ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ІОТ-РІШЕННЯ ДЛЯ ВІЙСЬКОВИХ ЗАСТОСУВАНЬ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми «Комп'ютерна інженерія»
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Павло БАКУН*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач(ка) вищої освіти гр. КІД-41
Павло БАКУН
Ім'я, ПРІЗВИЩЕ

Керівник: Денис ЖУЖКОВ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бакун Павло Вікторович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «IoT-рішення для військових застосувань»
керівник кваліфікаційної роботи: Денис ЖУЖКОВ, викладач кафедри КІ,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025р. №56
2. Строк подання кваліфікаційної роботи «05» червня 2025р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, стандарти та протоколи безпровідного зв'язку (LoRa, ZigBee, MQTT), типові архітектурні рішення військових IoT-систем, особливості побудови захищених мереж та автономного функціонування пристроїв, технічна документація мікроконтролерів і сенсорів, аналітичні огляди реалізованих волонтерських рішень, методи забезпечення енергетичної ефективності, підходи до аналізу криптографічного захисту, методики порівняльного аналізу архітектур і протоколів для задач спеціального призначення.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
    1. Теоретичні основи IoT у військових застосуваннях
    2. Аналіз архітектур та сценаріїв застосування IoT-систем
    3. Оцінка існуючих підходів та перспективи розвитку
5. Перелік ілюстративного матеріалу: *презентація*
    1. Мета, об'єкт, предмет дослідження
    2. Актуальність роботи
    3. Використання IoT-рішень у військових задачах
    4. Типова архітектура військової IoT-системи
    5. Приклади реалізації IoT-рішень
    6. Сценарії застосування в бойових умовах
    7. Алгоритми функціонування IoT систем
    8. Методи підвищення автономності
    9. Аналіз викликів щодо створення прототипів IoT-рішень
    10. Порівняння з іншими IoT-рішеннями

11. Висновки
12. Публікації та апробація роботи

6. Дата видачі завдання «24» лютого 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.02-19.03.2025	
2	Обробка матеріалу	20.03-02.04.2025	
3	Розробка теоретичної частини	03.04-07.04.2025	
5	Аналіз архітектур та сценаріїв застосування IoT-систем	08.04-27.04.2025	
6	Оцінка існуючих підходів та перспективи розвитку	28.04-11.05.2025	
7	Висновки за результатами аналізу	12.05-15.05.2025	
8	Розробка презентації	16.05-26.05.2025	
9	Передзахист	27.05-29.05.2025	
10	Здача в деканат	30.05-05.06.2025	

Здобувач(ка) вищої освіти _____ Павло БАКУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Денис ЖУЖКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 103 стор., 42 рис., 7 табл., 22 джерел.

Мета роботи – спрощення створення та підвищення стійкості розподілених IoT-систем для військових застосувань за рахунок використання принципів автономної роботи, захищеної передачі даних та енергоефективної модульної архітектури.

Об'єкт дослідження – процеси побудови та функціонування IoT-систем в умовах бойових дій.

Предмет дослідження – апаратно-програмні засоби захищеного зв'язку, протоколи безпровідного обміну, технології автономного живлення та конструктивної захищеності пристроїв.

Короткий зміст роботи: У роботі розглянуто особливості побудови IoT-рішень для військового використання в умовах обмеженого зв'язку, ризику перехоплення даних та складних фізичних впливів. Проведено порівняльний аналіз архітектур цивільних та спеціалізованих IoT-систем за критеріями автономності, захищеності, дальності зв'язку, енергоефективності та вартості впровадження.

Запропоновано логічну архітектуру вузькоспеціалізованих IoT-рішень, засновану на використанні відкритих компонентів (ESP32, LoRa, GPS, автономні джерела живлення) з модульним підходом до конфігурації. Розглянуто можливі алгоритми роботи таких систем з урахуванням бойових умов і вимог до енергозбереження та безпеки. На основі аналізу зроблено висновки щодо доцільності та потенціалу подальшої адаптації відкритих технологій для військових задач без необхідності створення дорогих та складних прототипів.

КЛЮЧОВІ СЛОВА: IOT, ВІЙСЬКОВІ СИСТЕМИ, АВТОНОМІЯ, ЗАХИЩЕНІСТЬ, LORA, ESP32, ШИФРУВАННЯ, ЕНЕРГОЕФЕКТИВНІСТЬ, ПОЛЬОВІ УМОВИ, STARLINK, МОДУЛЬНА АРХІТЕКТУРА.

ABSTRACT

Text part of the qualification work for obtaining a bachelor's degree: 103 pages, 42 figures, 7 tables, 22 sources.

The purpose of the work is to simplify the creation and increase the stability of distributed IoT systems for military applications by using the principles of autonomous operation, secure data transmission and energy-efficient modular architecture.

The object of the study is the processes of building and operating IoT systems in combat conditions.

The subject of the study is hardware and software tools for secure communication, wireless exchange protocols, autonomous power technologies and constructive security of devices.

Summary of the work: The work considers the features of building IoT solutions for military use in conditions of limited communication, the risk of data interception and complex physical influences. A comparative analysis of the architectures of civilian and specialized IoT systems is carried out according to the criteria of autonomy, security, communication range, energy efficiency and implementation cost.

A logical architecture of highly specialized IoT solutions is proposed, based on the use of open components (ESP32, LoRa, GPS, autonomous power sources) with a modular approach to configuration. Possible algorithms for the operation of such systems are considered, taking into account combat conditions and requirements for energy conservation and security. Based on the analysis, conclusions are drawn regarding the feasibility and potential for further adaptation of open technologies for military tasks without the need to create expensive and complex prototypes.

KEYWORDS: IOT, MILITARY SYSTEMS, AUTONOMY, SECURITY, LORA, ESP32, ENCRYPTION, ENERGY EFFICIENCY, FIELD CONDITIONS, STARLINK, MODULAR ARCHITECTURE.

ЗМІСТ

ВСТУП..... 9
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІОТ У ВІЙСЬКОВИХ ЗАСТОСУВАННЯХ 10
1.1 Поняття та еволюція IoT..... 10
1.2 Військовий контекст використання IoT..... 18
1.3 Компоненти військових IoT-систем..... 27
1.4 Огляд реальних IoT-рішень у військовій сфері 37
1.5 Порівняльна характеристика технологій зв'язку..... 47
РОЗДІЛ 2. АНАЛІЗ АРХІТЕКТУР ТА СЦЕНАРІЇВ ЗАСТОСУВАННЯ ІОТ-СИСТЕМ. 55
2.1 Архітектура IoT-системи для військових задач..... 55
2.2 Сценарії використання та варіанти побудови 64
2.3 Алгоритми функціонування IoT-систем..... 71
2.4 Аналіз можливостей реалізації та обмежень..... 80
РОЗДІЛ 3. ОЦІНКА ІСНУЮЧИХ ПІДХОДІВ ТА ПЕРСПЕКТИВИ РОЗВИТКУ 89
3.1 Методи покращення систем IoT. 89
3.2 Порівняння з іншими IoT-рішеннями 97
3.3 Перспективи розвитку IoT-систем 105
ВИСНОВКИ..... 111
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ……...……112
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)…….....114

ВСТУП

Інтернет речей (Internet of Things, IoT) став однією з ключових технологій цифрової трансформації у цивільному секторі — від автоматизації розумних будинків до оптимізації логістичних процесів і медичних систем. Його суть полягає в об’єднанні фізичних пристроїв у мережу для збирання, передавання та обробки даних у реальному часі. Такі системи забезпечують безперервний моніторинг, дистанційне керування та автоматичну реакцію на зміну зовнішніх умов.

Розвиток IoT супроводжується появою різноманітних безпровідних технологій, протоколів обміну та стандартів енергозбереження. Комерційні рішення зосереджені на мінімізації вартості, простоті масштабування та взаємодії з хмарними платформами. У центрі уваги опиняються такі технології, як Wi-Fi, Bluetooth Low Energy, LoRa, ZigBee, а також популярні мікроконтролери на зразок ESP32, STM32, Arduino тощо. Однак подібні рішення здебільшого не розраховані на використання в нестабільному середовищі або умовах обмеженого живлення та зв’язку.

