміють побудову параметричної функції, яка описує зміну зазначеної числової величини в зазначений проміжок часу. Ця функція будується на основі відомих даних, а потім використовується для передбачення подальших значень цієї ж величини. На вхід методу надходить послідовність пар виду «час - значення», що описує поведінку цієї величини при заданих умовах, наприклад, кількість продажів конкретного виду товару в конкретному регіоні.

На виході - параметри функції, яка описує поведінку досліджуваної величини. Незалежно від виду використовуваної параметричної функції підбір значень її параметрів здійснюється одним і тим же способом. Обчислюється сумарна різниця між що спостерігаються значеннями і значеннями, які дає функція при поточних значеннях її параметрів. Потім визначається, як слід підкоригувати значення параметрів для того, щоб зменшити поточну сумарну різницю. Ці операції повторюються до тих пір, поки сумарна різниця не досягне необхідного мінімуму або її подальше зменшення стане неможливим. З точки зору обробки даних при регресійному аналізі ключовими операціями є обчислення поточної сумарною різниці і коригування значень параметрів. Якщо перша операція розпараллелюється очевидним чином (сума обчислюється по частинах на окремих серверах, а потім підсумовується на центральному сервері), то з другої складніше.

У найбільш загальному випадку при коригуванні ваг використовують загальновідомий математичний факт: функція декількох параметрів зростає в напрямку градієнта і убуває в напрямку, протилежному градієнту. У свою чергу, обчислення градієнта полягає в обчисленні приватних похідних функції по кожному з параметрів, що зводиться до дискретного диференціювання,заснованому на обчисленні зважених сум. В результаті коригування значень параметрів також зводиться до підсумовування, яке може бути розпаралеліть [18].

Якщо регресійний аналіз зводиться до обчислення зважених сум, то він має приблизно тим же ступенем застосовності і при роботі з *Big Data*, що і багатовимірний аналіз. Таким чином, системи регресійного аналізу хвилі можуть масштабуватися і працювати в умовах розподіленого збору інформації. Класифікація - її завдання частково схожа на завдання регресії і полягає в спробі побудови і використання залежності однієї змінної від декількох інших. Наприклад, маючи базу даних про ціну об'єктів нерухомості, можна побудувати систему правил, що дозволяє на основі параметрів нового об'єкта передбачити його приблизну ціну.

Відмінність класифікації від регресії полягає в тому, що аналізується не тимчасовою ряд - подаються на вхід значення ніяк не можуть бути впорядковані. На поточний момент

розроблено безліч методів класифікації (функції Байеса, нейронні мережі, машини підтримують векторів, дерева рішень і т. Д.), Кожен з яких має під собою добре опрацьовану наукову теорію. Разом з тим всі методи класифікації будуються по одній і тій же схемі. Спочатку проводиться навчання алгоритму на порівняно невеликій вибірці, а потім - застосування отриманих правил до іншої вибірці. На першому етапі можливо копіювання масиву даних на один сервер для запуску «класичного» алгоритму навчання без розпаралелювання роботи. Однак на другому етапі дані можуть оброблятися незалежно - система правил, отримана за підсумками самонавчання, копіюється на кожен сервер, і через неї проганяється весь масив даних, що зберігається на цьому сервері. Отримані результати можуть або зберігатися там же на сервері, або відправлятися для подальшої обробки.

Таким чином, на етапі навчання класифікаторів про роботу з *Big Dat*а поки мова не йде - не існує вибірок такого обсягу, підготовлених для навчання систем, а на етапі класифікації окремі порції даних обробляються незалежно один від одного.

Кластеризація - її завдання полягає в розбитті безлічі інформаційних сутностей на групи, при цьому члени однієї групи більш схожі один на одного, ніж члени з різних (класифікація відносить кожен об'єкт до однієї з заздалегідь визначених груп). В якості критерію схожості використовується функція-відстань, на вхід якої надходять дві сутності, а на вихід - ступінь їх схожості. Відомо безліч різних способів кластеризації (графові, ієрархічні, ітеративні, мережі Кохонена).

Проблема кластеризації *Big Data полягає* в тому, що наявні алгоритми припускають можливість безпосереднього звернення до будь-якої інформаційної суті у вихідних даних (заздалегідь неможливо передбачити, які саме сутності знадобляться алгоритму). У свою чергу, вихідні дані можуть бути розподілені по різних серверах, і при цьому не гарантується, що кожен кластер зберігається строго на одному сервері. Якщо розподіл даних по серверах робити прозорим для алгоритму кластеризації, то це неминуче призведе до копіювання великих обсягів з одного сервера на інший.

Рішення проблеми може бути наступним. На кожному сервері запускається свій алгоритм, який оперує тільки даними цього сервера, а на виході дає параметри знайдених кластерів і їх ваги, які оцінюються виходячи з кількості елементів всередині кластера. Потім отримана інформація збирається на центральному сервері і проводиться метакластерізація - виділення груп близько розташованих кластерів з урахуванням їх ваг.

Цей метод універсальний, добре распараллеливается і може використовувати будь-які інші алгоритми кластеризації, однак він вимагає проведення серйозних наукових досліджень, тестування на реальних даних і порівняння отриманих результатів з іншими «локальними» методами. Таким чином, для аналізу *Big Data* переважна частина методів кластеризації непридатна в чистому вигляді і необхідні додаткові дослідження.

Пошук закономірностей - суть методу полягає в знаходженні правил, що описують взаємозалежності між внутрішніми елементами даних. Класичним прикладом є аналіз покупок в супермаркеті і виявлення правил виду «якщо людина купує фотоапарат, то зазвичай він купує ще до нього акумулятор і карту пам'яті». На вхід завдання пошуку закономірностей надходить неврегульована безліч сутностей, для кожної з яких відомий набір присутніх інформаційних ознак; наприклад, такими сутностями можуть бути чеки на покупки, а ознаками - куплені товари [19].

Завдання пошуку закономірностей зводиться до виявлення правил виду «якщо присутні ознаки Ai, A2, ..., An, то присутні і ознаки Б1; B2, ..., Bm, при цьому кожне правило характеризується двома параметрами: ймовірністю спрацьовування і підтримкою. Перший параметр показує, як часто виконується дане правило, а другий - як часто можна застосувати дане правило, тобто як часто зустрічається поєднання ознак A1, A2, ..., An.

A / B тестування - методика, в якій контрольна вибірка по черзі порівнюється з іншими. Таким чином удасться виявити оптимальну комбінацію показників для досягнення, наприклад, найкращою відповідної реакції споживачів на маркетингову пропозицію. Великі дані дозволяють провести величезну кількість ітерацій і таким чином отримати статистично достовірний результат.

Краудсорсінг - методика збору даних з великої кількості джерел: категоризація і збагачення даних силами широкого, невизначеного кола осіб.

Змішання і інтеграція даних - набір технік, що дозволяють інтегрувати різнорідні дані з різноманітних джерел для можливості глибинного аналізу.

Машинне навчання («штучний інтелект») - має на меті створення алгоритмів самонавчання на базі статистичного аналізу даних або машинного навчання для отримання комплексних прогнозів.

Генетичні алгоритми - в цій методиці можливі рішення представляють у вигляді «хромосом», які можуть комбінуватися і мутувати. Як і в процесі природної еволюції, виживає найбільш пристосована особина. Оптимізація - набір чисельних методів для ре-дизайну складних систем і процесів для поліпшення одного або декількох показників. Допомагає в прийнятті стратегічних рішень, наприклад, складу виведеної на ринок продуктової лінійки, проведенні інвестиційного аналізу. Візуалізація аналітичних даних - методи для подання інформації у вигляді малюнків, графіків, схем і діаграм з використанням інтерактивних можливостей та анімації як для результатів, так і для використання в якості вихідних даних.

13.8. Хмарна платформа Oracle для Big Data

Корпорація Oracle анонсувала хмарне рішення Oracle Cloud Platform for Big Data, компонент портфоліо PaaS-сервісів.

Рис. 13.5. Хмарна платформа Oracle для Big Data

Ключові вимоги середовища для роботи з big data включають в себе:

- ***Масштабованість***. Через високий і швидкого приросту даних будь-яка система завжди повинна бути готова до розширення.
- ***Відмовостійкість***. Якась частина машин в кластері, які проводять аналіз, гарантовано буде виходити з ладу, наслідки цього не повинні позначатися на процесі обробки інформації.

Контрольні питання до розділу

1. Дайте визначення терміну «Великі дані (Big Data)». Які операції при цьому повинні здійснюватися?
2. Які принципи роботи з великими даними відомі?
3. Які використовуються технології і тенденції роботи з Big Data?
4. В чому полягає обчислювальна парадигма *MapReduce?*
5. Які існують методи і техніка анализу великих даних?
6. Особливості великих даних у промисловості.

7. Технології *Big Data* можуть бути корисними при вирішенні наступних задач:
   a. *прогнозування ринкової ситуації;*
   b. *маркетинг і оптимізація продажів;*
   c. *вдосконалення продукції;*
   d. *ухвалення управлінських рішень;*
   e. *підвищення продуктивності праці;*
   f. *ефективна логістика;*
   g. *моніторинг стану основних фондів.*
8. Завдяки моніторингу інформації у режимі реального часу персонал підприємства має змогу:
   a. *скорочувати кількість простоїв;*
   b. *підвищувати продуктивність обладнання;*
   c. *зменшувати витрати на експлуатацію обладнання;*
   d. *запобігати нещасним випадкам.*
9. Процес консолідації даних для аналізу та прогнозування розвитку регіону генерує наступні задачі:
   a. *підвищення оперативності отримання, аналізу та використання інформації, необхідної для підтримання прийняття рішень щодо керування регіоном;*
   b. *підвищення якості та дієвості керуючих рішень завдяки оперуванню достовірною інформацією, отриманою безпосередньо з відповідногоджерела;*
   c. *визначення нових аспектів діяльності регіону завдяки аналізу даних, які не потрапляли у традиційні звіти, і тому не враховувалися приприйнятті рішень;*
   d. *своєчасного виявлення негативних тенденцій розвитку з метою їх подальшого усунення.*
10. Визначення Великих даних.
11. Порівняльна характеристика OLAP та BigData.
12. Обробка і методи аналізу Big Data.
13. Концептуальна модель MapReduce.
14. В чому полягає сутність багатовимірного аналізу? Типи системи багатовимірного аналізу.
15. Дайте визначення поняттю «регресія».
16. Дайте визначення поняттю «кластерізація».
17. Дайте визначення поняттю «пошук закономірностей».
18. Які існують методики «пошуку закономірностей»?
19. Ключові вимоги середовища для роботи з big data хмарної платформи Oracle для Big Data.

Список рекомендованої літератури

1. Н. Б. Шаховська, Ю. Я. Болюбаш Модель великих даних “сутність- характеристика”. [Електронний ресурс] Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/29775/1/20_186-196.pdf
2. А. Найдич Большие данные: насколько они большие? [Електронний ресурс] Режим доступу: http://compress.ru/article.aspx?id=23469
3. Большие_данные_(Big_Data) [Електронний ресурс] Режим доступу: http://www.tadviser.ru/index.php/Статья:Большие_данные_(Big_Data)
4. Что такое BigData? [Електронний ресурс] Режим доступу: https://rb.ru/howto/chto-takoe-big-data/
5. Что такое Big Data? [Електронний ресурс] Режим доступу: https://postnauka.ru/faq/46974

6. Is Big Data a Bubble Set to Burst?[Електронний ресурс]Режимдоступу:https://www.datacenterknowledge.com/archives/2015/03/30/big-data-bubble-set-burst
7. Большие_данные (Big_Data)? [Електронний ресурс] Режим доступу: http://www.tadviser.ru/index.php/Статья: Большие_данные (Big_Data).
8. Большие_данные [Електронний ресурс] Режим доступу: https://ru.wikipedia.org/wiki/Большие_данные
9. BigData[Електронний ресурс] Режимд оступу: https://intellect.ml/big-data-6821
10. Большие данные [Електронний ресурс]Режим доступу: http://sewiki.ru/index.php?title=Большие_данные&oldid=3075
11. Big data the next frontier for innovation [Електронний ресурс] Режим доступу: http://www.mckinsey.com/insights/business_technology/big_data_the_next_fro ntier_for_innovation
12. Технологии Big Data и их применение на современном промышленном предприятии [Електронний ресурс] Режим доступу: http://engjournal.ru/articles/1228/1228.pdf
13. BigData в промышленности: инновации, к которым придется привыкать [Електронний ресурс] Режим доступу: http://www.ogcs.com.ua/index.php/articles/121-big-data-v-promyshlennosti-innovatsii-k-kotorym-pridetsya-privykat
14. Shakhovska N. B. Big Data federated repository model / N. B. Shakhovska,Y. J. Bolubash, O. M. Veres // Proceedings of 13th International Conference: The Experience of Designing and Application of CADSystems in Microelectronics, CADSM, 24-27 February 2015, Lviv. – Lviv,2015. – P. 382–384.
15. «Big Data» [Електронний ресурс]. Режим доступу: http://www.tadviser.ru/index.php/Статья:Большие_данные_%28Big_Data%29#cite_note-g-6 .
16. Ohlhorst Frank J. A Cloudy Year for Big Data. eWeek [Electronic Resours] / Frank J. Ohlhorst. – Access mode: http://www.eweek.com/c/a/Cloud-Computing/2012-A-Cloudy-Year-for-Big-Data-102807.
17. Chernyak L. Big Data - the new theory and practice. Open the system[Electronic Resours] / Leonid Chernyak. – M. : Open Systems, 2011. – №10. – Access mode: http://www.osp.ru/os/2011/ 10/13010990.
18. «Big Data» Brighten BI Future. eWeek [Electronic Resours]. – Accessmode: http://www.eweek.com/c/a/Data-Storage/TBA-Hadoop-Yahoo-BigData-Brightens-BI-Future-254079.
19. Gartner Says Solving «Big Data» Challenge Involves More Than JustManaging Volumes of Data. [Electronic Resours]. – Access mode:http://www.gartner.com/newsroom/id/1731916.

РОЗДІЛ 14. SMART GRID

14.1. Історія розвитку енергосистем

Перша електрична мережа змінного струму була встановлена у 1886 у Грейт Беррінгтон, Масачусетс [1]. Того часу мережа була централізованою односпрямованою системою передачі та розподілу електричної енергії з керуванням за запитом.

У 20-му сторіччі локальні мережі зростали та були з'єднані з економічних міркувань та міркувань надійності. Протягом 60-х років 20-го ст. електричні мережі стали дуже великими, зрілими та дуже взаємоз'єднаними з тисячами 'центральних' генерувальних електростанцій, які постачають електроенергію до основних центрів споживання по лініям електропередач високої потужності, які розгалужуються для того, щоб доставити електроенергію до менших промислових та домашніх споживачів по всій території постачання. Топологія мереж 1960-х була результатом сильного ефекту масштабу: великі вугільні, газові і мазутні електростанції масштабу в 1 ГВт (1000 МВт) до 3 ГВт є рентабельним, через особливості ефективності: станції є рентабельними тільки у дуже великих масштабах.

Теплові електростанції були розміщені близько джерел викопного палива (власне копальні або порти, залізниці). Вибір майданчиків гідроелектростанцій в гірських районах також сильно вплинув на структуру мережі. Атомні електростанції були розташовані на з урахуванням наявності охолоджувальної води. Нарешті, теплові електростанції були дуже забруднюють навколишнє середовище, і розташовані подалі від населених пунктів в міру економічної можливості, наскільки це допускається розподільними електричними мережами. До кінця 1960-х років, електромережі досягли переважну більшість населення розвинутих країн, і тільки віддалені регіони залишились 'позамережевими'.

Облік споживання електроенергії по кожному споживачу необхідний для того, щоб забезпечити відповідне виставлення рахунків відповідно до високо змінного рівня споживання різних користувачів. Через обмежений збір даних і можливості обробки в період зростання мереж, були широко розповсюджені механізми фіксованих тарифів, а також угоди з подвійними тарифами, коли вночі енергія постачається за нижчими цінами, ніж удень.

Мотивацією для подвійного тарифу домовленостей було зниження попиту нічною добою. Подвійні тарифи уможливили використання дешевої електроенергії у нічний час у таких додатках, як підтримання 'теплових банків', призначених для згладжування денних потреб і зменшення кількості турбін, які необхідно вимкнути на ніч, тим самим покращуючи використання і рентабельність генерувальних і розподільчих об'єктів. Можливості обліку мережі 1960-х означали технологічні обмеження на ступінь, в якій цінові сигнали могли бути поширені по системі.

З 1970-х по 1990-і ростучі потреби привели до зростання кількості електростанцій. На деяких територіях постачання електроенергії, особливо у моменти пікового споживання, не могло задовольнити потреби. результатом чого були масові відключення та погіршення якості електроенергії. Все більше від електрики залежали промисловість, опалення, зв'язок, освітлення, і розваги, і тому споживачі, вимагають все більш високі рівні надійності.

До кінця 20-го століття була встановлена структура попиту на електроенергію: побутове опалення та кондиціювання повітря призвело до денних піків споживання, яким відповідали піки генерації, у яких генератори вмикались на короткий час. Порівняно низьке завантаження цих "пікових" генераторів разом з необхідною надмірністю в електромережі, привели до високих витрат для електроенергетичних компаній, які були перекладені на споживачів у вигляді збільшених тарифів. У 21-му столітті, деякі країни, що розвиваються, такі як Китай, Індія і Бразилія показали лідерство у впровадженні розумних енергосистем [2].

14.2. Можливості модернізації

З початку 21-го століття, можливості використання удосконалень у технологіях електронних комунікацій для усунення обмежень і витрат у електричних мережах стали очевидними. Технологічні обмеження у вимірюванні більше не примушували усереднювати і розподіляти на всіх споживачів в рівній мірі пікові ціни на електроенергію. Паралельно зростає стурбованість у зв'язку з нанесенням шкоди навколишньому середовищу електростанціями на викопному паливі, що привело до бажання використовувати великі обсяги енергії з поновлюваних джерел. Панівні форми, такі як енергія вітру і сонця, дуже непостійні та тому стала очевидною потреба у досконаліших системах управління для полегшення підключення цих джерел до високо контрольованої мережі [3].

Енергія від сонячних батарей (і в меншій мірі вітрових турбін) також важлива у розгляді питання щодо імперативу великих централізованих електростанцій. Швидко падучі витрати вказують на істотну трансформацію від централізованої топології мережі до сильно розподіленої, де енергія одночасно генерується і споживається у межах мережі.

Нарешті, ростуче занепокоєння з приводу терористичних атак в деяких країнах привело до закликів до будівництва більш надійної енергосистеми, яка менше залежить від централізованих електростанцій, які розглядаються як потенційні об'єкти атаки [4].

14.3. Системи на базі технологічної платформи Smart Grid

Сучасний розвиток паливно-енергетичного комплексу у глобальному та національному масштабах має відповідати не тільки новим цілям і тенденціям розвитку світової та національних економік країн у XXI ст., але й новому характеру загроз економічного, екологічного та соціального характеру.

Дослідження проблем, пов’язаних з негативним впливом діяльності людини на навколишнє середовище, та шляхів його зменшення призвело до розробки ще в 90-х рр. XX ст. основних положень стратегії «*сталого розвитку – sustainable development*». При цьому термін «сталий розвиток» розглядається як розвиток, при якому задоволення сьогоденних потреб людини не призводить до обмежень здатності майбутніх поколінь задовольняти їхні потреби. Для забезпечення сталого розвитку суспільства мають бути забезпечені відповідні умови функціонування всіх його складових, серед яких однією з найважливіших є енергетика.

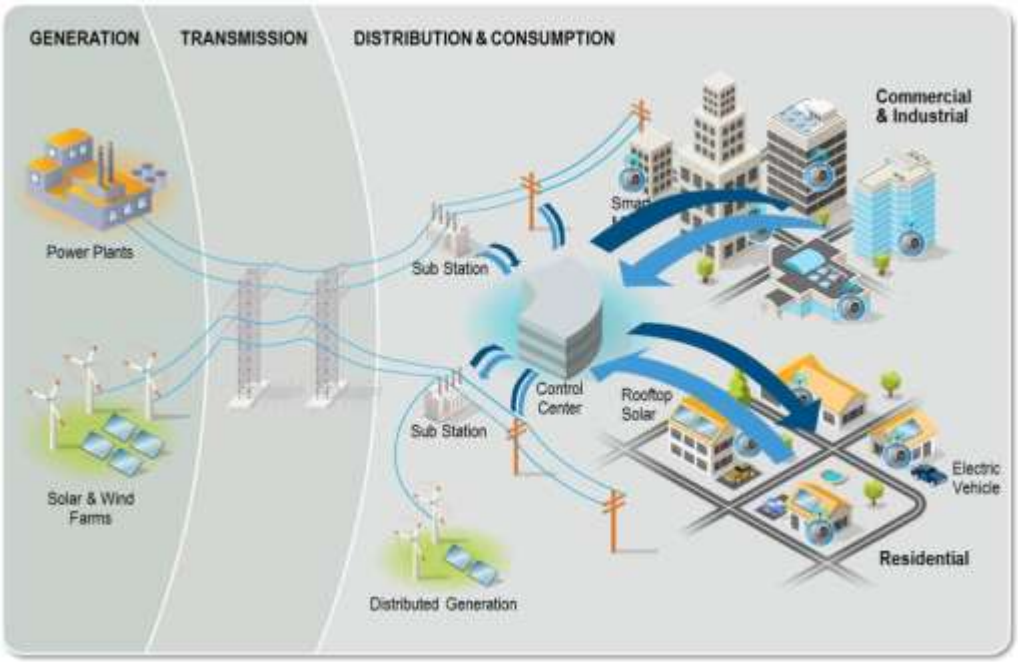


Рис. 14.1. Системи на базі технологічної платформи Smart Grid

У світі відбулися значні зміни щодо стратегії розвитку енергетики. Був визначений комплекс завдань для різних країн з побудови енергетичних стратегій XXI ст. Головний наголос зроблено на забезпеченні нерозривності та узгодженості дій при забезпеченні трьох складових: енергозабезпечення (безперебійне постачання електричною енергією відповідної якості), енергодоступність (енергоощадність та доступна ціна на електроенергію) та енергоприйнятність (мінімальний вплив на навколишнє середовище). Ці складові розглядаються як основа для досягнення глобальної мети – забезпечення стабільного розвитку, що гарантує стале зростання економіки, рівня життя населення, захист навколишнього природного середовища.

Проведений аналіз можливих шляхів розвитку електроенергетики показав наявність серйозних обмежень можливостей розвитку електроенергетичної галузі в рамках колишньої екстенсивної концепції, заснованої переважно на покращенні окремих видів обладнання і технологій. Одним із магістральних шляхів розвитку енергетики визначено шлях її «інтелектуалізації».

Для оцінки рівня «інтелектуалізації» енергетики у світі став загальновживаним у світі термін *Smart*. За найбільш поширеним трактуванням *Smart Grid* – концепція повністю інтегрованої, саморегулюючої і самовідновлюваної електроенергетичної системи, що має мережеву топологію і включає в себе всі генеруючі джерела, магістральні та розподільні мережі і всі типи споживачів електричної енергії, керовані єдиною мережею інформаційно-керуючих пристроїв і систем в режимі реального часу.

Так, в США концепції *Smart Grid* відводиться роль революційної ініціативи, яка дає енергетиці «друге дихання» і стимулює економічний розвиток. Концепція *Smart Grid* в країнах ЄС розглядається як ідеологія загальноєвропейської програми розвитку електроенергетики, база інноваційної модернізації та перетворення електроенергетики, основа побудови «Європейської електричної мережі майбутнього».

Сьогодні зворот «інтелектуальна енергетика» стає терміном, що позначає нові принципи роботи енергетики, як в Україні, так і за кордоном. Сучасні електронні, інформаційні, телекомунікаційні, обчислювальні технології вдосконалюють процеси енерговиробництва та керування енергетичними потоками на підприємствах, роблять їх надійними, безпечними і ефективними, наділяють споживача новими можливостями.

У цьому шарі також присутні спеціалізовані процеси для обробки таких функцій, як хмарне обчислення та керування даними.

Рівень управління сервісом діє як проміжне програмне забезпечення для системи IoT. Цей шар надає конкретні послуги своєму запиту на основі адрес і імен. Забезпечує гнучкість програмістів IoT у роботі над різними типами неоднорідних об'єктів незалежно від їхніх платформ. Цей шар також обробляє дані, отримані від транспортного рівня. Після обробки даних приймаються необхідні рішення щодо надання необхідних послуг, які потім виконуються за допомогою мережевих протоколів.

Виникла нагальна необхідність у розробці нових підходів до керування зростаючими та різноплановими за інтенсивністю і напрямками потоками паливно-енергетичних ресурсів (ПЕР), що дозволяє безпечно та ефективно їх використовувати в існуючих і майбутніх енергетичних системах, зокрема, необхідно відзначити актуальність розробка положень концепції *Smart Grid* та її адаптації до українських реалій.

В основу реалізації такої концепції мають бути покладені наступні принципові позиції:

- енергетика є інфраструктурної базою розвитку економіки, в якій зацікавлені всі інститути: держава, бізнес, наука, населення; товари та послуги, вироблені в енергетичному секторі, мають високий рівень суспільної значущості і практично не мають замінників.
- оптимізація якості та ефективності використання всіх видів ресурсів (паливних, технічних, управлінських, інформаційних тощо) і енергетичних активів;
- у сучасному і майбутньому суспільстві енергія розглядається як джерело (інструмент або засіб), що забезпечує отримання людиною та суспільством певних споживчих цінностей (життєвих благ, рівня комфорту тощо);

– визначаючи для себе такий набір, рівень і характеристики цих цінностей, споживач (з урахуванням його особливостей) не повинен отримувати обмеження з боку енергетики, вибираючи, де йому жити, якими приладами та послугами користуватися, здійснювати свою діяльність і т.ін.;
– задоволення потреби в електричній енергії суспільства у XXI ст. має здійснюватися при одночасному істотному зниженні тиску на екологію планети.

У рамках концепції *Smart Grid* інтелектуальна електроенергетична система розглядається як єдина мережа інформаційно-керуючих систем, що забезпечує:
– інтеграцію всіх видів генерації (у тому числі малої генерації) і будь-які типи споживачів (від домашніх господарств до великої промисловості) для ситуаційного керування попитом на їхні послуги та забезпечення активної їх участі у роботі енергосистеми;
– зміну в режимі реального часу параметрів і топології мережі за поточними режимними умовами, виключаючи виникнення та розвиток аварій;
– розширення ринкових можливостей інфраструктури шляхом взаємного надання широкого спектру послуг суб'єктами ринку та інфраструктурою;
– мінімізацію втрат, розширення самодіагностики і самовідновлення при дотриманні умов надійності та якості електроенергії;
– інтеграцію електромережевої та інформаційної інфраструктури для створення всережимної системи керування з повномасштабним інформаційним забезпеченням.

Спільним елементом для більшості визначень є застосування цифрової обробки і цифрових комунікацій з енергосистемою, що створює потік даних і управління інформацією центром розумної енергосистеми. Результатом глибоко використання цифрових технологій інтегрованих енергосистеми є різні нові можливості. Інтеграція нової інформації з енергосистеми є одним з ключових питань при проектуванні інтелектуальних мереж.

Електроенергетика зараз через три класи перетворень: поліпшення інфраструктури, називається *міцна мережа* в Китаї; Додавання цифрового шару, який є суттю *інтелектуальної мережі*; і трансформація бізнес-процесів, необхідна для отримання вигоди з інвестицій в технології розумних енергосистем. Велика частина роботи, яка була відбувається в модернізації енергосистем, особливо підстанцій та автоматизації розподілу, в даний час включена в загальну концепцію розумної енергосистеми.