У той же час, військові задачі висувають значно жорсткіші вимоги до IoT-систем. Йдеться про надійність роботи в агресивних умовах, довготривалу автономність, захист переданих даних від перехоплення, стійкість до радіоелектронної боротьби та фізичну безпеку обладнання. Стандартні підходи з цивільної сфери виявляються недостатніми, тому потребують глибокої адаптації або повної заміни на спеціалізовані розробки.

З огляду на актуальні виклики, виникає потреба в побудові доступних, енергоефективних та стійких до зовнішніх впливів IoT-рішень, придатних до використання в умовах бойових дій. Такі рішення мають поєднувати переваги відкритих технологій і військових вимог до захисту, автономії та масштабованості.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ІОТ У ВІЙСЬКОВИХ ЗАСТОСУВАННЯХ

1.1 Поняття та еволюція IoT

Інтернет речей (Internet of Things, IoT) — це концепція, яка передбачає об’єднання фізичних об’єктів, оснащених сенсорами, виконавчими пристроями, засобами обчислення та комунікацій, у єдину мережу для збору, обміну та обробки даних без необхідності постійної участі людини. В основі цієї парадигми лежить ідея, що не лише комп’ютери або смартфони можуть бути учасниками інформаційного обміну, а будь-які об’єкти — від датчика температури до автономного дрона. Така система відрізняється від традиційної архітектури «клієнт-сервер», де пристрої пасивно чекають команд від центрального вузла. У випадку IoT відбувається тісна взаємодія між численними пристроями, що можуть самостійно обробляти дані, приймати рішення та реагувати на події, утворюючи розгалужену, гнучку та динамічну інфраструктуру. Таким чином, IoT не просто розширює межі комп’ютерних мереж, а створює новий пласт цифрової взаємодії, де кожен пристрій потенційно може стати активним учасником процесів збору інформації, аналізу та впливу на фізичне середовище [1-3].

Ключові характеристики IoT. Основою побудови IoT-систем є низка ключових характеристик, без яких неможливе ефективне функціонування розподіленої мережі взаємодіючих об’єктів. Однією з таких характеристик є сенсорність — здатність пристроїв вимірювати параметри навколишнього середовища, зокрема температуру, вологість, рух, рівень освітленості, шум, положення в просторі або інші фізичні характеристики. Завдяки широкому спектру сенсорів IoT-система отримує можливість постійного моніторингу реального світу, що відрізняє її від традиційних цифрових платформ, які оперують переважно в рамках обробки вже наявних даних. У той час як класичні IT-системи здебільшого

працюють із введеною вручну інформацією або переданими файлами, IoT дозволяє «бачити» і «чути» середовище в реальному часі завдяки фізичному контакту з ним через сенсори [1].

Наступною фундаментальною характеристикою є безперервна передача зібраних даних між компонентами системи. Передача інформації в IoT здійснюється через як безпровідні, так і провідні канали: Wi-Fi, Bluetooth, LoRa, Zigbee, а також мобільні протоколи зв'язку (4G, 5G) або супутникові канали — усе це забезпечує можливість роботи системи в найрізноманітніших умовах, включно з віддаленими районами чи навіть зонами, де відсутня базова телеком-інфраструктура. Канал зв'язку є невід'ємним елементом, який несе в собі не лише функцію передачі, а й підтримку логіки розподіленості, синхронізації вузлів, відправки команд, запитів, оновлень і підтверджень. Інакше кажучи, зв'язок є технологічною артерією, що об'єднує всі функціональні складові IoT у цілісну живу систему.

Важливою ознакою є також локальна або віддалена обробка зібраних даних. В IoT-системах ця обробка може виконуватись безпосередньо на рівні вузла — наприклад, мікроконтролера ESP32, одноплатного комп'ютера Raspberry Pi або ж на зовнішньому сервері, з урахуванням принципів fog або edge computing. Такий підхід дозволяє здійснювати попередню фільтрацію, агрегацію, інтерпретацію отриманих даних ще до їх передачі далі в мережу або приймати рішення прямо на місці, знижуючи затримки і залежність від центрального хмарного сервера, що є особливо актуальним у ситуаціях, коли швидкість реакції критично важлива, наприклад, при виявленні несанкціонованого проникнення або зміні обстановки на полі бою [1].

Автономність — ще одна базова властивість IoT-системи, особливо у контексті військового застосування. Йдеться не лише про здатність працювати без участі людини, а й про роботу без постійного зовнішнього живлення, що надзвичайно важливо у віддалених районах, де неможливо організувати централізовану подачу енергії. У більшості випадків IoT-вузли працюють на акумуляторах, батареях або джерелах альтернативної енергії, а тому всі апаратні та

програмні рішення повинні бути оптимізовані під мінімальне енергоспоживання. На відміну від традиційних пристроїв, IoT-компоненти здатні обмінюватися невеликими порціями даних, використовуючи енергоефективні протоколи та режим сну для зниження навантаження, що забезпечує тривалу роботу без втручання оператора [1].

Під час розгортання в умовах бойових дій IoT-технології отримують нове значення. Завдяки своїй розподіленій структурі, гнучкій топології, підтримці автономності та стійкості до зовнішніх впливів вони можуть використовуватись для побудови систем виявлення, контролю, спостереження або навіть координації дій у режимі реального часу. Наприклад, можливим є створення мережі з численних автономних сенсорних вузлів, які фіксують переміщення, зміну звукового фону або температуру, передаючи дані до командного пункту або безпосередньо до виконавчих модулів, які реагують на зміну ситуації. Завдяки цьому виникає можливість не просто моніторингу, а й активного управління тактичними ресурсами в динамічному середовищі, що суттєво розширює межі традиційних підходів до інформаційної підтримки на полі бою (див. рис. 1.1).

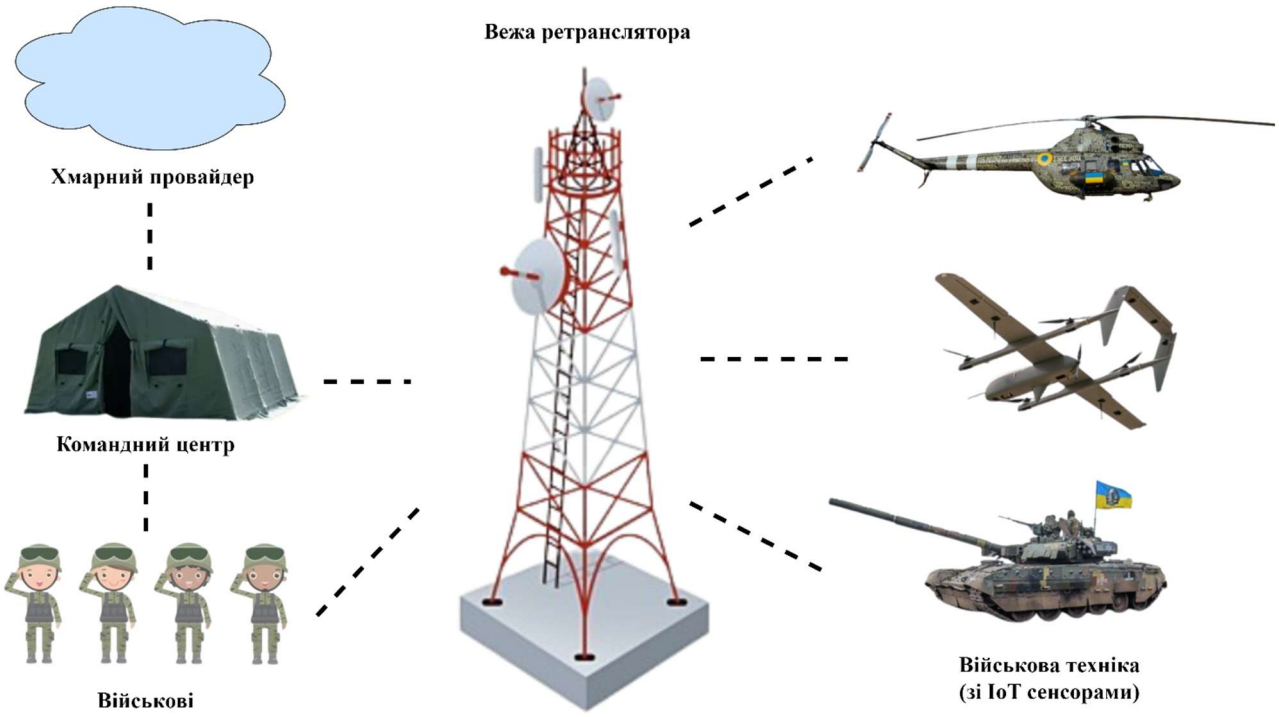


Рисунок 1.1 – Структура IoT-систем військового значення

У цьому контексті, еволюція поняття IoT від первинної ідеї «розумного будинку» чи «розумного міста» поступово переходить до систем тактичного призначення, де основними пріоритетами стають:

— надійність;
— автономність;
— безпека;
— адаптивність;
— енергоефективність.

Усе це підкреслює, що IoT вже не є суто цивільною концепцією, а перетворюється на важливу складову нової цифрової інфраструктури, здатної функціонувати у високоризикових умовах та забезпечувати інформаційну перевагу на різних рівнях прийняття рішень [1-2].

Етапи розвитку технологій IoT у світі. Еволюція Інтернету речей як технологічного напрямку тісно пов’язана з поступальним розвитком обчислювальної техніки, мікроелектроніки та телекомунікацій, що дозволяє простежити послідовне формування IoT з моменту появи перших концепцій до сучасного високотехнологічного впровадження у складні сфери, зокрема військову. Витоки цієї концепції сягають 1990-х років, коли в контексті промислової автоматизації почали з’являтися ідеї про так звані «розумні об’єкти», зокрема у рамках систем типу SCADA, які дозволяли віддалено моніторити і керувати обладнанням. Сам термін «Інтернет речей» був запропонований у 1999 році Кевіном Ештоном і заклав основи для подальшого розвитку нової парадигми взаємодії фізичних об’єктів з цифровим середовищем [1-2].

Упродовж 2000–2010-х років відбувся стрімкий ріст кількості прототипів розумних пристроїв, чому сприяло здешевлення мікроконтролерів, поява безпровідної технологій на зразок Wi-Fi та поступове розширення доступу до Інтернету. З’явилися перші хмарні платформи, які дозволяли об’єднувати ці пристрої в єдину екосистему, зосереджену навколо таких застосувань як розумні будинки. У цей період активно велися експерименти з інтеграцією сенсорних модулів, підключенням до Інтернету, автоматизованим прийняттям рішень та

віддаленим керуванням. Починаючи з 2010-х років і до 2020 року відбулося масштабне розширення сфери застосування IoT за межі побутового сегменту та промисловості — технології почали впроваджувати у медицині, агропромисловому комплексі, міській інфраструктурі та транспорті. З'явилися стандарти передачі даних, такі як MQTT, CoAP, а також спеціалізовані операційні системи на кшталт FreeRTOS, RIOT OS, які забезпечували гнучке і надійне функціонування пристроїв із обмеженими ресурсами [2].

З 2020-х років IoT почав тісно інтегруватися з іншими високотехнологічними напрямами, зокрема зі:

— штучним інтелектом;

— кібербезпекою;

— технологіями аналізу великих даних.

Поява 5G, міні-комп'ютерів нового покоління, енергоефективних мікроконтролерів, а також розвиток мереж LoRaWAN, NB-IoT і подібних технологій забезпечили можливість масштабного впровадження IoT у середовищах із підвищеним рівнем ризику, зокрема на полі бою, де традиційні безпровідні технології, як-от Wi-Fi чи Bluetooth, через обмежену дальність і енергозалежність не могли забезпечити стабільний зв'язок. Завдяки цьому відкрилися нові горизонти для використання розподілених систем спостереження, контролю та реагування в реальному часі в умовах, які вимагають не лише надійності, але й надзвичайної мобільності [2].

Роль мініатюризації та енергозбереження у військових IoT. У рамках військових IoT-рішень особливе значення набувають два фактори — мініатюризація пристроїв та енергозбереження, оскільки в польових умовах відсутні стаціонарні джерела енергії, наявні суттєві обмеження щодо масогабаритних характеристик обладнання, а доступ до обслуговування систем може бути надзвичайно ускладнений. Мініатюризація дозволяє розміщувати сенсори на:

— дронах;

— військовій техніці;

— елементах екіпірування;

— конструкціях будівель.

Усе це без негативного впливу на їх функціональність чи маневреність. Сучасні GPS-трекери можуть мати розмір у кілька сантиметрів, забезпечуючи при цьому точне відстеження об’єктів у режимі реального часу й залишаючись практично непомітними. Енергозбереження досягається через використання низькопотужних мікроконтролерів типу ESP32 або STM32, які підтримують режими глибокого сну, застосування енергоефективних радіомодулів, автономних акумуляторів або сонячних батарей, що дає змогу функціонувати системам упродовж тижнів або навіть місяців без потреби в заміні живлення або ручному втручанні [2-3].

Крім того, технології зв’язку LPWAN (Low Power Wide Area Network), як-от LoRa та NB-IoT, дозволяють передавати невеликі обсяги даних на відстані до 10 км при мінімальному енергоспоживанні, що робить їх надзвичайно придатними для використання в польових умовах, де традиційні технології не справляються з завданням забезпечення сталого і безпечного зв’язку (див. рис. 1.2).

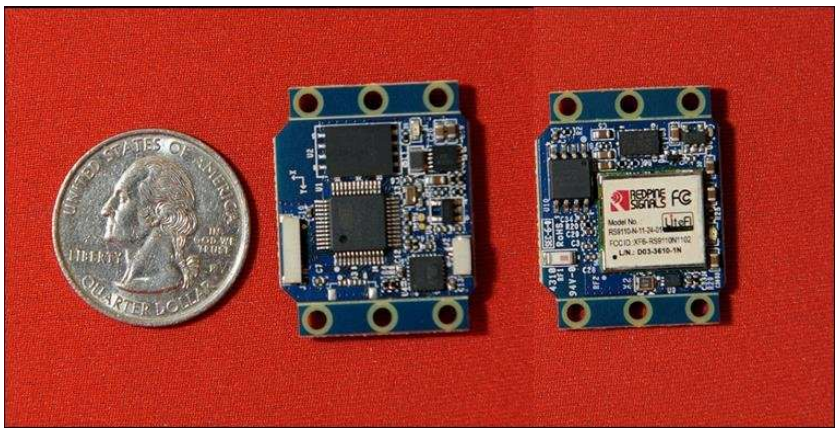


Рисунок 1.2 – Вплив мініатюризації на розміри сенсорів

Усе це свідчить про те, що поєднання мініатюризації та оптимального енергоспоживання не лише розширює межі застосування IoT у військовій галузі, а й робить можливим розгортання масштабних інтелектуальних мереж у надзвичайно агресивному середовищі, де використання традиційних комп’ютерних технологій є або неможливим, або надто затратним [2-3].

Особливості впровадження IoT у критичних умовах. У військових умовах, що належать до категорії критичних середовищ, технічні системи, зокрема IoT-рішення, зобов'язані відповідати специфічним вимогам, серед яких автономність вважається однією з основних, адже відсутність стабільного енергоживлення або доступу до мережевої інфраструктури передбачає здатність пристроїв діяти самостійно, з мінімальним людським втручанням, що дозволяє, наприклад, автоматично активувати тривогу чи передати координати у відповідь на визначену подію без необхідності стороннього контролю. Такий підхід зменшує час реакції, мінімізує людський фактор і підвищує загальну ефективність реагування, особливо коли йдеться про ситуації, де кожна секунда може коштувати життя.

Крім автономності, критичне значення має стійкість систем до зовнішніх загроз, зокрема до спроб зламу, радіоперешкод, перехоплення даних або фізичного знищення пристроїв, тому впровадження механізмів шифрування (зокрема TLS), автентифікації пристроїв, протоколів захисту від перевантаження та фізичних оболонок, здатних витримувати удар, тиск, пил та вологу, є необхідною умовою для успішного використання IoT у зонах бойових дій. Підвищені ризики на полі бою обумовлюють також вимоги до малопомітності обладнання: воно не повинно випромінювати зайвого тепла чи радіосигналів, які могли б бути виявлені противником. Зниження рівня теплової помітності та загальна маскувальність дозволяють застосовувати такі пристрої в безпосередній близькості до противника без суттєвого ризику викриття, що особливо критично для розвідувальних чи оборонних задач.