Технології розумних енергосистем вийшли з ранніх спроб використання електронного управління, вимірювання і моніторингу. У 1980 році автоматичне зчитування показань було використане для моніторингу споживання великих клієнтів, і перетворилася в автоматизовану систему комерційного обліку електроенергії 1990-х років, чиї вимірювання зберігали дані про те, як електрика використовується в різний час доби [5]. Інтелектуальні лічильники додають безперервний зв'язок, що дозволяє виконання моніторингу у реальному часі, та стають шлюзом до пристроїв, що реагують на попит, та інтелектуальних розеток у домогосподарстві. Ранніми формами таких технологій керування з боку попиту були пристрої, що реагують на попит, які пасивно отримують інформацію про завантаження енергосистеми спостерігаючи за змінами частоти струму.

Індустріальні та домашні кондиціонери, холодильники та нагрівачі підлаштовували свої цикли роботи щоб уникнути включення, коли енергосистема проходить пік споживання. Починаючи з 2000-го року проект Telegestore в Італії вперше об’єднав велику кількість (27 мільйонів) домогосподарств, які використовують інтелектуальні лічильники, у мережу вузькосмуговими каналами зв'язку по лініям електроживлення.[6]. У деяких експериментах використовувався широкосмуговий зв'язок по лініям електроживлення, тоді як у інших використовувались безпровідні технології, такі як mesh-мережі, що сприяло більш надійному з'єднанню різнорідних пристроїв у будинку, а також підтримувало облік інших комунальних послуг, таких як газ і вода [7].

Моніторинг та синхронізація через глобальні мережі стала революцією на початку 1990-х, коли Енергетична адміністрація Бонневіля розширила свої дослідження розумних енергосистем прототипом датчика фази, який дозволяє виконувати швидкий аналіз аномалій якості електроенергії на дуже великих географічних просторах. Кульмінацією цієї роботи

стала робота першої глобальної системи керування у 2000 [8]. Інші країни швидко інтегрували цю технологію — Китай започаткував всеосяжну національну систему керування в 2012 році [9].

Ранні розгортання розумних енергосистем включають італійську систему *Telegestore* (2005), mesh-мережу у Остіні, Техас (з 2003), і розумну енергосистему у Баулдері, Колорадо (2008).

14.4. Властивості розумних енергосистем

Надійність

Розумна енергосистема буде використовувати технології оцінки стану [10], які покращують **виявлення несправностей** і дозволяють **самовідновлення** мережі без втручання фахівців. Це дозволить забезпечити більш надійну подачу електроенергії, а також зниження вразливості до стихійних лих або нападу.

Хоча дубльовані маршрути рекламуються як особливість розумної енергосистеми, старі електромережі також забезпечували кілька маршрутів. Початкові лінії електропередач в електромережі були побудовані з використанням радіальної моделі, пізніше підключення було гарантовано за допомогою декількох маршрутів, відповідно до мережевої структури.

Проте, це створило нову проблему: якщо струм або пов'язані ефекти по мережі перевищують обмеження будь-якого конкретного елемента електромережі, він може відмовити, і струм буде передаватися через інші елементи мережі, які в кінцевому підсумку можуть також відмовити, викликаючи ефект доміно. Методикою запобігання цьому є скидання навантаження по методом віялових відключень або зниження напруги [11].

Економічний ефект від підвищення надійності та стійкості електромережі є предметом ряду досліджень і може бути розрахована з використанням методології, розробка якої профінансована Міністерством енергетики США, для місць США з використанням щонайменше одного інструменту розрахунків.

Гнучкість топології мережі

Інфраструктура наступного покоління для передачі та розподілу електроенергії буде краще пристосована для двонаправлених потоків енергії, що дозволяє розподілену генерацію від сонячних батарей на дахах будинків, паливних елементів, заряджання/розряджання батарей електромобілів, вітрових турбін, гідроакумулювальних електростанцій та інших джерел.

Класичні електромережі сконструйовані для односпрямованої передачі електроенергії, а коли у місцевій підмережі виробляється енергії більше, ніж споживається, зворотній потік енергії може викликати проблеми з надійністю і безпечністю [12]. Розумні енергосистеми придатні для роботи у цих ситуаціях [7].

Ефективність

Численні внески в загальне поліпшення ефективності енергетичної інфраструктури очікуються від розгортання технології розумної енергосистеми, зокрема в тому числі керування попитом, наприклад відключення кондиціонерів у короткочасні піки в ціні електроенергії reducing the voltage when possible on distribution lines, зниження напруги, коли це можливо на розподільчих лініях через оптимізації *Напруга / Реактивна потужність*, усуваючи виїзди для зняття показань лічильників, а також зниження кількості виїздів щодо поліпшення керування відключеннями за рахунок використання даних систем передової вимірювальної інфраструктури. Загальним ефектом стало зменшення надлишковості в лініях передачі і розподілу, а також більш повне використання генераторів, що призвело до зниження цін на електроенергію.

Скорочення/вирівнювання піків і ціноутворення відповідно до часу

Щоб зменшити попит у дорогі періоди активного використання, комунікації та вимірювальні технології інформують інтелектуальні пристрої в будинку і бізнесі, коли потреба в енергії висока, і відслідковувати, скільки електроенергії використовується і коли вона використовується. Це також дає комунальним підприємствам здатність знижувати споживання, спілкуючись з пристроями безпосередньо, щоб не допустити перевантажень

системи. Прикладами можуть служити пристрої, що скорочують споживання групи зарядних станцій електричних транспортних засобів, або зсуву налаштування температури кондиціонерів в місті [13]. Щоб мотивувати їх урізати використання і виконати таким чином **скорочення піків** або **вирівнювання піків**, ціни на електроенергію підвищуються в періоди високого попиту, і знижуються в період низького попиту [14].

Керування навантаженням/балансування навантаження

Загальне навантаження на енергосистему може змінюватись у широких межах увесь час. Хоча загальне навантаження є сумою багатьох індивідуальних виборів клієнтів загальне навантаження є нестабільним, повільно змінюється. зростає під час популярних телепередач, коли мільйони телеглядачів споживають струм. Розумна енергосистема може попросити індивідуальні телевізори або інших великих споживачів зменшити споживання тимчасово [16], щоб дати час для запуску генератора, або постійно, якщо ресурси є обмеженими. Використання математичних алгоритмів прогнозування дозволяє передбачити скільки генераторів потрібно щоб досягти певного відмов. У традиційних енергосистемах досягнення заданого рівня відмов можливе лише за рахунок збільшення числа генераторів у режимі очікування. У розумних енергосистемах зменшення навантаження навіть невеликої частки клієнтів може вирішити проблему.

Вважається, що споживачі і підприємства матимуть тенденцію споживати менше в періоди високого попиту, якщо це можливо для споживачів та споживчих пристроїв, якщо їм відомо про високу ціну використання електроенергії в пікові періоди. Це означає можливість компромісів, таких як циклічне вмикання / вимикання кондиціонера або запуск посудомийні машини о 9-й годині вечора замість 5-ї години вечора. Коли компанії і споживачі бачать пряму економічну вигоду від використання енергії не на піках, то вони будуть у своїх рішеннях враховувати витрати енергії на роботу користувацьких пристроїв і цивільне будівництво і, отже, стануть більш енергоефективними.

Стійкість

Покращена гнучкість розумної енергосистеми дозволяє більше проникнення поновлюваних джерел енергії, потужність яких сильно змінюється, таких як сонячна енергія і енергія вітру, навіть без додавання акумуляторів енергії. Поточна мережева інфраструктури побудована не для того, щоб забезпечувати роботу багатьох розподілених джерел живлення, і, зазвичай, навіть якщо джерела живлення можуть працювати з розподільчою мережею, лінії електропередач не можуть підлаштуватись під них. Швидкі коливання у мережі розподіленої генерації, наприклад, в моменти хмарної погоди або поривчастого вітру, представляють значні проблеми для енергетиків, які повинні забезпечити стабільні рівні потужності варіюючи генерацію більш керованих генераторів, таких як газові турбіни та гідроагрегати. Технологія розумної енергосистеми є необхідною умовою для використання великої кількості електроенергії з поновлюваних джерел.

Ринкові можливості

Розумна енергосистема дозволяє систематичне спілкування між постачальниками (за рахунок ціни на їх енергію) і споживачами (за рахунок їх готовності платити), і дозволяє і постачальникам, і споживачам бути більш гнучкими у своїх стратегіях роботи. Рекордні ціни на енергоносії треба заплатити тільки у період критичних навантажень, і споживачі будуть мати можливість бути більш далекоглядними у стратегії споживання енергії. Постачальники з більшою гнучкістю зможуть продавати електроенергію з максимальним прибутком, в той час як негнучкі постачальники, такі як парові турбіни базового навантаження, і більш змінні вітрові турбіни отримують різні тарифи в залежності від рівня попиту та стану інших генераторів в даний час. Загальним ефектом є сигнал про нагороду за енергоефективність і споживання енергії з урахуваннямо нестаціонарних обмежень на постачання. На рівні країни, техніка з можливістю зберігання енергії або з накопиченням тепла (наприклад, холодильники, теплові акумулятори і теплові насоси) буде "грати" на ринку щоб звести до мінімуму витрати енергії шляхом адаптації попиту до дешевших періодів постачання енергії. Це розширення ціноутворення подвійного тарифу на енергію.

Підтримка відповіді на попит

Підтримка відповіді на попит дозволяє генераторам і споживачам взаємодіяти у автоматичному режимі у реальному часі, координуючи попит для того, щоб згладити викиди. Прибирання частки споживання, яка відповідає цим викидам, прибирає і вартість додавання резервних генераторів, зменшує знос і продовжує термін служби обладнання, а також дозволяє користувачам скоротити свої витрати на електроенергію, кажучи низькопріоритетним пристроям використовувати енергію тільки тоді, коли вона є найдешевшою [17].

На даний час енергосистеми мають різну ступінь комунікації всередині систем управління їх коштовних активів, таких, як в електростанції, лінії електропередачі, підстанції і великі споживачі енергії.

У загальному випадку інформаційні потоки спрямовані в одну сторону, від користувачів і навантаження до виробників, якими вони керують. Виробники намагаються задовольнити попит у тій чи іншій мірі успішно або невдало (при зниженні напруги, віялових відключеннях). - Підтримка ідентифікаторів об'єктів та відкриття сервісів. Загальний обсяг попиту на електроенергію з боку користувачів може мати дуже широкий розподіл ймовірностей, що вимагає запасних генерувальних потужностей в режимі очікування, щоб реагувати на швидко мінливе енергоспоживання. Це односторонній потік інформації коштує дорого; останні 10% генерувальних потужностей можуть знадобитися всього лише протягом 1% від часу, і перебої можуть бути дорогими для споживачів.

Затримка потоку даних є основним предметом уваги, оскільки у ранніх архітектурах розумних лічильників можуть затримувати отримання даних до 24 годин, фактично унеможливлючи будь-яку можливу реакцію пристроїв постачальників та споживачів [18].

Платформа для розвинутих сервісів

Як і у інших галузях, використання стійких двонаправлених комунікацій, розвинутих датчиків і технології розподілених обчислень покращують ефективність, стійкість та безпеку постачання та споживання енергії. Вони також відкривають можливості для створення нових або удосконалення дійсних послуг, таких як пожежна сигналізація, яка вимикає електрику, телефонує до екстрених служб тощо.

Надання мегабіт, керування енергією кілобітами, решта на продаж

Обсяг даних, необхідний для проведення моніторингу та комутації приладів автоматичного відключення дуже малий в порівнянні з тим, який вже іде навіть до віддалених будинків для підтримки передачі голосу, безпеки, Інтернет і телебачення. Багато оновлень смуги пропускання розумних енергосистем оплачуються надмірними капіталовкладенням також для підтримки послуг споживачам, і субсидування зв'язку зі службами, пов'язаними з енергетикою або субсидування пов'язаних з енергетикою послуг, таких, як підвищення вартості в години пік. Це особливо вірно, коли уряди запускають обидва набору послуг як державну монополію. Оскільки електричні та комунікаційні компанії, як правило, є окремими комерційними підприємствами в Північній Америці і Європі, потрібні значні зусилля уряду і великих постачальників для заохочення різних підприємств до співпраці.

Деякі, як Cisco, бачать можливість в наданні пристроїв для споживачів, дуже схожих на тих, якими вони вже давно забезпечують промисловість [19]. Інші, такі як Silver Spring Networks [20] або Google, [21][22] є інтеграторами даних, а не продавцями обладнання. Тим часом як стандарти керування потужністю змінного струму пропонують улаштування зв'язку по лініях живлення як основний засіб зв'язку між інтелектуальними пристроями енергосистеми і домогосподарства, біти можуть дійти до будинку не за допомогою широкосмугового зв'язку по ЛЕП, а по фіксованому бездротовому зв'язку.

14.5. Технології розумних енергосистем

Більшість технологій розумних енергосистем вже використовуються у інших галузях, таких як виробництво та телекомунікації, адаптовані для використання у енергосистемі. У загальному випадку технології розумних енергосистем можуть бути згруповані у п'ять основних напрямків:[23]

- *Інтегровані комунікації*
- *Датчики та вимірювачі*
- *Інші високотехнологічні компоненти*
- *Інтелектуальне керування*
- *Удосконалені інтерфейси і підтримка прийняття рішень*

Інтегровані комунікації.

Деякі комунікації є сучасними, але не всі, оскільки енергосистеми розроблялись інкрементально і не є повністю інтегрованими. У більшості випадків дані збираються по модемному з'єднанню, а не по прямому мережевому з'єднанню.

Можливості для удосконалення включають: автоматизацію підстанцій, реагування на попит, автоматизацію розподілу, системи керування та спостереження (SCADA), системи керування енергією, безпровідні меш-мережі, комунікації по лініям електропередач і оптичному волокну [7].