Паралельно з цим пристрої повинні демонструвати високу надійність і здатність функціонувати у надзвичайно жорстких умовах — при різких перепадах температур, підвищеній вологості, механічних ударах та постійному впливі вібрацій, адже будь-яке обладнання, розгорнуте у бойовій зоні, не повинно виходити з ладу через дрібні зовнішні впливи і має зберігати функціональність щонайменше до моменту планової заміни або ремонту. Така витривалість розглядається не лише як перевага, а як обов'язкова характеристика.

Гнучкість до масштабування та адаптації також є важливою умовою, оскільки структура військових операцій динамічна за своєю природою, фронт постійно змінюється, з’являються нові запити і нові задачі, а тому IoT-системи мають бути здатні до оперативного додавання нових вузлів, перебудови топології мережі та адаптації до різних рівнів доступності ресурсу. Усе це потребує відповідного підходу до розробки — орієнтованого не лише на апаратну потужність або програмну функціональність, а перш за все на практичну експлуатацію у нестабільних і складних польових умовах, де системи не обслуговуються щоденно і повинні залишатися максимально ефективними в автономному режимі (див. рис. 1.3).



Рисунок 1.3 – Приклади адаптації IoT до екстремальних умов

Практичний досвід останніх років, зокрема з 2022 року в Україні в умовах повномасштабної війни, підтверджує, що навіть найпростіші рішення, реалізовані на базі платформ на кшталт Arduino чи ESP32, можуть бути критично значущими, виконуючи функції:

— розвідки;

— автоматизованої сигналізації;

— моніторингу руху або об’єктів;

— збирання та передавання телеметрії на безпечну відстань.

Таким чином, простота, доступність і адаптивність стають не менш важливими за складність і технологічну досконаліть, адже саме такі рішення можуть бути швидко розгорнуті, легко замінені або оновлені та використовувані в умовах, де інші системи просто не виживають, що і формує основу підходу до IoT у військовій галузі — через поєднання:

— мінімалізму;

— надійності;

— скритності;

— автономності;

— здатності до динамічної адаптації.

1.2 Військовий контекст використання IoT

Сучасне ведення війни значно виходить за межі традиційної фізичної протидії, все частіше зміщуючи акценти в бік:

— інформаційної переваги;

— точного контролю;

— мінімізації людської участі;

— автоматизованого управління процесами.

У цьому контексті технології Інтернету речей дозволяють створювати гнучкі, автономні, розподілені системи збору даних, моніторингу та реагування, які здатні підтримувати ситуаційну обізнаність, забезпечувати логістику, моніторити навколишнє середовище та посилювати захист об’єктів військової інфраструктури. Завдяки цим системам стає можливим впровадження рішень, спрямованих на зниження втрат, пришвидшення прийняття рішень, підвищення точності дій та ефективності використання ресурсів, що безпосередньо впливає на хід бойових дій і стійкість збройних формувань [4-5].

Основні сфери застосування IoT у військовій справі. Однією з найважливіших сфер використання IoT у військовому контексті залишається розвідка та ситуаційна обізнаність, де завданням є оперативне отримання даних про дії противника, зміни на місцевості чи потенційні загрози. Використання мініатюрних сенсорних вузлів, розташованих уздовж лінії фронту або на підходах до стратегічних об'єктів, дозволяє фіксувати переміщення техніки, особового складу, джерела звуку, вібрації та інші фізичні показники, що сигналізують про активність ворога. Сенсори з вбудованими акселерометрами, мікрофонами та геолокаційними модулями здатні виявляти наближення техніки ще до її візуального розпізнавання, дозволяючи значно раніше реагувати на загрозу. У поєднанні з безпілотними літальними апаратами, оснащеними IoT-модулями, можна створити єдину ситуаційну картину, в якій дані з багатьох джерел об'єднуються та передаються на командні пункти, де приймаються рішення на основі актуальної та точної інформації. Інтеграція даних із сенсорних вузлів, дронів і супутників у єдину систему дозволяє командуванню не просто бачити події в режимі реального часу, а й оперативно змінювати стратегію відповідно до нових обставин [4].

Не менш важливою сферою застосування є логістика, адже ефективне постачання армії необхідними ресурсами прямо пов'язане з її здатністю до виконання завдань і збереженням життів. IoT-системи дозволяють автоматизовано відстежувати переміщення боєприпасів, пального, техніки та інших критичних ресурсів, а також контролювати їхній стан у режимі реального часу. Контейнери з вантажем можуть містити GPS-модулі, сенсори температури, вологості або ударів, передаючи інформацію до координаційних центрів, що дозволяє уникати втрат вантажів або затримок у доставці. Крім цього, платформи IoT застосовуються для моніторингу технічного стану бойових машин — датчики рівня мастила, напруги акумулятора або справності гальмівної системи дають змогу вчасно здійснювати технічне обслуговування навіть у польових умовах, що істотно знижує ймовірність поломок у критичні моменти [4].

Ще однією надзвичайно важливою сферою є моніторинг навколишнього середовища та стану об'єктів, що дозволяє виявляти потенційні екологічні або

техногенні загрози. Сенсори, здатні фіксувати рівень радіації, хімічного забруднення чи диму, стають вкрай актуальними в умовах загрози ураження стратегічно небезпечних об’єктів, таких як атомні електростанції або хімічні заводи. У разі застосування заборонених видів зброї, зокрема хімічної, швидкий збір та аналіз даних про середовище дозволяє оперативно організовувати захист персоналу та населення, а також адаптувати тактику дій. Додатково системи дистанційного моніторингу життєвих показників поранених військовослужбовців у польових шпиталях дозволяють медичним підрозділам швидко реагувати на зміну стану без постійної фізичної присутності біля пацієнтів.

Об’єкти військової інфраструктури, такі як командні штаби, склади, блокпости або пункти зв’язку, також можуть бути обладнані засобами контролю доступу та виявлення несанкціонованих проникнень з використанням IoT-технологій — наприклад, камери з автоматичним розпізнаванням руху, магнітні сенсори для дверей, сенсори вібрації, тепловізори, а також системи дистанційного сповіщення. Усе це спрямоване на забезпечення постійного контролю за безпекою об’єктів у реальному часі та зниження ризику диверсій, несанкціонованого доступу чи пошкодження критично важливих ресурсів (див. рис. 1.4).



Рисунок 1.4 – Основні сфери військового застосування IoT: розвідка, логістика, моніторинг стану середовища та об’єктів

У сукупності різні напрями застосування IoT у військовому контексті створюють потужну технологічну основу, яка дозволяє організовувати дії ефективніше, швидше та з меншими втратами, забезпечуючи збройним силам новий рівень координації, захисту та стійкості до загроз.

Вимоги до надійності, безпеки та масштабованості. У військовому середовищі технічні системи повинні відповідати суворим вимогам, оскільки середовище експлуатації є надзвичайно агресивним, а самі IoT-рішення становлять потенційно вразливий сегмент, що потребує особливої уваги. Вимоги до надійності охоплюють не лише фізичну стійкість пристроїв, а й їхню здатність безперебійно функціонувати в умовах:

- екстремальних температур (від мінус 40 до плюс 60 градусів Цельсія);
- підвищеної вологості;
- запиленості;
- вібрацій;
- механічних ударів.

Водночас критично важливою є програмна стабільність, зокрема здатність систем до самостійного відновлення після збоїв, реалізація резервних алгоритмів та забезпечення неперервного функціонування в умовах перебоїв зв’язку або втрати окремих компонентів. Використання ненадійних сенсорів або несправність у каналах передачі даних може призвести до хибних тривог або, навпаки, до відсутності сповіщення про загрозу, що у військових умовах здатне мати фатальні наслідки. Саме тому якість і стабільність усіх елементів системи має бути предметом постійного контролю (див. рис. 1.5) [4-5].