Інтегровані комунікації дозволяють керування у реальному часі, обмін даними для оптимізації надійності, ефективності використання активів та безпеки [24].

Датчики та вимірювачі

Основними задачами є оцінка стабільності енергосистеми, моніторинг стану обладнання, попередження крадіжки енергії і підтримання стратегії керування. Технології включають в себе: передові мікропроцесорні системи моніторингу та вимірювання (розумні лічильники) і обладнання зчитування даних з лічильників, системи розподіленого моніторингу - динамічної оцінки ліній (зазвичай основані на розподілених датчиках температури, поєднаних з системами оцінки температури у реальному часі), системи вимірювання/аналізу електромагнітних параметрів (так знаний електромагнітний підпис), системи вимірювання часу споживання та ціноутворення у реальному часі, передові перемикачі і кабелі, радіотехнології зворотного розсіювання і цифрові захисні реле.

Розумні лічильники

Розумна енергосистема часто замінює аналогові механічні лічильники цифровими лічильниками, які записують споживання у реальному часі. Часто ця технологія називається передова вимірювальна інфраструктура, оскільки лічильники самі по собі не є корисними, і повинні встановлюватись разом з комунікаційною інфраструктурою для передачі даних (провідною, оптоволоконною, WiFi, сотовою або передачі по лініям електропередачі). Передова вимірювальна інфраструктура може надати канал зв'язку між електростанціями з однієї сторони і кінцевими споживачами у домогосподарствах і виробництвах з іншої. Ці пристрої кінцевих споживачів можуть включати розумні розетки та інші пристрої, здатні взаємодіяти з розумною енергосистемою, такі як водонагрівачі та термостати. У залежності від програми постачальника можуть бути сповіщені споживачі, або пристрої можуть вимикатись, або їх налаштування можуть автоматично змінюватись в залежності від часу піку споживання.

Вимірювачі фаз

Високошвидкісні датчики, які називаються вимірювачами фаз, розподілені по мережі передачі, використовуються для моніторингу стану енергосистеми. Вимірювачі фаз можуть проводити вимірювання до 30 разів за секунду, що значно швидше наявних технологій SCADA [25]. Вимірювачі фаз представляють магнітуду і фазу змінної напруги у певному місці електромережі. У 1980-х стало ясно, що супутники глобальної системи позиціювання (GPS) можуть дати дуже точні сигнали часу пристроям "у полі", що дозволяє вимірювання вимірювання різниці фаз на великих відстанях. Дослідження показують, що при великій кількості вимірювачів фаз і можливість порівняти фазові кути напруги в ключових точках у

мережі, автоматизовані системи можуть революціонізувати керування енергосистемами, шляхом швидкої, динамічної відповіді на умови роботи системи [26].

Широкомасштабна система вимірювання — мережа вимірювачів фаз, які можуть здійснювати моніторинг у реальному часі на регіональному та національному рівні [7]. Багато хто з інженерів-енергетиків вважає, що Північно-східний блекаут 2003-го міг бути утриманий на значно меншій площі, якщо б була розгорнута широкомасштабна система вимірювання фаз [27].

Інновації у надпровідності, стійкості до відмов, зберіганні енергії, силовій електроніці і діагностичних компонентах змінюють фундаментальні властивості мереж. Технології в межах цих широких категорій R&D включають в себе: пристрої гнучкої системи передачі струму, постійний струм високої напруги, дріт з надпровідників першого і другого роду, кабель з високотемпературних надпровідників, розподілену генерацію і зберігання енергії, композитні провідники і "інтелектуальні" прилади.

Розподілене керування потоками енергії

Пристрої керування потоком енергії встановлені на дійсних лініях для керування потоком енергії. Лінії передачі з підтримкою таких пристроїв підтримують більш широке використання відновлюваних джерел енергії, забезпечуючи більш послідовне керування в режимі реального часу тим, як ця енергія спрямовується в мережі. Ця технологія дозволяє більш ефективно зберігати переривчастий потік енергії з відновлюваних джерел для подальшого використання [28].

Інновації у надпровідності, стійкості до відмов, зберіганні енергії, силовій електроніці і діагностичних компонентах змінюють фундаментальні властивості мереж. Технології в межах цих широких категорій R&D включають в себе: пристрої гнучкої системи передачі струму, постійний струм високої напруги, дріт з надпровідників першого і другого роду, кабель з високотемпературних надпровідників, розподілену генерацію і зберігання енергії, композитні провідники і "інтелектуальні" прилади.

Інтелектуальна генерація енергії

Інтелектуальна генерація електроенергії являє собою концепцію узгодження виробництва електроенергії зі споживанням шляхом використання кількох однакових генераторів, які можуть запускатись, зупинятись і ефективно працювати при обраному навантаженні, незалежно від інших, що робить їх придатними і для покриття базового навантаження, і для вироблення електроенергії на піку споживання [19]. Забезпечення рівності постачання і попиту, яке називається балансуванням навантаження,[16] є необхідним для стабільного і надійного постачання електроенергії. Короткочасні відхилення від балансу ведуть до зміни частоти, а більш довгі ведуть до відключень енергії. Оператори енергосистеми зайняті балансуванням — узгодженням вихідної потужності усіх генераторів з навантаженням електромережі.

Задача балансування навантаження стала набагато складнішою зі зростанням частки більш переривчастих і змінних джерел, таких як вітрові турбіни і сонячні батареї, змушуючи інших виробників адаптувати свою генерацію набагато частіше, ніж було потрібно в минулому.

Перші дві електростанції, які реалізують концепцію динамічної стабільності мережі, були замовлені *Elering* і будуть побудовані *Wärtsilä в Kiisa, Естонія*. Їх мета полягає в "забезпеченні динамічних генерувальних потужностей для покриття раптових і несподіваних провалів в електромережі. Їх готовність планується протягом 2013 і 2014, а їх загальна потужність складе 250 МВт [15].

Автоматизація енергосистеми дозволяє швидке діагностування точні рішення на порушення у мережі або відключення. Ці технології спираються на і сприяють кожній з інших чотирьох ключових областей.

Інтелектуальне керування

Три категорії технологій для інтелектуального керування включають: *розподілених інтелектуальних агентів (системи керування), інструменти аналітики (програмне забезпечення та швидкодіючі комп'ютери) і операційні застосування (SCADA, автоматизація підстанцій, відповідь на попит тощо).* Використовуючи програмні

технології штучного інтелекту енергосистема *Фуджиян* у Китаї створила широкомасштабну систему захисту, яка здатна швидко і точно прораховувати стратегію керування і точно її виконувати [31]. Програмне забезпечення моніторингу і керування стабільністю напруги використовує метод послідовного лінійного програмування щоб достовірно визначити оптимальне рішення для керування [32].

14.6. Дослідження в Smart Grid

Основні програми

IntelliGrid – створена Інститутом дослідження електроенергетики (*Electric Power Research Institute, EPRI*), архітектура *IntelliGrid* надає методологію, інструменти та рекомендації щодо стандартів і технологій для підприємств щодо планування, специфікації вимог та отримання IT-систем, таких як інтелектуальні вимірювачі, автоматизація розподілу та відповідь на попит. Архітектура також надає лабораторію для оцінки пристроїв, систем та технологій. Архітектуру *IntelliGrid* застосовують *Southern California Edison, Long Island Power Authority, Salt River Project, та TXU Electric Delivery. Консорціум IntelliGrid* заснований на державно-приватному партнерстві, яке об'єднує та оптимізує зусилля у глобальних дослідженнях, фінансує дослідження і розробку технологій, працює над інтеграцією технологій та поширює технічну інформацію [23].

Grid 2030 – Grid 2030 є об'єднаним баченням розвитку електричної системи США, розробленим енергетичними компаніями, виробниками обладнання, постачальниками інформаційних технологій, агенціями урядів штатів та федерального уряду, групами зацікавлених, університетами та національними лабораторіями. Воно покриває генерацію, передачу, розподіл, зберігання та споживання [24]. Дорожня карта національних технологій постачання є основним документом щодо реалізації бачення Grid 2030. Дорожня карта окреслює основні проблеми та завдання щодо модернізації електромережі і пропонує шляхи для уряду і галузі до побудови майбутньої енергосистеми Америки.[25].

Modern Grid Initiative (MGI) є зусиллями зі співробітництва між Департаментом енергетики США, Національною лабораторією технологій енергетики (National Energy Technology Laboratory, NETL), підприємствами, споживачами, дослідниками та іншими зацікавленими у модернізації та інтеграції електричної мережі Сполучених Штатів. Офіс постачання електроенергії та надійності Департамента енергетики США спонсорує ініціативи в рамках Grid 2030 та Дорожньої карти національних технологій постачання, узгоджені з іншими програмами, такими як GridWise та GridWorks [26].

Сонячні міста — програма у Австралії, що включає співпрацю з енергетичними компаніями для випробування інтелектуальних лічильників, пікового та позапікового ціноутворення, віддаленого відключення та пов'язані з цим зусилля. Вона також передбачає обмежене фінансування на оновлення мережі [31].

GridWise – програма Офісу постачання електроенергії та надійності Департамента енергетики США, яка фокусується на розвитку інформаційних технологій модернізації електричної мережі США. Працюючи у рамках GridWise Alliance програма передбачає інвестиції у архітектуру та стандарти зв’язку, інструменти аналізу та симуляції, інтелектуальні технології, тестові стенди та демонстраційні проекти, нові регуляторні, інституційні та ринкові основи. GridWise Alliance є консорціумом публічних (у значенні державних та комунальних) та приватних зацікавлених осіб енергетичного сектору, надає майданчик для обміну ідеями, кооперації зусиль та зустрічей з регуляторними органами, які визначають політику на федеральному рівні та на рівні штатів [27].

Рада архітектури GridWise (GridWise Architecture Council, GWAC) була сформована Департаментом енергетики США для просування та забезпечення інтероперабельності серед багатьох учасників взаємодії у національній енергосистемі. Члени Ради є збалансованою і шанованою командою, що представляє усі ланки ланцюжка поставок і споживання електроенергії.Рада надає настанов та інструменти для формулювання цілей інтероперабельності у енергосистемі, визначає концепції та архітектури для того, щоб зробити інтероперабельність можливою, розробляє кроки для досягнення взаємодії систем,

пристроїв та інституцій, які охоплюють національну електричну систему. Рамковий документ з інтероперабельності в. 1.1 (*Interoperability Context Setting Framework, V 1.1)* Ради архітектури *GridWise* визначає необхідні настанови та принципи [28].

GridWorks – програма Департамента енергетики США, зосереджена на покращенні надійності енергетичної системи через модернізацію ключових компонентів електромережі, таких як кабелі, підстанції, захисні системи та силова електроніка. Програма також передбачає координацію зусиль щодо систем високотемпературних надпровідників, технологій забезпечення надійності передачі, технологій розподілу електроенергії, пристроїв зберігання енергії та систем GridWise [29].

Демонстраційний проект розумної енергосистеми Pacific Northwest (Pacific Northwest Smart Grid Demonstration Project) — демонстраційний проект у північно-західних штатах — Айдахо, Монтана, Орегон, Вашингтон та Вайомінг. Він включає близько 60 000 споживачів з інтелектуальними лічильниками, і містить основні функції майбутньої розумної енергосистеми [30].

14.7. Моделювання розумних енергосистем

Для моделювання розумних енергосистем використовуються багато різних концепцій. У загальному випадку вони вивчаються як складні системи. У мозковому штурмі,[32] енергосистема розглядалась у контекстах оптимального керування, екології, людського пізнання, теорії інформації, мікрофізики хмар тощо.

Захисні системи, що перевіряють себе та керують собою

Pelqim Spahiu ma Ian R. Evans у своєму дослідженні запропонували концепцію підстанції, основану на інтелектуальному захисті та гібридному інспекційному вузлі [43][44].

Осцилятори Курамото

Модель Курамото є добре вивченою системою. Енергосистема добре описується у цьому контексті [25][26]. Метою є зберегти систему у балансі, або підтримати синхронність фаз. Неоднорідні осцилятори також допомагають моделювати різні технології, різні типи генераторів, моделі споживання тощо. Ця модель також використовується для опису візерунків синхронізації в миготінні світлячків[45].

Біологічні системи

Електричні мережі пов'язані зі складними біологічними системами в багатьох контекстах. У одному дослідженні електричні мережі були зіставлені з соціальною мережею дельфінів [27]. Ці істоти оптимізують або посилюють комунікацію в разі незвичайної ситуації. Взаємозв'язки, що дозволяють їм вижити, є дуже складними.

Мережі випадкових запобіжників

У теорії перколяції, були вивчені мережі випадкових запобіжників. Щільність струму може бути занадто низькою в деяких районах, і занадто високою в інших. Аналіз може бути використаний, щоб згладити потенційні проблеми в мережі. Наприклад, аналіз, виконаний високошвидкісним комп'ютером, може передбачати згорілі запобіжники і запобігти цьому, або аналізувати зразки, які могли б призвести до аварії електромережі [28]. Для людей важко передбачити довгострокові закономірності в складних мережах, тому замість них використовуються мережі запобіжників або діодів.

Передбачення попиту

Одним із застосувань штучних нейронних мереж є передбачення попиту. Для економічної та надійної роботи енергосистем передбачення попиту є важливим, оскільки дозволяє визначити кількість електроенергії, яка буде спожита навантаженням. Це залежить від погодних умов, часу доби, випадкових подій тощо. Для нелінійного навантаження профіль навантаження не є гладким і передбачуваним, що веде до більшої невизначеності та меншої точності традиційних моделей штучного інтелекту. Факторами, які враховуються при розробці цих моделей є класифікація профілів споживання різних класів споживачів, активна реакція попиту, передбачена на основі ціноутворення у реальному часі, необхідність введення минулого попиту через різні компоненти, такі як пікове навантаження, базове навантаження, мінімальне навантаження, середнє навантаження тощо. замість об’єднання

цих значень у спільне вхідне значення, і залежність від специфічних вхідних змінних. Прикладом таких специфічних змінних може бути тип дня (робочий чи вихідний), який не має значного впливу на мережу лікарні, але значно впливає на профіль споживання домогосподарств [29][30][31][32][33].

Нейронні мережі

Нейронні мережі визнані придатними для керування енергосистемою. Електричні мереж можуть класифікуватись багатьма способами як нелінійні, динамічні, дискретні, випадкові та/або стохастичні. Штучні нейронні мережі намагаються розв'язати більшість з цих проблем.

Марківські процеси

Із набуттям популярності вітровою енергетикою стає необхідним враховувати її у реалістичних дослідженнях енергосистем. Від'єднані від мережі сховища енергії, непостійність вітру, постачання, споживання, ціноутворення та інші фактори моделюються у математичній грі. Метою є розробка переможної стратегії. Марківські процеси використовуються для моделювання і вивчення систем такого типу [24].

Максимальна ентропія

Усі ці методи з того чи іншого боку є методами максимальної ентропії, які активно досліджуються [25][26]. Це є поверненням до ідей Шеннона та інших дослідників, які вивчали комунікаційні мережі. Продовжуючи в аналогічному ключі сьогодні, сучасні дослідження бездротових мереж часто розглядають проблему перевантаження мережі, [27] і алгоритми його мінімізації, зокрема теорію ігор, [28] інноваційні комбінації частотного розділення каналів, часового розділення каналів та інші.

Більшість аргументів проти та приводів для занепокоєння зосереджені навколо інтелектуальних лічильників та можливостей, які вони відкривають (віддалене керування, віддалене відключення та змінна вартість). Там, де висловлюється занепокоєння щодо інтелектуальних лічильників, інтелектуальні лічильники продаються як розумна енергосистема, що зав'язує інтелектуальний лічильник з розумною енергосистемою в цілому в очах опонентів. Основні критичні аргументи представлені нижче:

- занепокоєння щодо приватності споживачів, зокрема використання даних для виконання функцій держави;
- соціальне занепокоєння щодо "чесної" доступності електроенергії;
- занепокоєння щодо складної системи обліку спожитого (у т.ч. змінні ціни), яка є непрозорою і непідконтрольною споживачу, що дозволяє постачальнику отримати перевагу над споживачем;
- занепокоєння щодо віддалено керованого вимикача у інтелектуальному лічильнику;
- соціальне занепокоєння щодо зловживань інформаційним важелем у стилі Enron;
- занепокоєння щодо надання уряду механізмів керування усією діяльністю зі споживання енергії;
- занепокоєння щодо радіовипромінювання від інтелектуальних лічильників.

Технічною причиною побоювань щодо приватності є те, що інтелектуальні лічильники надсилають детальну інформацію про споживання електроенергії по запиту. Частіші запити означають детальнішу інформацію. Рідкі звіти несуть мало користі постачальнику, і не дозволяють виконувати керування попитом у відповідь на зміну потреби у електроенергії. З іншого боку дуже часті звіти дозволяють постачальнику визначити шаблони поведінки мешканців будинку, наприклад час, коли вони відсутні або сплять. Сучасним трендом є збільшення частоти звітів. Рішенням, яке задовольняє і потреби постачальника, і вимоги приватності споживача, є динамічне налаштування інтервалу опитування [4]. У Британській Колумбії, Канада енергопостачальна організація належить уряду і тому повинна підкорятися вимогам законодавства у галузі приватності, що забороняє продаж даних, зібраних інтелектуальними лічильниками, у той час як приватні постачальники можуть продавати такі дані [5]. У Австралії боргові колектори використовували ці дані для того, щоб визначити коли люди знаходяться вдома [6].

У суді м. Остін, Техас, як доказ були представлені дані про споживання енергії тисячами жителів для визначення відхилень від типових шаблонів для того, щоб визначити хто вирощував марихуану [7].

Дані, які збираються інтелектуальними лічильниками, можуть відкрити значно більше, ніж скільки енергії споживається. Проведені дослідження показали, що виміряні значення потужності з двосекундним інтервалом дозволяють надійно ідентифікувати використання різних електричних приладів і, навіть, канал або програму, який переглядається на телевізорі, на основі шаблонів споживання та шумів, які випромінюються.

З появою кіберзлочинності також з'явилось занепокоєння щодо безпеки інфраструктури, в основному тієї, що використовує комунікаційні технології. Занепокоєння в основному відносяться до комунікаційної технології у ядрі розумної енергосистеми. Є ризик, що можливості, сконструйовані для взаємодії між виробниками, лічильниками у домогосподарствах і виробництві у реальному часі, також можуть бути використані для злочинів або терористичних атак [7]. Однією з основних властивостей є можливість віддалено вимкнути постачання, легко припинити або змінити поставки для клієнтів, які прострочили платіж. Це є знахідкою для постачальників енергії, однак також значно збільшує ризики інформаційної безпеки [6]. Кіберзлочинці проникали до енергосистеми США неодноразово [7]. Разом з проникненням у комп'ютери, також існує ризик використання шкідливого програмного забезпечення типу Stuxnet, яке націлене на системи SCADA, які широко використовуються у галузі, і може бути використане для атаки на мережу розумної енергосистеми.

Також потенційними проблемами є нав'язування неправдивих показів від інтелектуальних лічильників, які використовують технології радіообміну [8][9], та нав'язування підробленого сигналу GPS [10][11][12][13][14] фазовимірювальним пристроям.

Перед встановленням розвинутої вимірювальної системи або будь-якої інтелектуальної системи виробники повинні отримати умову для інвестицій. Деякі компоненти, такі як стабілізатори потужності, які встановлені на генератори, є дуже дорогими, потребують складної інтеграції у систему керування енергосистемою, потрібні тільки за надзвичайних обставин та ефективні тільки якщо інші постачальники їх мають. Без стимулів постачальники не будуть їх встановлювати [15]. Більшості постачальників важко обґрунтувати розгортання комунікаційної інфраструктури для єдиного застосування (наприклад зчитування показів).

Через те постачальники визначають кілька застосувань, які використовують спільну комунікаційну інфраструктури: наприклад, для зчитування показів, моніторингу якості електроенергії, віддаленого ввімкнення/вимкнення споживачів, отримання можливості відповіді на попит тощо. У ідеалі, комунікаційна інфраструктура буде не тільки підтримувати застосування найближчої перспективи, але і непередбачені застосування, які будуть з'являтися в майбутньому.

Регуляторні та законодавчі зміни також підштовхують постачальників до складання пазлу розумної енергосистеми. Кожен виробник має унікальний набір бізнесових, регуляторних та законодавчих умов, які впливають на їх інвестиції. Це означає, що кожен постачальник обере власний відмінний від інших шлях до створення розумної енергосистеми, і що постачальники впроваджуватимуть розумну енергосистему з різною швидкістю.

Деякі функції розумних енергосистем стикаються з протидією від галузей, які впроваджують або сподіваються впроваджувати схожі послуги. Прикладом може служити конкуренція з боку кабельних і DSL інтернет-провайдерів з широкосмуговим доступом за доступ до інтернету по системі електропроводки. Постачальники систем керування SCADA для мереж навмисно розробили пропрієтарні апаратні засоби, протоколи та програмне забезпечення таким чином, щоб вони не можуть взаємодіяти з іншими системами для того, щоб прив'язати своїх клієнтів до постачальника [16].

Крадіжка та втрата енергії

Деякі розумні енергосистеми мають подвійні функції. Інфраструктура інтелектуальних лічильників у використанні спільно з різноманітним програмним забезпеченням може використовуватись для виявлення крадіжки електроенергії, а процес усунення відмов — виявити місце. Це додаткова можливість до основних функцій з усунення необхідності зчитування показів лічильника людиною і вимірювання часу використання електроенергії.

Втрати від крадіжок електроенергії у світовому масштабі оцінюються у 200 мільярдів доларів США щороку [17].

14.8. Розгорнуті розумні енергосистеми

Enel. Найпершим, одним з найбільших прикладів розумної енергосистеми є італійська система, встановлена компанією *Enel S.p.A*. Завершений у 2005 проект *Telegestore* був дуже незвичним для виробників, тому що компанія, яка його розробляла, розробила і виготовила власні лічильники, виступила у ролі власного системного інтегратора та розробили власну програмну систему. Проект *Telegestore* вважається першим впровадженням технології розумних енергосистем у домогосподарствах у комерційному масштабі, та економить 500 мільйонів євро щороку при вартості проекта 2,1 мільярда євро [20].

Остін, Техас. У м. Остін, Техас працювали над розбудовою розумної енергосистеми з 2003, коли постачальник вперше замінив 1/3 власних лічильників з ручним зчитуванням показів на інтелектуальні лічильники, які зв'язуються через безпровідну mesh-мережу. Вона керувала 200 тисячами пристроїв у реальному часі (інтелектуальні лічильники, термостати і датчики на площі обслуговування), і очікувалась підтримка 500 тисяч пристроїв у реальному часі у 2009 [18].

US Dept. of Energy - ARRA Smart Grid Project**:** Одна з найбільших програм розгортання розумних енергосистем в світі - програма Департаменту енергетики США , що фінансується згідно з *American Recovery and Reinvestment Act*. Ця програма потребувала відповідного фінансування від окремих виробників. Всього близько 9 мільярдів доларів з публічних та приватних коштів було інвестовано в рамках цієї програми. Технології включають розвинуту вимірювальну інфраструктуру з 65 мільйонами інтелектуальних лічильників, системи інтерфейсу споживача, автоматику розподілу та підстанцій, системи оптимізації Вольт/ВАР, близько 1000 синхронізаторів фаз, динамічну оцінку ліній, проекти в галузі кібербезпеки, системи керування розподілом, системи зберігання енергії та проекти з інтеграції відновлюваних джерел енергії.

Ця програма складалась з грантів на інвестиції, демонстраційних проектів, вивчення прийняття споживачами і освітніх програм. Звіти окремих учасників та загальні звіти щодо впливу були завершені у другому кварталі 2015 р.

Баулдер, Колорадо. Завершено першу фазу проекта розумної енергосистеми у серпні 2008.

Обидві системи використовують інтелектуальні лічильники для мережі автоматизації домогосподарств, яка керує розумними розетками та пристроями. Деякі конструктори мережі сприяють відділенню функції керування від лічильників, з побоювань майбутніх розбіжностей з новими стандартами і технологіями, доступними у бізнес-сегменті домашніх електронних пристроїв, який швидко рухається [19].

Hydro One. У Онтаріо, Канада, в розпалі великомасштабна ініціатива розумної енергосистеми із розгортанням інфраструктури, сумісної зі стандартами зв'язку від Trilliant. Планувалось, що до кінця 2010 року система буде обслуговувати 1,3 млн клієнтів в провінції Онтаріо. Ініціатива отримала нагороду «Найкраща ініціатива розгортання інтелектуальних лічильників у Північній Америці» від *Utility Planning Network* [20].

Місто Мангайм у Німеччині використовує широкосмуговий зв'язок по лініях електропередач у реальному часі у своєму проекті "MoMa" [21].

InovGrid, Évora. — інноваційний проект у Évora, Португалія, який спрямований на обладнання електричної мережі інформацією і пристроями для автоматизації керування

мережею, поліпшення якості обслуговування, зниження експлуатаційних витрат, підвищення ефективності використання енергії та екологічної стійкості, а також збільшення проникнення відновлюваних джерел енергії і електричних транспортних засобів. Стане можливим керувати станом всієї мережі розподілу електроенергії в будь-який момент часу, що дозволяє постачальникам і компаніям, які надають енергетичні послуги, використовувати цю технологічну платформу, щоб запропонувати споживачам інформацію та продукти і послуги з доданою вартістю в галузі енергетики. Цей проект встановлення розумної енергосистеми ставить Португалію на передньому краї технологічних інновацій і надання послуг в Європі [22][23].

Аделаїда у Австралії також планує реалізувати локальну зелену розумну енергосистему при перебудові парка Тонслі [23].

Сідней, Австралія у партнерстві з урядом Австралії реалізував програму "Розумна енергосистема, розумне місто"[24][25].

E-Energy. У так званих проектах E-Energy кілька німецьких компаній створювали перше ядро в шести незалежних регіонах моделі. Технологічне змагання визначило ці модельні регіони для проведення науково-дослідних і дослідно-конструкторських робіт з головною метою створення «Інтернету енергетики» [26].

Консорціум **eEnergy Vermont** [28] - ініціатива рівня штату у Вермонті, яка частково фінансується відповідно до American Recovery and Reinvestment Act, у якій електричні компанії штату повинні швидко впровадити різні технології розумних енергосистем, включно з розгортанням 90% розвинутої вимірювальної інфраструктури і оцінкою різних структур динамічних тарифів.

Масачусетс. Одна з перших спроб розгортання розумної енергосистеми у США була відхилена у 2009 регуляторами енергетики у Commonwealth, Масачусетс [27]. Згідно зі статтею, опублікованою в *Boston Globe,* Північно-східна дочірня компанія *Massachusetts Electric Co*. намагалися створити програму розумної енергосистеми за допомогою державних субсидій, згідно з якою малозабезпечених споживачів будуть перемикати від післяплати до попередньої оплати рахунків (за допомогою смарт-карт), і, на додаток, вводитись спеціальні "преміум" тарифи на електроенергію, яка використовується вище обумовленої кількості [27]. Цей план був відкинутий регуляторами, як такий, що підриває важливі засоби захисту від відключень для клієнтів з низьким рівнем доходу. [27]. Відповідно до *Boston Globe*, план є несправедливо спрямований на клієнтів з низьким рівнем доходів і обходить закони штату Массачусетс, покликані допомогти споживачам отримати світло" [27]. Представник екологічної групи підтримки планів розумної енергосистеми *Massachusetts Electric Co* заявив:" при правильному використанні технології розумної енергосистеми мають великий потенціал для зниження пікового попиту, що дозволило б нам закрити деякі з найстаріших, найбрудніших електростанцій.