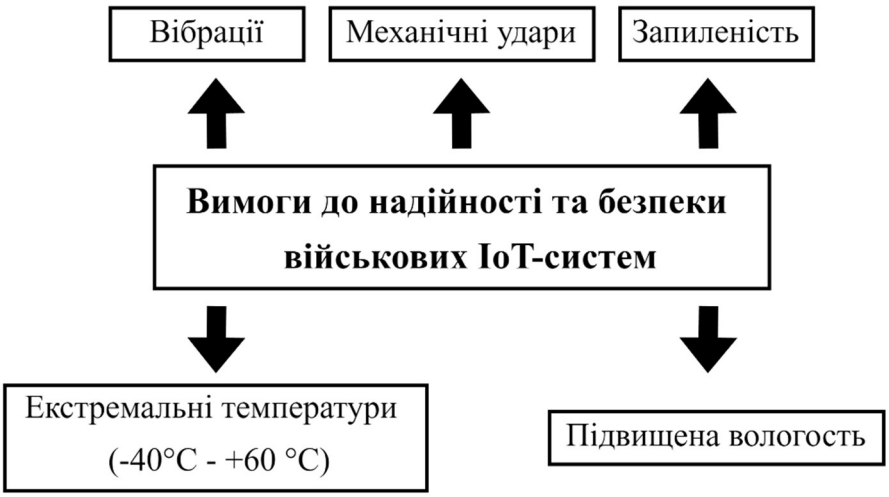


Рисунок 1.5 – Вимоги до надійності та безпеки військових IoT-систем

Окрім вимог до надійності, надзвичайно важливо враховувати і безпековий аспект, адже обмін даними в IoT-системах часто відбувається через відкриті або напіввідкриті канали зв’язку, що створює серйозні ризики їх перехоплення, підміни чи злому. Передача даних у зонах бойових дій без належного шифрування може стати інструментом ворога, тому для запобігання таким сценаріям застосовуються сучасні методи криптографічного захисту, включно з TLS, автентифікацією пристроїв через ключі доступу, зокрема апаратні, а також захистом прошивки від модифікацій шляхом використання secure boot та OTP-механізмів. Особливо це важливо при створенні пристроїв на основі мікроконтролерів, які потребують захисту не лише на рівні софту, а й апаратної частини. Також має бути передбачено обмеження доступу до фізичних інтерфейсів, що унеможливлює стороннє втручання в налаштування або перехоплення трафіку. Не менш важливими є регулярні оновлення програмного забезпечення, які мають здійснюватися лише через захищені канали, адже в іншому випадку є ризик встановлення зловмисного коду, що може повністю змінити функціональність системи та поставити під загрозу життя військових [4-5].

Крім вимог до безпеки та надійності, не менш важливою є масштабованість рішень, адже умови на фронті змінюються динамічно — не щомісяця чи щотижня, а щогодини. Системи мають підтримувати легке додавання нових пристроїв без

потреби повного переналаштування, що можливо завдяки використанню протоколів самоорганізації, таких як Zigbee, LoRaMesh, або шляхом гнучкого конфігурування через централізовану платформу керування, яка дозволяє швидко масштабувати систему чи переносити конфігурацію на інший майданчик у разі втрати або знищення обладнання. Така гнучкість критично необхідна в умовах бойових дій, де стабільність і швидкість розгортання нових елементів мережі мають безпосередній вплив на ефективність виконання завдань [5].

Обмеження при використанні IoT на фронті. Утім, упровадження IoT у зонах бойових дій супроводжується низкою суттєвих обмежень, які вимагають як апаратної, так і програмної адаптації. Багато рішень, створених для цивільного використання, не здатні функціонувати ефективно у військовому середовищі без додаткового захисту, інакше їхня робота може бути не лише неефективною, а й небезпечною. Одним із головних обмежень є живлення, оскільки у фронтових умовах часто немає доступу до електромереж, і пристрої повинні працювати автономно — від акумуляторів, сонячних панелей або одноразових батарей. У зв’язку з цим надзвичайно важливим стає використання енергоощадних технологій: сплячі режими мікроконтролерів, рідкісна передача даних, застосування енергоефективних протоколів на кшталт MQTT або LoRa, які хоч і обмежують швидкість передачі, проте суттєво подовжують час автономної роботи, що в умовах бойових дій є ключовою перевагою. Часто автономна робота протягом двох-трьох діб без зарядки вже може стати критичною перевагою, адже у порівнянні з цивільними системами, що можуть працювати роками, військові рішення мають набагато ширший функціонал і відповідно — вищі енергоспоживання [4-5].

Значний вплив мають також завади зв’язку та спроби його приглушення, оскільки радіоканали піддаються впливу засобів радіоелектронної боротьби, які можуть створювати перешкоди, глушити частоти, здійснювати спуфінг чи перехоплення пакетів. Тому важливо мати резервні канали зв’язку та можливість перемикання між ними, наприклад із Wi-Fi на LoRa чи GSM, а також реалізувати періодичну зміну ключів доступу, шифрування трафіку та механізми повторної

передачі з перевіркою цілісності. Значну роль відіграє застосування пасивних сенсорів, які не випромінюють сигнали, а лише приймають їх, або активація зв’язку лише за потреби, що знижує ризик виявлення пристрою ворогом. Така архітектура дозволяє забезпечити більшу стійкість систем до зовнішнього втручання та зберегти їх функціональність навіть у найгірших сценаріях [4-5].

Окрему увагу необхідно приділити мобільності та можливостям розгортання систем у польових умовах. Пристрої часто встановлюються на місцевості без жодної інфраструктури — на деревах, в ґрунті, на техніці, одязі або безпілотниках — тому конструкція повинна бути максимально компактною, замаскованою, без світлодіодних індикаторів, із захистом від води, пилу та механічних пошкоджень. Інтерфейс налаштування має бути інтуїтивно простим, із можливістю конфігурації з мобільного пристрою через Bluetooth або NFC без використання комп’ютера, що дозволяє забезпечити гнучкість, зручність та оперативність налаштувань навіть у складних умовах, не вимагаючи додаткового навчання військовослужбовців (див. рис. 1.6).



Рисунок 1.6 – Типові обмеження IoT-рішень у бойових умовах: коротка тривалість роботи, фізична та радіо- незахищеність

Усі обмеження, що існують у використанні IoT на фронті, повинні бути зведені до мінімуму шляхом ретельної інженерної адаптації, що дозволить значно підвищити ефективність таких систем у реальних бойових умовах.

Приклади бойових кейсів застосування IoT. Серед бойових кейсів застосування IoT можна розглядати кілька типових сценаріїв, які вже реалізуються на практиці в умовах активних бойових дій. Одним із найбільш поширених прикладів є система спостереження за периметром, коли в зоні відповідальності підрозділу розміщується множина малопомітних сенсорів руху та вібрації, які працюють автономно і передають сигнал лише у випадку активації. При виявленні руху передається інформація щодо координат події та типу спрацювання — наприклад, чи йдеться про людину, чи про техніку — безпосередньо до мобільного командного пункту (див. рис. 1.7).



Рисунок 1.7 – Бойові кейси застосування IoT

Такий підхід забезпечує можливість виявляти противника ще до безпосереднього контакту, не потребуючи постійної присутності спостерігача в небезпечній зоні, що значно підвищує рівень оперативності реагування та зменшує ризики для особового складу.

Інший приклад — моніторинг стану техніки, що передбачає встановлення IoT-модулів безпосередньо на броньовані машини або інші транспортні засоби для фіксації технічних показників, як-от температура двигуна, напруга бортової мережі чи витрата пального. Дані надходять до планшета або іншого пристрою водія, що дає змогу виявити потенційну несправність до її реального прояву та провести необхідне технічне обслуговування або заміну елементів, не чекаючи поломки в критичний момент. Такий підхід суттєво підвищує надійність технічних засобів у польових умовах, особливо коли враховується фактор відсутності часу чи ресурсів на екстрений ремонт під час бою, а мініатюризація та енергоефективність IoT-пристроїв дозволяють інтегрувати їх у вже наявні системи без значного ускладнення їхньої структури.

Ще одним прикладом бойового використання є логістичне відстеження вантажів, де всі поставки — як гуманітарні, так і військового призначення — можуть маркуватися спеціальними IoT-маячками, які дозволяють відстежувати їхнє місцезнаходження в реальному часі. Такий підхід зменшує ймовірність втрати чи крадіжки вантажів, а також дає можливість оперативно координувати передачу матеріальних засобів між підрозділами. Разом із тим важливо враховувати загрози, пов’язані з безпекою передачі даних, оскільки відкрите передавання координат може бути перехоплене противником, тому обов’язковим є впровадження засобів шифрування, автентифікації та обмеження доступу до систем управління такими маячками. Водночас у разі безпечної реалізації логістичний трекінг дозволяє реагувати на зміну обстановки на фронті майже в режимі реального часу та більш точно координувати дії постачання відповідно до потреб підрозділів, що значно підвищує стійкість військової інфраструктури.

Також окремо варто виділити приклад інтелектуальної системи раннього попередження, яка базується на сенсорній мережі, розгорнутій поблизу лінії фронту або в критичних районах, де існує ймовірність прориву, штурму або раптової активізації ворога. Така мережа здатна автоматично виявляти стрільбу, підриви, переміщення техніки або груп солдатів і в разі підтвердження загрози генерує сигнал тривоги або ініціює автоматизований зворотній удар за

визначеними координатами. Важливою характеристикою цієї системи є відсутність участі людини на етапі збору і первинної обробки даних, що дозволяє зосередитися на аналізі і прийнятті рішень, не витрачаючи час на ручне спостереження. При цьому автономність функціонування таких мереж дозволяє підтримувати їхню роботу з мінімальним втручанням, а енергоефективність і стійкість до збоїв робить їх застосування доцільним навіть у найскладніших ділянках фронту.

Загалом кожен із розглянутих кейсів ілюструє конкретні приклади підвищення ефективності бойових дій за рахунок інтеграції IoT-рішень у вже наявні процеси:

— командування;
— технічного обслуговування;
— логістики;
— розвідки.

Таке впровадження не тільки покращує ситуаційну обізнаність і скорочує час реакції, а й сприяє більш гнучкому використанню ресурсів у змінних умовах війни, дозволяючи реагувати на динаміку бойової обстановки з максимальною точністю та мінімальним людським ризиком.

1.3 Компоненти військових IoT-систем

IoT-система у військовому контексті являє собою сукупність пристроїв та технологій, здатних забезпечити повний цикл збору, обробки, передачі й відображення критично важливої інформації з поля бою, де її ефективність визначається взаємодією чотирьох базових груп компонентів, адаптованих під специфіку збройного конфлікту, а саме:

— сенсорних модулів;
— засобів передачі даних;
— пристроїв обробки інформації;

— кінцевих точок користувача.

Усе це в сукупності дозволяє структурувати систему за функціональним принципом і створювати гнучкі рішення, здатні до масштабування й оперативного налаштування згідно з потребами конкретної операції [6-7].

Сенсорні модулі та типи датчиків. У цій структурі сенсори виступають своєрідними «очима» та «вухами» IoT-систем, адже саме вони здійснюють первинне зчитування інформації з навколишнього середовища або технічних об’єктів, що в умовах динамічного і нестабільного військового середовища набуває особливої ваги, оскільки вимагає підвищеної надійності, автономності та стійкості до зовнішніх впливів. Серед базових типів сенсорів, які застосовуються у військовому середовищі, насамперед варто розглянути сенсори руху — пасивні інфрачервоні (PIR), ультразвукові або комбінаційні модулі, призначені для фіксації присутності та переміщення об’єктів. У реальних бойових кейсах такий сенсор здатен безшумно визначити наближення піхоти або тварин у зоні периметру, виступаючи складовою безпілотних систем охорони, тилових спостережних пунктів або механізмом активації складніших ланцюгів детекції, коли одночасне спрацювання кількох сенсорів автоматично передає координати і контекст події до командного центру через інтегровані планшети або комп’ютери (див. рис. 1.8) [6].

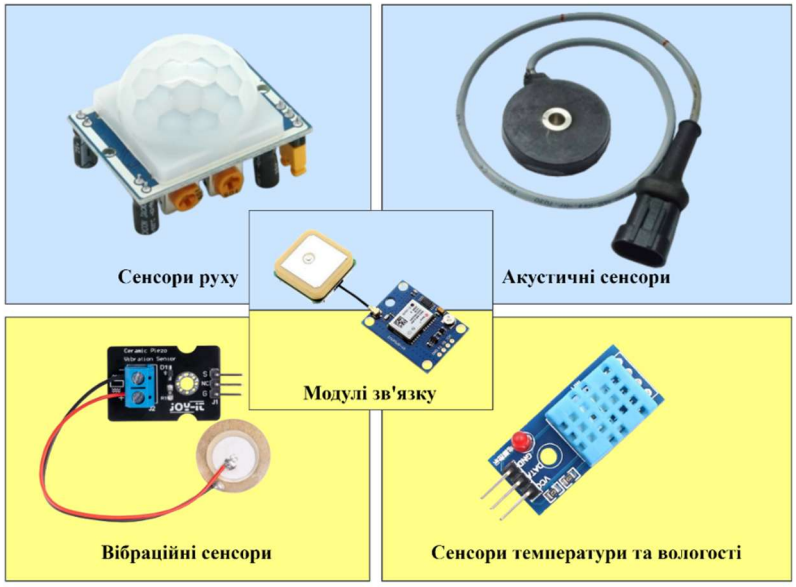


Рисунок 1.8 – Приклади сенсорних модулів для військових цілей

Окремо функціонують акустичні сенсори, що включають мікрофони, спектральні аналізатори та інші аудіомодулі, призначені для виявлення звуків двигунів, пострілів і вибухів. Їх особливість полягає в здатності класифікувати тип об’єкта на основі звукового профілю — наприклад, розпізнати характерний шум гусениць танка, роботи двигуна БМП або навіть польоту дрона, завдяки попередньо завантаженим шаблонам, що дозволяє здійснювати аудіорозвідку, локалізувати джерело загрози через методи триангуляції і надати точні координати для контрудару або запобігання прориву.

Ще одним важливим класом сенсорів є сенсори вібрації, до яких належать акселерометри, геофони та інші модулі фіксації механічних коливань поверхні або ґрунту. У військових умовах вони можуть бути замасковані як непомітні пастки або слугувати механізмом контролю стратегічних інфраструктурних елементів, таких як мости, дороги, вузькі проходи. Із їх допомогою можливе створення віртуального «силуету» об’єкта за даними коливань, що дозволяє реагувати навіть на мінімальні зміни в середовищі.

Температурні й вологісні сенсори, добре відомі у цивільному секторі, в бойових умовах знаходять своє місце в моніторингу стану техніки, підтримці мікроклімату в медичних шпиталях, контролі умов зберігання боєприпасів, а також у виявленні теплових аномалій — таких як присутність людини, тління, запуск двигуна. Завдяки своїй простоті та енергоефективності вони можуть працювати в автономному режимі і передавати дані лише у разі виявлення відхилення, що особливо корисно при прихованому спостереженні.

GPS-модулі як частина сенсорних систем застосовуються не тільки для навігації, а й для відстеження руху техніки, вантажів, автономних сенсорних станцій, безпілотників та бойових одиниць. Їх інтеграція з картою реального часу дозволяє бачити просторову динаміку всієї IoT-системи, координувати переміщення, формувати логістичні маршрути та здійснювати автоматичне оновлення позицій об’єктів. Поєднання різних типів сенсорів у межах однієї платформи дозволяє створювати спеціалізовані гібридні пристрої, що виходять за

рамки стандартних рішень ринку і орієнтовані виключно на потреби конкретного театру військових дій.

Загалом сенсорні модулі військових IoT-систем формують основу для подальшого аналізу, прийняття рішень і автоматичного реагування, забезпечуючи автономність, прихованість і стійкість системи в цілому, а також відкриваючи нові можливості для інтеграції з іншими компонентами — обчислювальними модулями, передавачами, енергоживленням і засобами взаємодії з оператором, що у свою чергу формує єдине інформаційне поле з високим рівнем адаптивності до реального бойового середовища.