У **Нідерландах** був ініційований широкомасштабний проект (>5000 підключень, >20 партнерів) для демонстрації інтегрованих технологій, послуг та бізнес-кейсів розумної енергосистеми [28].

LIFE Factory Microgrid **(LIFE13 ENV / ES / 000700)** - це демонстраційний проект, частина програми LIFE+ 2013 Європейської комісії, метою якого було продемонструвати шляхом реалізації повномасштабної індустріальної розумної енергосистеми, що мікромережа може стати одним з найбільш вдалих рішень для генерації електроенергії та керування на виробництвах, які прагнуть зменшити вплив на навколишнє середовище.

14.9. Настанови, стандарти та групи користувачів

IEC TC57 створила сімейство міжнародних стандартів, які можуть бути використані як частина розумної енергосистеми. Ці стандарти включають в себе стандарт IEC 61850, який визначає архітектуру для автоматизації підстанцій, а також IEC 61970/61968 - загальну інформаційна модель. Загальна інформаційна модель передбачає загальну семантику, щоб використовується для перетворення даних в інформацію.

OpenADR є стандартом зв'язку розумних енергосистем з відкритим вихідним кодом, який використовується для застосувань реагування на попит [28]. Він, як правило, використовується для передачі інформації і сигналів, для того, щоб примусити електричні пристрої вимкнути споживання під час періодів високого споживання.

MultiSpeak створила специфікацію, яка підтримує функціональні можливості розумної енергосистеми. MultiSpeak має надійний набір визначень інтеграції, який підтримує практично всі програмні інтерфейси, необхідні для розподільчої компанії або для розподільчого підрозділу вертикально інтегрованої компанії. Інтеграція MultiSpeak визначається з використанням розширюваної мови розмітки (XML) і веб-сервісів.

IEEE створив стандарт для підтримки синхронізаторів фаз — C37.118 [29].

UCA International User Group обговорює і підтримує реальний світовий досвід стандартів, які використовуються в розумних енергосистемах.

Група компаній в рамках *LonMark International* займається питаннями, пов'язаними з розумними енергосистемами.

Існує зростаюча тенденція до використання технології TCP/IP як загальної комунікаційної платформи для застосувань для інтелектуальних лічильників, так що комунальні підприємства можуть розгорнути кілька систем зв'язку одночасно з використанням технології IP як загальної платформи керування [30][31].

IEEE P2030 є проектом IEEE з розробки "Чернетки настанови для розумної енергосистеми з експлуатаційної сумісності енергетичних технологій та інформаційних технологій роботи з енергосистемою (EPS), і кінцевих застосувань і навантаження" [31][32].

NIST включив ITU-T G.hn як один із "стандартів, визначених для реалізації для розумної енергосистеми", щодо якого, як він вважає, "існує міцний консенсус зацікавлених сторін" [33]. G.hn є стандартом для високошвидкісних комунікацій за лініями електропередач, телефонними лініями та коаксіальними кабелями.

Контрольні питання до розділу

1. Історія розвитку енергосистем. Можливості модернізації.
2. Системи на базі технологічної платформи Smart Grid.
3. Які принципові позиції мають бути покладені в основу реалізації такої концепції *Smart Grid* та її адаптації до українських реалій?
4. У рамках концепції *Smart Grid* інтелектуальна електроенергетична система розглядається як єдина мережа інформаційно-керуючих систем, що забезпечує:

a. інтеграцію всіх видів генерації (у тому числі малої генерації) і будь-які типи споживачів (від домашніх господарств до великої промисловості) для ситуаційного керування попитом на їхні послуги та забезпечення активної їх участі у роботі енергосистеми;

b. зміну в режимі реального часу параметрів і топології мережі за поточними режимними умовами, виключаючи виникнення та розвиток аварій;

c. розширення ринкових можливостей інфраструктури шляхом взаємного надання широкого спектру послуг суб'єктами ринку та інфраструктурою;

d. мінімізацію втрат, розширення самодіагностики і самовідновлення при дотриманні умов надійності та якості електроенергії;

e. інтеграцію електромережевої та інформаційної інфраструктури для створення всережимної системи керування з повномасштабним інформаційним забезпеченням.

5. Властивості розумних енергосистем. Надійність та гнучкість топології мережі.
6. Властивості розумних енергосистем. Ефективність. Скорочення/вирівнювання піків і ціноутворення відповідно до часу.
7. Властивості розумних енергосистем. Керування навантаженням/балансування навантаження.
7. Властивості розумних енергосистем. Стійкість.

8. Властивості розумних енергосистем. Підтримка відповіді на попит.
9. Технології Smart Grid. Основні напрямки.
10. Технології Smart Grid. Інтегровані комунікації.
11. Технології Smart Grid. Датчики та вимірювачі.
12. Технології Smart Grid. Розумні лічильники.
13. Технології Smart Grid. Вимірювачі фаз.
14. Технології Smart Grid. Високотехнологічні компоненти.
15. Високотехнологічні компоненти. Інтелектуальне керування.
16. Високотехнологічні компоненти. Інтелектуальна генерація енергії.
17. Високотехнологічні компоненти. Розподілене керування потоками енергії.
18. Основні програми в Smart Grid.
19. Моделювання розумних енергосистем.
20. Розгорнуті розумні енергосистеми.
21. Переваги та недоліки Smart Grid.
22. **С**тандарти Smart Grid.

Список рекомендованої літератури

1. Federal Energy Regulatory Commission Assessment of Demand Response & Advanced Metering. *United States Federal Energy Regulatory Commission*. Федеральна комісія з регулювання енергетики Сполучених штатів Америки.
2. Smart Grids European Technology Platform | www.smartgrids.eu. *smartgrids.eu*. 2011.
3. Smart Grids European Technology Platform | www.smartgrids.eu. *smartgrids.eu*. 2011.
4. J. Torriti, Demand Side Management for the European Supergrid Energy Policy, vol. 44, pp. 199-206, 2012.
5. The History of Electrification: The Birth of our Power Grid. *Edison Tech Center*. Процитовано November 6, 2013.
6. Mohsen Fadaee Nejad, AminMohammad Saberian and Hashim Hizam (June 3, 2013). Application of smart power grid in developing countries. *7th International Power Engineering and Optimization Conference (PEOCO)* (IEEE). doi:10.1109/PEOCO.2013.6564586.
7. Berger, Lars T. and Iniewski, Krzysztof, ред. (April 2012). *Smart Grid - Applicacions, Communications and Security*. John Wiley and Sons. ISBN 978-1-1180-0439-5.
8. Smart Grid Working Group (June 2003). Challenge and Opportunity: Charting a New Energy Future, Appendix A: Working Group Reports (PDF). Energy Future Coalition.
9. Federal Energy Regulatory Commission staff report (August 2006). *Assessment of Demand Response and Advanced Metering (Docket AD06-2-000)* (PDF). United States Department of Energy. с. 20.
10. National Energy Technology Laboratory (August 2007). *NETL Modern Grid Initiative — Powering Our 21st-Century Economy* (PDF). United States Department of Energy Office of Electricity Delivery and Energy Reliability. с. 17.
11. Gridwise History: How did GridWise start?. Pacific Northwest National Laboratory. 2007-10-30.
12. Qixun Yang, Board Chairman, Beijing Sifang Automation Co. Ltd., China and .Bi Tianshu, Professor, North China Electric Power University, China. (2001-06-24). WAMS Implementation in China and the Challenges for Bulk Power System Protection (PDF). *Panel Session: Developments in Power Generation and Transmission — Infrastructures in China, IEEE 2007 General Meeting, Tampa, FL, USA, 24–28 June 2007 Electric Power, ABB Power T&D Company, and Tennessee Valley Authority* (Institute of Electrical and Electronics Engineers).
13. Yih-Fang Huang; Werner, S.; Jing Huang; Kashyap, N.; Gupta, V., "State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid," Signal Processing Magazine, IEEE , vol.29, no.5, pp.33,43, Sept. 2012

14. Наказ від 01.12.2003 № 714 Про затвердження Правил застосування системної протиаварійної автоматики запобігання та ліквідації небезпечного зниження або підвищення частоти в енергосистемах (uk). Міністерство палива та енергетики України.
15. ↑ Tomoiagă, B.; Chindriş, M.; Sumper, A.; Sudria-Andreu, A.; Villafafila-Robles, R. Pareto Optimal Reconfiguration of Power Distribution Systems Using a Genetic Algorithm Based on NSGA-II. Energies 2013, 6, 1439-1455.
16. N. A. Sinitsyn. S. Kundu, S. Backhaus (2013). Safe Protocols for Generating Power Pulses with Heterogeneous Populations of Thermostatically Controlled Loads. *Energy Conversion and Management* **67**: 297–308. arXiv:1211.0248. doi:10.1016/j.enconman.2012.11.021.
17. Energy Future Coalition, "Challenge and Opportunity: Charting a New Energy Future," Appendix A: Working Group Reports, Report of the Smart Grid Working Group. https://web.archive.org/web/20080910051559/http://www.energyfuturecoalition.org/pubs/app_smart_grid.pdf
18. Why the Smart Grid Won't Have the Innovations of the Internet Any Time Soon: Cleantech News and Analysis «. Earth2tech.com (2009-06-05). Retrieved on 2011-05-14.
19. Cisco's Latest Consumer Play: The Smart Grid: Cleantech News and Analysis «. Earth2tech.com Retrieved on 2011-05-14.
20. Silver Spring Networks: The Cisco of Smart Grid?: Cleantech News and Analysis «. Earth2tech.com (2008-05-01). Retrieved on 2011-05-14.
21. Utility Perspective: Why Partner With Google PowerMeter?: Cleantech News and Analysis «. Earth2tech.com (2009-05-20). Retrieved on 2011-05-14.
22. E-Commerce News: Deals: Utility Companies Plug In to Google PowerMeter. Ecommercetimes.com. Retrieved on 2011-05-14. *that PMUs can revolutionize the way power systems are monitored and controlled."*»
23. U.S. Department of Energy, National Energy Technology Laboratory, Modern Grid Initiative, http://www.netl.doe.gov/moderngrid/opportunity/vision_technologies.html Архівовано 11 липень 2007 у Wayback Machine.
24. F.R. Yu, P. Zhang, W. Xiao, and P. Choudhury, "Communication Systems for Grid Integration of Renewable Energy Resources," IEEE Network, vol. 25, no. 5, pp. 22-29, Sept. 2011.
25. Factors Affecting PMU Installation Costs. United States Department of Energy. October 2014. Процитовано January 5, 2015.
26. Yilu Liu, Lamine Mili, Jaime De La Ree, Reynaldo Francisco Nuqui, Reynaldo Francisco Nuqui (2001-07-12). State Estimation and Voltage Security Monitoring Using Synchronized Phasor Measurement. *Research paper from work sponsored by American Electric Power, ABB Power T&D Company, and Tennessee Valley Authority* (PDF) (Virginia Polytechnic Institute and State University). CiteSeerX: 10.1.1.2.7959. «*"Simulations and field experiences suggest*
27. Patrick Mazza (2005-04-27). *Powering Up the Smart Grid: A Northwest Initiative for Job Creation, Energy Security, and Clean, Affordable Electricity.* (doc). Climate Solutions. с. 7. Архів оригіналу за 2008-12-30.
28. Smart Wire Grid Distributed Power Flow Control. arpa-e.energy.gov. Процитовано 2014-07-25.
29. Klimstra, Jakob; Hotakainen, Markus (2011). *Smart Power Generation*. Helsinki: Avain Publishers. ISBN 9789516928466. Архів оригіналу за 10 листопад 2011.
30. *Wide Area Protection System for Stability* (PDF). Nanjing Nari-Relays Electric Co., Ltd. 2008-04-22. с. 2. Архів оригіналу за 2009-03-18.
31. Zhao, Jinquan; Huang, Wenying; Fang, Zhaoxiong; Chen, Feng; Li, Kewen; Deng, Yong (2007-06-24). *On-Line Voltage Stability Monitoring and Control (VSMC) System in Fujian power grid*. 2007 IEEE Power Engineering Society General Meeting. *Proceedings, Power Engineering Society General Meeting, 2007*. (PDF) (Tampa, FL, USA: IEEE): 1. ISBN 1-4244-1296-X. doi:10.1109/PES.2007.385975. Загальний огляд.

32. Electric Power Research Institute, IntelliGrid Program Архівовано 18 травень 2007 у Wayback Machine.
33. U.S. Department of Energy, Office of Electric Transmission and Distribution, "Grid 2030" A National Vision for Electricity's Second 100 Years Архівовано 21 липень 2011 у Wayback Machine., July 2003

ДОДАТОК 1. ОСНОВНІ ВИДИ ДАТЧИКІВ ІНТЕРНЕТУ РЕЧЕЙ

Датчики, що використовуються в IoT дуже різноманітні і можуть бути класифіковані за різними ознаками:

Залежно від виду вхідної (вимірюваною) величини розрізняють: датчики механічних переміщень (лінійних і кутових), пневматичні, електричні, витратоміри, датчики швидкості, прискорення, зусилля, температури, тиски та ін. Нині існує приблизно наступний розподіл долі вимірів різних фізичних величин в промисловості: температура - 50%, витрата (масовий і об'ємний) - 15%, тиск - 10%, рівень - 5%, кількість (маса, об'єм) - 5%, час - 4%, електричний і магнітний величина - менше 4%.

По виду вихідної величини, в яку перетвориться вхідна величина, розрізняють неелектричні і електричні: датчики постійного струму (ЕДС або напруга), датчики амплітуди змінного струму (ЕДС або напруга), датчики частоти змінного струму (ЕДС або напруга), датчики опору (активного, індуктивного або ємнісного) та ін.

Більшість датчиків є електричними. Це обумовлено наступними перевагами електричних вимірів :

- електричні величини зручно передавати на відстань, причому передача здійснюється з високою швидкістю;
- електричні величини універсальні в тому сенсі, що будь-які інші величини можуть бути перетворені в електричні і навпаки;
- вони точно перетворяться в цифровий код і дозволяють досягти високої точності, чутливості і швидкодії засобів вимірів.