Пристрої обробки інформації. У контексті військових IoT-систем передавання даних є критично важливим етапом після первинного збору інформації сенсорами, оскільки лише на основі своєчасного й надійного транспортування цієї інформації до вузлів обробки чи зберігання можна забезпечити дієве реагування. Для досягнення цього застосовуються різноманітні протоколи і технології передачі даних, що підбираються залежно від потреб, типу розгортання та навколишнього середовища. У військових умовах, що супроводжуються ризиками знищення інфраструктури, блокуванням сигналів і необхідністю мобільності, ключовими стають ті протоколи, які здатні забезпечити дальню і стабільну передачу з низьким енергоспоживанням. Однією з таких технологій є LoRa (Long Range Radio), що, хоча й характеризується низькою швидкістю передачі даних — від 0,3 до 50 кб/с — дозволяє встановлювати зв’язок на відстані до 10–15 км у відкритій місцевості за умови прямої видимості, при цьому споживаючи мінімум енергії. В умовах фронту такі характеристики дають змогу будувати сенсорні мережі трекінгу, сповіщення про події або активації систем, які працюють автономно й стійкі до перешкод, адже вузькополосний сигнал LoRa складніше виявити й заглушити [7].

Розширеною версією цієї технології є LoRa Mesh, яка додає можливість самовідновлення мережі: кожен вузол здатен не лише приймати, а й ретранслювати сигнал, утворюючи гнучку й «живучу» мережу, здатну зберігати працездатність навіть у випадку втрати окремих вузлів. Такі мережі не вимагають жорстко

зафіксованої інфраструктури, що особливо корисно у військових операціях, коли конфігурація мережі може змінюватися в реальному часі залежно від дій противника, рельєфу чи руху підрозділів. Наприклад, навіть якщо частина мережі буде знищена або втратить зв’язок, інформація продовжить передаватися іншими шляхами завдяки автоматичному перемаршрутизуванню, що суттєво підвищує надійність всієї системи [7].

Ще одним засобом безпровідної передачі є Wi-Fi, відомий своєю високою швидкістю та сумісністю з великою кількістю пристроїв, однак у військовому застосуванні він має суттєві обмеження. Дальність дії в середньому не перевищує 100 метрів, а енергоспоживання може бути критичним у польових умовах, що накладає обмеження на тривалість роботи від батарей. Проте Wi-Fi часто використовується там, де необхідна швидка передача великих обсягів даних — наприклад, відео або знімків з дронів, польових планшетів, або при сполученні з більш потужними пристроями обробки даних, які мають доступ до джерел живлення. Його використання виправдане у точках концентрації інфраструктури або для короткотривалого зв’язку [7].

Окремий клас засобів передачі — супутниковий зв’язок, який в умовах втрати або відсутності традиційної інфраструктури дозволяє зберегти постійний канал зв’язку. Найбільш поширеним рішенням у цьому напрямку стало використання Starlink, який завдяки сузір’ю супутників забезпечує широке покриття і порівняно високу швидкість, а також інші системи на кшталт Iridium або Thuraya. Головна перевага — стійкість до втрати наземної інфраструктури, адже дані передаються безпосередньо між польовими пристроями й супутниками, що дозволяє працювати навіть у зонах активного бойового зіткнення. У типових прикладах польовий сенсорний вузол передає дані на проміжний вузол, а звідти через супутниковий канал — до головного штабу, що ілюструє вертикальну схему передачі інформації без участі звичайної інфраструктури зв’язку.

Однак ефективність такої передачі неможлива без пристроїв, які здатні не лише прийняти дані, а й обробити їх, проаналізувати або трансформувати перед

тим, як передати далі. У цій ролі виступають пристрої з обчислювальними можливостями, які розподіляються на дві ключові категорії:

— мікроконтролери;

— одноплатні комп’ютери.

До перших належать такі рішення як Atmega 328, STM32, Arduino, ESP32, що мають низьке енергоспоживання, компактність, дешевизну і здатні виконувати базову обробку сигналів — наприклад, реагувати на перевищення певного порогу чи активувати передачу лише при виявленні конкретного тригера. Їхні обмеження полягають у відносно невисокій обчислювальній потужності та обсязі пам’яті, однак саме це дозволяє їм залишатися автономними протягом тривалого часу, що критично у зоні бойових дій (див. рис. 1.9).

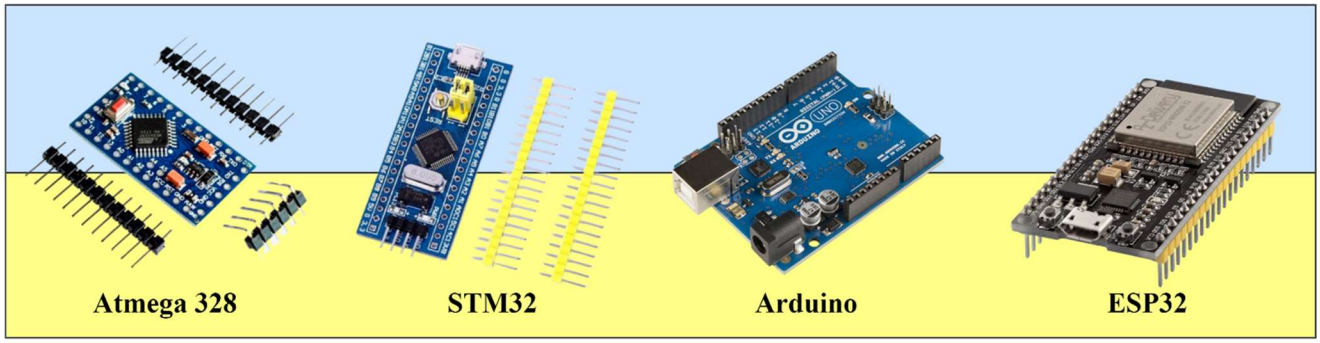


Рисунок 1.9 – Мікроконтролер як вузол обробки

Інша категорія — одноплатні комп’ютери (SBC — Single Board Computer), як-от Raspberry Pi, Orange Pi, Jetson Nano — які здатні обробляти зображення, працювати з відео, аудіо, запускати Python-скрипти й навіть моделі машинного навчання, що дає змогу реалізовувати складні системи розпізнавання подій, класифікації пострілів чи автоматичного трекінгу (див. рис. 1.10).

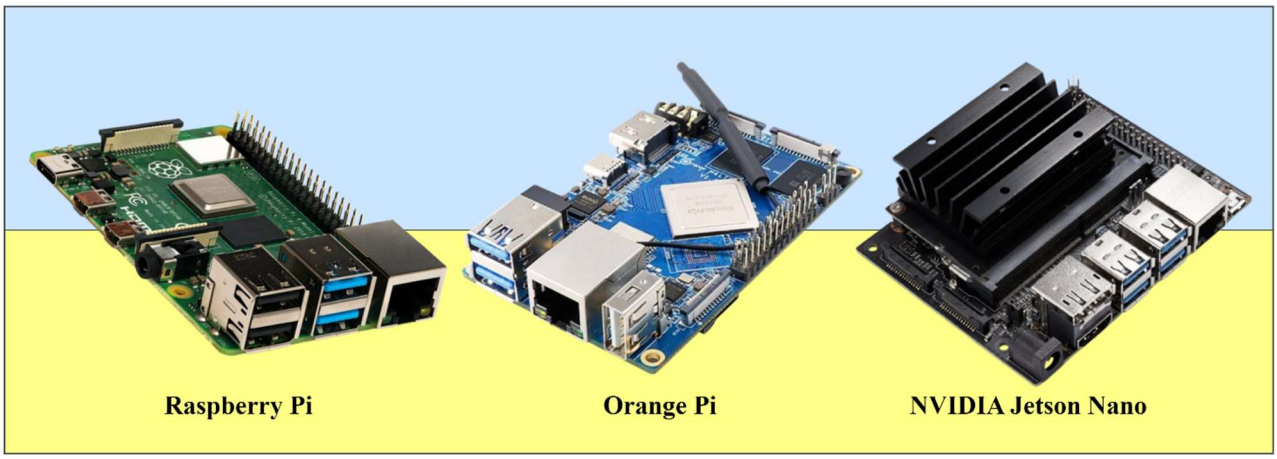


Рисунок 1.10 – Одноплатний комп’ютер як вузол обробки

Ці пристрої мають вищі вимоги до живлення й охолодження, однак відкривають ширші можливості щодо інтеграції складних функцій, зокрема — аналітики з відеозронів або обробки сигналів з кількох джерел.