За принципом дії датчики можна розділити на два класи: генераторні і параметричні (датчики-модулятори). Генераторні датчики здійснюють безпосереднє перетворення вхідної величини в електричний сигнал. Параметричні датчики вхідну величину перетворять в зміну якого-небудь електричного параметра (R, L або C) датчика.

За принципом дії датчики також можна розділити на омічні, реостатні, фотоелектричні (оптико-електронні), індуктивні, ємнісні і д.р.

Розрізняють три класи датчиків :

- аналогові датчики, тобто датчики, що виробляють аналоговий сигнал, пропорційно зміні вхідної величини;
- цифрові датчики, що генерують послідовність імпульсів або двійкове слово;
- бінарні (двійкові) датчики, які виробляють сигнал тільки двох рівнів : "включено/вимкнено" (інакше кажучи, 0 або 1); отримали широке поширення завдяки своїй простоті.

Вимоги, що пред'являються до датчиків :

- однозначна залежність вихідної величини від вхідної;
- стабільність характеристик в часі;
- висока чутливість;
- малі розміри і маса;
- відсутність зворотної дії на контрольований процес і на контрольований параметр;
- робота за різних умов експлуатації;
- різні варіанти монтажу.

Параметричні датчики (датчики-модулятори) вхідну величину X перетворять в зміну якого-небудь електричного параметра (R, L або C) датчика. Передати на відстань зміну перерахованих параметрів датчика без сигналу (напруги або струму), що енергонесе, неможливо. Виявити зміну відповідного параметра датчика тільки і можна по реакції датчика на струм або напругу, оскільки перераховані параметри і характеризують цю реакцію. Тому параметричні датчики вимагають застосування спеціальних вимірювальних ланцюгів з живленням постійним або змінним струмом.

Омічні (резистивні) датчики - принцип дії грунтується на зміні їх активного опору при зміні довжини l, площі перерізу S або питомого опору *p: R= pl/S*. Крім того, використовується залежність величини активного опору від контактного тиску і освітлення

фотоелементів. Відповідно до цього омічні датчики ділять на: контактні, потенціометри (реостатні), тензорезисторні, терморезисторні, фоторезистори.

Подібно до того, як база даних управляє доступом до збережених даних, шина даних управляє доступом до даних та оновленнями одночасно багатьох користувачів. Це саме те, що потрібно високопродуктивним пристроям, щоб вони працювали разом, як єдина система.

Контактні датчики - це простий вид датчиків резисторів, які перетворять переміщення первинного елементу в стрибкоподібну зміну опору електричного ланцюга. За допомогою контактних датчиків вимірюють і контролюють зусилля, переміщення, температуру, розміри об'єктів, контролюють їх форму і т. д. До контактних датчиків відносяться путні і кінцеві вимикачі, контактні термометри і так звані електродні датчики, використовувані в основному для виміру граничних рівнів електропровідних рідин.

Недолік контактних датчиків - складність здійснення безперервного контролю і обмежений термін служби контактної системи. Але завдяки граничній простоті цих датчиків їх широко застосовують в системах автоматики.

Реостатні датчики є резистором з активним опором, що змінюється. Вхідною величиною датчика є переміщення контакту, а вихідний - зміна його опору. Рухливий контакт механічно пов'язаний з об'єктом, переміщення (кутове або лінійне) якого необхідно перетворити.

Датчики потенціометрів, що конструктивно є змінними резисторами, виконують з різних матеріалів - обмотувального дроту, металевих плівок, напівпровідників і т. д.

Тензорезистори *(датчики тензометрувань)* служать для виміру механічної напруги, невеликих деформацій, вібрації. Дія тензорезисторів грунтується на тензоефекті, що полягає в зміні активного опору провідникових і напівпровідникових матеріалів під впливом докладених до них зусиль.

Індуктивні датчики служать для безконтактного отримання інформації про переміщення робочих органів машин, механізмів, роботів і тому подібне і перетворення цієї інформації в електричний сигнал. Принцип дії індуктивного датчика грунтований на зміні індуктивності обмотки на магнітопроводі залежно від положення окремих елементів магнітопровода (якоря, сердечника та ін.).

Переваги індуктивних датчиків :

- немає механічного зносу, відсутні відмови, пов'язані із станом контактів;
- відсутній брязкіт контактів і неправдиві спрацьовування;
- висока частота перемикань до 3000 Hz;
- стійкий до механічних дій;

Основні недоліки - порівняно мала чутливість, залежність індуктивного опору від частоти живлячої напруги, значна зворотна дія датчика на вимірювану величину (за рахунок притягнення якоря до сердечника).

Ємнісні датчики - принцип дії грунтований на залежності електричної місткості конденсатора від розмірів, взаємного розташування його обкладань і від діелектричної проникності середовища між ними.

Переваги ємнісних датчиків - простота, висока чутливість і мала інерційність. *Недоліки* - вплив зовнішніх електричних полів, відносна складність вимірювальних пристроїв. Ємнісні датчики застосовують для виміру кутових переміщень, дуже малих лінійних переміщень, вібрацій, швидкості руху і т. д., а також для відтворення заданих функцій (гармонійних, пилкоподібних, прямокутних і т. п.).

Генераторні датчики здійснюють безпосереднє перетворення вхідної величини X в електричний сигнал. Такі датчики перетворять енергію джерела вхідної (вимірюваною) величини відразу в електричний сигнал, тобто вони є як би генераторами електроенергії (звідки і назва таких датчиків - вони генерують електричний сигнал).

Температурні датчики.

Якщо розглядати датчики температури для промислового застосування, то можна виділити їх основні класи: *кремнієві датчики температури, біметалічні датчики, рідинні і газові термометри, термоіндикатори, термістори, термопари, термоперетворювачі опору, інфрачервоні датчики.*

Кремнієві датчики температури використовують залежність опору напівпровідникового кремнію від температури. Діапазон вимірюваних температур - 50…+150 ^{0} С. Застосовуються в основному для виміру температури усередині електронних приладів.

Біметалічний датчик зроблений з двох різнорідних металевих пластинів, скріплених між собою. Різні метали мають різний температурний коефіцієнт розширення. Якщо сполучені в пластину метали нагрівати або охолодити, то вона зігнеться, при цьому замкне (розімкне) електричні контакти або переведе стрілку індикатора. Діапазон роботи біметалічних датчиків – 40...+550 ^{0} С.

Використовуються для виміру поверхні твердих тіл і температури рідин. Основні сфери застосування - автомобільна промисловість, системи опалювання і нагріву води.

Термоіндикатори - це особливі речовини, що змінюють свій колір під впливом температури. Зміна кольору може бути оборотною і безповоротною. Робляться у вигляді плівок. ***Термоперетворювачі опору*** - принцип дії термоперетворювачів опору (терморезисторів) грунтується на зміні електричного опору провідників і напівпровідників залежно від температури.

Інфрочервоні датчики (пірометри) - використовують енергію випромінювання нагрітих тіл, що дозволяє вимірювати температуру поверхні на відстані. Пірометри діляться на радіаційні, яскравісні і колірні.

Кварцеві термоперетворювачі. Для виміру температур від - 80 до +250 градусів часто використовуються так звані кварцеві термоперетворювачі, що використовують залежність власної частоти кварцевого елементу від температури. Робота цих датчиків грунтується на тому, що залежність частоти перетворювача від температури і лінійність функції перетворення змінюються залежно від орієнтації зрізу відносно осей кристала кварцу. Ці датчики широко використовуються в цифрових термометрах.

П'єзоелектричні датчики. Дія п'єзоелектричних датчиків грунтується на використанні п'єзоелектричного ефекту (п'єзоефекту), що полягає в тому, що при стискуванні або розтягуванні деяких кристалів на їх гранях з'являється електричний заряд, величина якого пропорційна діючій силі. П'єзоефект обернений, тобто прикладена електрична напруга викликає деформацію п'єзоелектричного зразка - стискування або розтягування його відповідно до знаку прикладеної напруги. Це явище, що називається зворотним п'єзоефектом, використовується для збудження і прийому акустичних коливань звукової і ультразвукової частоти. Використовуються для виміру сил, тиску, вібрації і т. д.

Оптичні (фотоелектричні) датчики. Розрізняють аналогові і дискретні оптичні датчики. У аналогових датчиків вихідний сигнал змінюється пропорційно зовнішній освітленості. Основна сфера застосування - автоматизовані системи управління освітленням. Датчики дискретного типу змінюють вихідний стан на протилежне досягши заданого значення освітленості. Фотоелектричні датчики можуть бути застосовані практично в усіх галузях промисловості. Датчики дискретної дії використовуються як своєрідні безконтактні вимикачі для підрахунку, виявлення, позиціонування і інших завдань на будь-якій технологічній лінії.

Оптичний безконтактний датчик, реєструє зміну світлового потоку в контрольованій області, пов'язану зі зміною положення в просторі яких - небудь частин механізмів і машин, відсутності або присутності об'єктів, що рухаються. Завдяки великим відстаням спрацьовування оптичні безконтактні датчики знайшли широке застосування в промисловості і не лише.

По своєму призначенню фотодатчики діляться на дві основні групи: *датчики загального застосування* і *спеціальні датчики*. До спеціальних, відносяться типи датчиків, призначені для вирішення вужчого круга завдань. Приміром, виявлення кольорової мітки на об'єкті, виявлення контрастної межі, наявність етикетки на прозорій упаковці і т. д.

Завдання датчика виявити об'єкт на відстані. Ця відстань варіюється в межах 0,3мм-50м, залежно від вибраного типу датчика і методу виявлення.

Сенсор PM2.5/Температура/Вологість Netvox RA0716

Netvox RA0716 використовується для вимірювання PM2,5, температури і вологості в приміщенні. Зв'язок по стандартному протоколу *LoRaWAN ™ (клас А). RA0716* має датчик PM2.5, для визначення концентрації зважених часток на одиницю об'єму в повітрі. Сенсор RA0716 сертифікований LoRaWAN ™.

Можливості застосування:

- Вимірювання концентрації частинок PM2,5
- Вимірювання температури
- Вимірювання вологості

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- *LoRaWAN™* Класс А сумістний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- *Encrypt-RF ™ Security* (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Безпроводове поновлення (в майбутньому)
- Стороння онлайн-система моніторингу та оповіщення бездротових датчиків для настройки датчиків, перегляду даних і установки оповіщень за допомогою текстових повідомлень SMS і електронної пошти (додатково)
- Доступна стороння платформа: Actility / ThingPark, TTN, MyDevices / Cayenne, ThingsBoard.io.

Сенсор аварійна кнопка Netvox R312A

Сенсор R312A є пристроєм аварійного кнопкового вимикача, яке виявляє сигнал включення або виключення аварійного кнопкового перемикача і відправляє сигнал тривоги на шлюз для обробки. Він використовує модуль бездротового зв'язку SX1276.

Аварійний кнопковий вмикач активується, коли виникає аварійна ситуація. Сенсор зручний для перенесення та має перемикач, простий в експлуатації. При натисканні аварійного кнопкового перемикача порт IO модуля (19-й контакт U1) виявляє низький рівень, а коли аварійний кнопковий вимикач відпущений, порт IO модуля KEY1 (19-й ніж U1) виявляє високий рівень.

Можливості застосування:

- Аварійне вимикання пристроїв;
- Пожежна тривога;
- Безпека.

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- LoRaWAN™ Класс А сумістний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- *Encrypt-RF ™ Security* (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Строк служби батареї *[2]:

- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10)
- Безпроводове поновлення (в майбутньому)
- Стороння онлайн-система моніторингу та оповіщення бездротових датчиків для настройки датчиків, перегляду даних і установки оповіщень за допомогою текстових повідомлень SMS і електронної пошти (додатково)
- Доступна стороння платформа: *Actility / ThingPark, TTN, MyDevices / Cayenne, ThingsBoard.io.*
- Серія R718X має в корпусі магніти для кріплення сенсорів до феромагнітних матеріалів та об'єктів.

IoT сенсор Tektelic KONA Industrial Transceiver and Sensor

Промисловий KONA трансивер і датчик - ідеальне рішення для взаємодії автоматики і контрольно-вимірювальних приладів з мережами *LoRaWAN*. Промисловий трансивер підтримує до 3х аналогових і цифрових входів, що дозволяють здійснювати дистанційний збір даних, 2 перемикаємих вихода для активації виконавчих механізмів і різних компонентів системи управління, а також зручний інтерфейс *RS-232, RS-422* або *RS-485* з численними протоколами. Він також вимірює і повідомляє температуру, вологість та інші призначені для користувача функції. Вбудована батарея *Li-SOCl2* служить до 10 років.

Можливість застосування:

- Автоматизація промислових процесів
- Розумне сільське господарство
- Розумна виробнича будівля
- Промисловий контроль
- Лічильник і енергосистема
- Автоматично налаштовується протокол *CANbus*
- Модернізація *M2M LoRaWAN*.

LoRa Terminal

F8L10T LoRa Terminal - це бездротовий термінал передачі даних, заснований на технології *LoRa Spread Spectrum* Communication. Він використовує мережу LoRa для забезпечення бездротової передачі даних користувачам.

В якості платформи підтримки програмного забезпечення використовується високопродуктивне рішення LoRa промислового класу з вбудованою операційною системою реального часу. Він підтримує інтерфейси RS232 і RS485 (або RS422) одночасно, може бути підключений до послідовних пристроїв безпосередньо для даних. Термінал має конструкцію з низьким енергоспоживанням, мінімальне енергоспоживання становить менше 5 мА при 12 В постійного струму. Він має 5 входів / виходів для функцій агрегату, таких як цифровий вхід і вихід, аналоговий вхід, лічильник імпульсів і т. д.

Продукт широко використовується в індустрії M2M промислового ланцюга IoT, такого як інтелектуальна мережа, інтелектуальний транспорт, розумний будинок, фінанси, мобільні термінали POS, автоматизація ланцюжка поставок, промислова автоматизація,

інтелектуальний будинок, протипожежний захист, громадська безпека, охорона навколишнього середовища захист, метеорологія, цифрова медицина, телеметрія, сільське, лісове, водне, вугільне, нафтохімічне і інші суміжні галузі.

Tektelic KONA All-in-One Smart Room Sensor

Датчик *KONA All-in-One Smart Room Sensor* включає в себе можливість виміру всіх основних параметрів середовища в одному маленькому пристрої. Датчик ідеально підходить для комплексного моніторингу дому та офісу, надаючи дані і звіти про температуру, вологість, силі освітлення, наявності руху в приміщенні, вібрації або виявленні витоку, відкритих / закритих дверей і вікон. Датчик *KONA All-in-One Smart Room* Sensor відображає стан елементів живлення (батареї), що забезпечує зручність обслуговування і експлуатації.

Датчик оптимально використовує радіочастотні ресурси, тому сенсор All-in-One розрахований на тривалий термін служби акумулятора. Можливість віддаленого поновлення датчиків дає право користувачу налаштовувати параметри кастомізірованих додатків, порогових значень датчика. подій запуску і звітів, дозволяючи йому підтримувати безліч різних додатків «*Умий будинок» IoT* з одним і тим же пристроєм. Датчик *All-in-One* є багатофункціональним пристроєм, що робить його економічно ефективним, а використання єдиної екосистеми *LoRaWAN* дає можливість застосування сенсорів для різних додатків і інтеграцій замовника.

Можливість застосування:

- Визначення руху (двері, висувний ящик)
- Визначення руху в приміщенні (PIR)
- Визначення відкриття дверей / вікон
- Контроль статусу зовнішнього контакту
- Управління магнітним перемикачем (запуск пристроїв)
- Вимірювання G-Force (настроюється пусковий механізм)
- Читання імпульсів (вода, газ, інші показники)
- Визначення рівня освітлення у кімнаті
- Вимірювання температури / вологості
- Визначення витоку.

Безпроводовий датчик рівня заповнюваності бака для збору побутових відходів

Датчик *BrighterBins* - це безпроводовий пристрій контролю рівня заповнення контейнера побутових відходів. Унікальне апаратне обладнання та інтелектуальна прошивка роблять його найбільш підходящим рішенням для управління збору сміття.

Інтелектуальний датчик *BrighterBins* - це продукт *IoT від Smart End*, який робить ваш збір відходів інтелектуальним і економічно ефективним. Пристрій має багато переваг у порівнянні з доступними в даний час рішеннями на ринку. Пристрій оснащений міцною конструкцією, має менший на 40% дизайн корпусу і має регульований кут нахилу датчика тунелю, для можливості інтеграції з 90% бункерів. Рухомий тунель дозволяє встановлювати

пристрій в різних напрямках, а установка займає близько 10 хвилин. Діапазон робочих температур становить від -40 ° С до + 70 ° С, щоб охопити всі регіони по всьому світу.

Інтелектуальний датчик *BrighterBins* повністю сумісний з технологіями *LoRaWAN*. Технологія *LoRaWAN* забезпечує тривалий термін служби пристрою від однієї баьарei і великий радіус дії бездротового зв'язку.

Конструкція апаратного забезпечення *Brighter Bins* забезпечує високу перешкодозахищеність від електромагнітних завад. Термін служби пристрою *BrighterBins* від однієї батареї ємністю 20 Ач (літій-тіонілхлорид) становить понад 7 років (залежить від кількості передач).

Рис. Демонстрація роботи датчика рівня заповнюваності бака

Особливості датчика *BrighterBins:*

Зумер:

Подає сигнал при включенні пристрою.

Звукові сигнали після завершення самоперевірки.

Ультразвуковий датчик:

Регулюється в будь-якому напрямку під будь-яким кутом.

Діапазон: 20-500 см. Точність: зазвичай ± 5%.

Вимірювання температури:

Вимірювання температури в градусах Цельсія.Генерація тривоги при виявленні пожежі.

Моніторинг:

Монітори рівня заповнення, батареї і температури.

Вимірювання рівня заповнення:Конфігурація: відстань до рівня заповнення або рівень заповнення у відсотках (передача через 25% або 50% або 75% і т. д.).Може вимірювати тверді об'єкти.

Стан батареї:Регулярно передає відсоток заряду батареї. Регульована і оптимізована передача в залежності від рівня заповнення.

Бездротовий накладний датчик парковки Netvox R719

Сенсор R719 - це пристрій для виявлення припарковнного автомобіля. Він може бути використаний для виявлення наявності або відсутності на парковці транспортних засобів. Він заснований на модулі бездротового зв'язку SX1276, і зв'язок повністю сумісний з протоколом LoRaWAN ™ (клас А).

Можливості застосування:

– Смарт паркінг

- Особливості датчиків Netvox:
- Дальність передачі даних 10 км *[1]
- *LoRaWAN™* Класс А сумістний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- Encrypt-RF ™ Security (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Строк служби батареї *[2]:
- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10).

Двоконтактний герконовий сенсор виявлення відкриття/закриття дверей/вікон Netvox R718F2

Сенсор R718F2 використовує геркон для виявлення сигналів закриття/відкриття вікна/двері. Прикладом застосування R718F2 є виявлення стану двері або вікна з метою безпеки. Він заснований на модулі бездротового зв'язку SX1276, і зв'язок повністю сумісний з протоколом LoRaWAN ™ (клас А).

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- *LoRaWAN™* Класс А сумісний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- *Encrypt-RF ™ Security* (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Строк служби батареї *[2]:
- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10)
- Безпроводове поновлення (в майбутньому)
- Стороння онлайн-система моніторингу та оповіщення бездротових датчиків для настройки датчиків, перегляду даних і установки оповіщень за допомогою текстових повідомлень SMS і електронної пошти (додатково)
- Доступна стороння платформа: *Actility / ThingPark, TTN, MyDevices / Cayenne, ThingsBoard.io.*

Можливості застосування:

- Відстеження будь-яких процесів на виробничій лінії
- Відстеження статусу відкрито / зачинено
- Комерційна нерухомість. Контроль доступу двері і вікна
- Житлова власність. Контроль доступу двері і вікна
- Контроль доступу до будь-яких закритих об'єктів
- Моніторинг обмеженого простору
- IT серверні кімнати і шафи
- Морозильні та холодильні двері
- Моніторинг дверей вантажного відсіку
- Моніторинг гаражних воріт

Сенсор виявлення диму Netvox RA02A

Сенсор RA02A - це високонадійний бездротовий сигнальний пристрій для інтелектуального будинку, який виявляє концентрацію диму в повітрі і посилає попереджувальний сигнал. Він заснований на модулі бездротового зв'язку SX1276, і зв'язок повністю сумісний з протоколом *LoRaWAN* ™ (клас А).

Можливості застосування:

- Машинне відділення
- Склад
- Розумний будинок
- Підприємства
- Дата центр
- Готельні комплекси

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- *LoRaWAN™* Класс А сумісний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- *Encrypt-RF* ™ *Security* (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Строк служби батареї *[2]: 5 років (Умови: температура навколишнього середовища 25°C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10)
- Стороння онлайн-система моніторингу та оповіщення бездротових датчиків для настройки датчиків, перегляду даних і установки оповіщень за допомогою текстових повідомлень SMS і електронної пошти (додатково).

Сенсор для визначення каламутності води Netvox RA0710

Серія сенсорів Netvox RA07XX має інтерфейс зв'язку RS485. Сенсор RA0710 підключений до датчика каламутності ZS-206. ZS-206 розроблений і виготовлений з використанням принципу вимірювання каламутності в розсіяному світлі. Коли промінь світла падає на пробу води, світло розсіюється в пробі води, і інтенсивність розсіяного світла в напрямку, перпендикулярному падаючому світлу, вимірюється і порівнюється зі значенням внутрішнього калібрування для розрахунку каламутності в пробі води.

Корпус і датчик з'єднані через інтерфейс RS485, і виявлені дані передаються в центр обробки даних через бездротову мережу для відображення. Він заснований на модулі бездротового зв'язку SX1276, і зв'язок повністю сумісний з протоколом LoRaWAN ™ (клас А).

Можливості застосування:

- Визначення якості води
- Смарт пральна машина

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- *LoRaWAN™* Класс А сумістний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- *Encrypt-RF ™ Security* (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Безпроводове поновлення (в майбутньому)

Сенсор з датчиком термопари Netvox R718CX

Сенсор R718CX застосовується для визначення температури об'єкта і середовища, з якою контактує термопара. Він використовує модуль бездротового зв'язку SX1276, і зв'язок повністю сумісний з протоколом LoRaWAN ™ (клас А).

Можливості застосування:

- Устаткування для вимірювання температури
- Устаткування для систем опалення

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- *LoRaWAN™* Класс А сумісний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- *Encrypt-RF ™ Security* (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Строк служби батареї *[2]:
- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10)
- Безпроводове поновлення (в майбутньому)

Сенсор з датчиком термопари Netvox R718CX

Сенсор R718CX застосовується для визначення температури об'єкта і середовища, з якою контактує термопара. Він використовує модуль бездротового зв'язку SX1276, і зв'язок повністю сумісний з протоколом LoRaWAN ™ (клас А).

Можливості застосування:

- Устаткування для вимірювання температури
- Устаткування для систем опалення

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- LoRaWAN™ Класс А сумістний

- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- Encrypt-RF ™ Security (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Строк служби батареї *[2]:
- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10)
- Безпроводове поновлення (в майбутньому)
- Стороння онлайн-система моніторингу та оповіщення бездротових датчиків для настройки датчиків, перегляду даних і установки оповіщень за допомогою текстових повідомлень SMS і електронної пошти (додатково)
- Доступна стороння платформа: Actility / ThingPark, TTN, MyDevices / Cayenne, ThingsBoard.io.

Сенсор зовнішній CO2/Температури/Вологості Netvox R72715

Сенсор NETVOX R72715 має датчик температури і вологості, який передає дані про температуру і вологість навколишнього середовища. R72715 має датчик CO2, який визначає концентрацію CO2 в повітрі і передає виявлені дані на інші пристрої через бездротову мережу LoRa. Він використовує модуль бездротового зв'язку SX1276.

R72715 має вбудований датчик температури, вологості повітря і датчик CO2. Датчик температури і вологості повітря SHT-30 повідомляється з модулем через I2C, а датчик CO2 - з модулем LoRa через послідовний порт UART.

Можливості застосування:

- Визначення температури і вологості
- Моніторинг CO_2

Особливості датчиків Netvox:

- Дальність передачі даних 10 км *[1]
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- Encrypt-RF ™ Security (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)
- Строк служби батареї *[2]:
- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10)
- Безпроводове поновлення (в майбутньому).

Сенсор протікання води Netvox R311W

Netvox R311W - це датчик протікання води, заснований на протоколі *LoRaWAN ™ (ClassA*), з функцією виявлення витоків і сигналізації. Коли R311W виявляє витік, він відправляє повідомлення тривоги на шлюз. Сенсор повідомить про стан, відправивши повідомлення на шлюз. В комплекті два датчика витоку води, які дозволяють користувачам контролювати дві плями.

Можливості застосування:

- Моніторинг протікання (появи) води в дата-центрі та серверній кімнаті;
- Моніторинг центру зберігання документів;
- Моніторинг протікання води у підвалі;
- Виявлення протікання сантехніки;
- Контроль трюму човна;
- Моніторинг складських приміщень;

Особливості сенсорів Netvox:

- Дальність передачі даних 10 км *[1]
- LoRaWAN™ Класс А сумістний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- Encrypt-RF ™ Security (обмін ключами Диффи-Хеллмана + AES-128 для повідомлень з даними датчиків)

Строк служби батареї *[2]:

- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення LoRa SF = 10)
- Безпроводове поновлення (в майбутньому)

Сенсор освітленості Netvox R718G

Сенсор R718G має вбудований датчик освітленості, який можна використовувати для визначення інтенсивності навколишнього освітлення. R718G визначає значення інтенсивності навколишнього освітлення і відправляє їх на сервер. Зібрані дані відображаються на інших пристроях. Він використовує модуль бездротового зв'язку SX1276, і зв'язок повністю сумісна з протоколом *LoRaWAN ™ (клас А).*

Можливості застосування:

- Визначення рівня освітленості
- Інтеграція з системами освітлення та управління

Особливості сенсорів Netvox:

- Дальність передачі даних 10 км *[1]
- LoRaWAN™ Класс А сумістний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- *Encrypt-RF ™ Security* (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)

Строк служби батареї *[2]:

- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення *LoRa SF* = 10)
- Безпроводове поновлення (в майбутньому)
- Стороння онлайн-система моніторингу та оповіщення бездротових датчиків для настройки датчиків, перегляду даних і установки оповіщень за допомогою текстових повідомлень SMS і електронної пошти (додатково)

Сенсор сирена (оповіщувач) Netvox R602A

Сенсор R602A - це інтелектуальна бездротова сигналізація, яка може зв'язуватися з іншими пристроями через бездротову мережу. Сенсор має потужні динаміки і світлодіоди високої яскравості для звукової та світлової сигналізації. Заснований на модулі бездротового зв'язку SX1276, і зв'язок повністю сумісний з протоколом LoRaWAN ™ (клас C).

Особливості сенсорів Netvox:

- Дальність передачі даних 10 км *[1]
- LoRaWAN™ Класс А сумістний
- Поширення спектру стрибкоподібної перебудови частоти (FHSS)
- Покращена завадостійкість
- Поліпшене керування живленням для збільшення терміну служби батареї
- Encrypt-RF ™ Security (обмін ключами Діффі-Геллмана + AES-128 для повідомлень з даними датчиків)

  Строк служби батареї *[2]:
- 5 років (Умови: температура навколишнього середовища 25 ° C, 20 тригерів в день, потужність tx = 20 дБм, коефіцієнт поширення *LoRa SF* = 10)
- Безпроводове поновлення (в майбутньому).