Окрему нішу займають гібридні модулі, на кшталт ESP32-CAM, які поєднують у собі мікроконтролер, модуль Wi-Fi, Bluetooth і камеру. Завдяки цьому можливе створення автономних мініатюрних систем спостереження, що активуються лише у разі події, фіксованої сенсорною мережею — наприклад, зафіксований рух викликає активацію камери, що передає знімки або коротке відео по Wi-Fi (див. рис. 1.11).

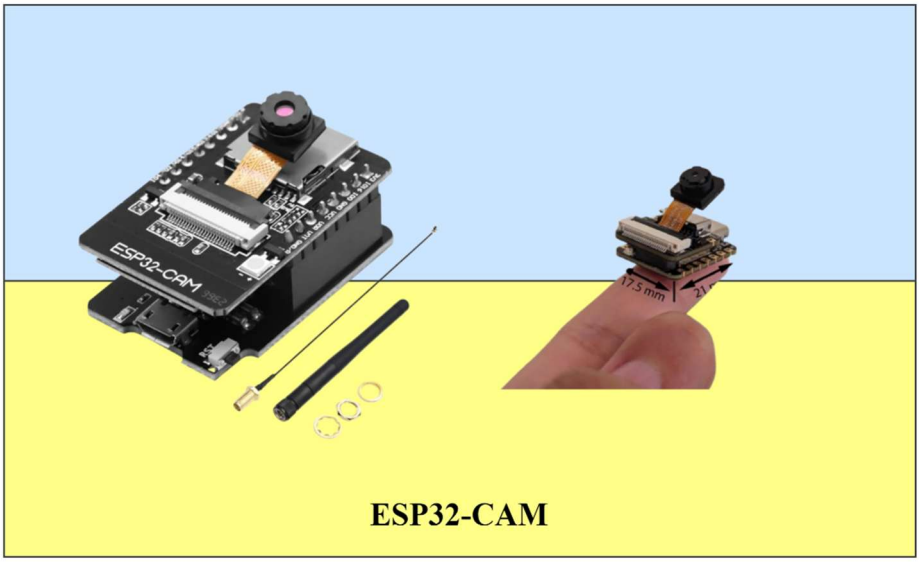


Рисунок 1.11 – Гібридний модуль ESP32-CAM

Такий підхід дозволяє суттєво зекономити заряд батареї, водночас забезпечуючи актуальну візуальну інформацію в реальному часі, що особливо важливо в польових умовах, де кожна одиниця енергії на рахунку. У сукупності ці технології й компоненти формують багаторівневу, гнучку і стійку до зовнішніх впливів систему збору, обробки та передавання інформації, адаптовану під вимоги сучасного ведення війни.

Кінцеві точки – інтерфейси доступу для військових. Інформація, що збирається з розгалуженої системи сенсорів і пристроїв, має не лише зберігатися чи передаватися, а й ефективно доходити до тих, хто приймає рішення, зокрема до командирів, операторів чи спеціалістів, які мають швидко оцінити ситуацію і вжити відповідних заходів, тому системи повинні передбачати надійні, захищені та зручні кінцеві точки доступу, що дозволяють отримувати й обробляти дані у зрозумілому та контекстно доцільному вигляді з урахуванням реалій бойового поля. Найбільш поширеним прикладом таких кінцевих пристроїв у польових умовах є планшети та смартфони, які поєднують мобільність, компактність, інтегровані GPS-модулі, камери, доступ до цифрових мап і сенсорних даних із можливістю запуску спеціального програмного забезпечення для управління пристроями, аналізу обстановки чи перегляду сповіщень від IoT-вузлів. Використання планшетів і смартфонів передбачає наявність програм із шифруванням, захистом від несанкціонованого доступу, режимами енергозбереження й «тиші», а також спеціальними антивандальними оболонками для фізичного захисту, що дозволяє зберігати безпечний доступ до даних навіть у випадку потрапляння пристрою до рук противника.

Окрім мобільних пристроїв, вагому частку у структурі інтерфейсів займають ноутбуки та портативні робочі станції, які мають вищу продуктивність і здатні виконувати аналітичні чи координаційні завдання в реальному часі, працюючи з кількома потоками інформації одночасно. Їхнє використання доцільне в межах командних пунктів, де відбувається прийом, обробка та візуалізація телеметрії, аналіз даних ситуаційної обстановки та координація дій підрозділів, а сам пристрій

часто розміщується в захищеному корпусі й інтегрується з іншими компонентами системи для комплексної роботи (див. рис. 1.12).



Рисунок 1.12 – Кінцева точка доступу для військового персоналу

Важливою складовою є і повноцінні командні центри, які виходять за межі портативних рішень і являють собою стаціонарні або мобільні комплекси з розгорнутою інфраструктурою — великими екранами, серверами, системами зберігання даних, інструментами для геоаналітики, прийому відео з БПЛА, повідомлень від польових сенсорів, супутникових знімків і результатів розвідки, що забезпечує об’єднання розрізнених джерел інформації у єдине інформаційне поле для прийняття стратегічних рішень (див. рис. 1.13).

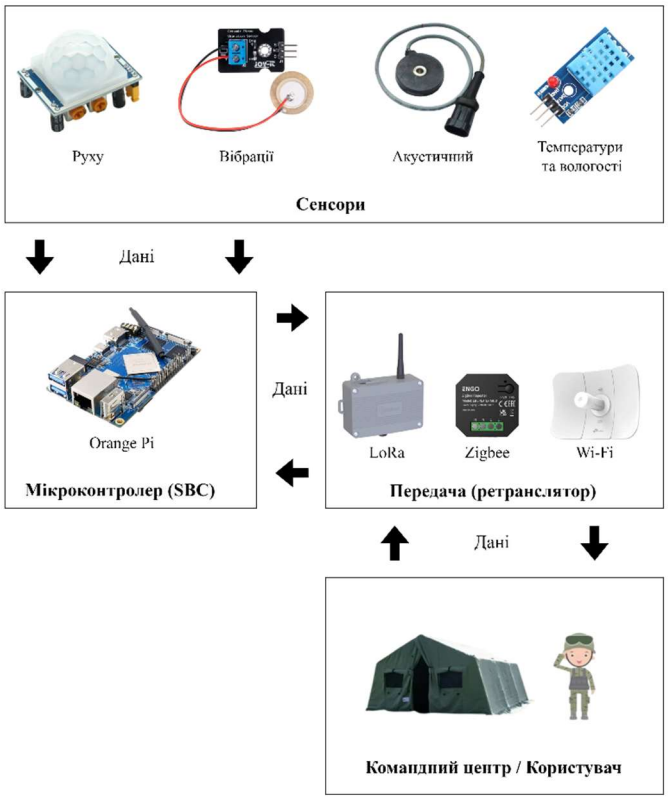


Рисунок 1.13 – Схема взаємодії компонентів IoT-системи

Таблиця 1.1 – Основні компоненти військових IoT-систем

№	Група компонентів	Основні приклади	Ключові функції та застосування
1	Сенсорні модулі	PIR, акустичні, геофони, температурні, GPS	Виявлення руху, звуків, вібрацій, температури; позиціювання; запуск тригерів
2	Засоби передачі даних	LoRa, Zigbee, Wi-Fi, супутниковий інтернет	Надійна передача інформації в різних умовах: від ближньої дії до глобального покриття
3	Обчислювальні пристрої	MCU (STM32, ESP32), SBC (Raspberry Pi), ESP32-CAM	Обробка даних, агрегація, локальне прийняття рішень, запуск ML-алгоритмів
4	Кінцеві точки для користувача	Смартфони, планшети, ноутбуки, центри управління	Візуалізація, управління, командування, аналіз бойової ситуації

У підсумку (див. табл. 1.1), уся структура військової IoT-системи є не просто набором пристроїв чи засобів обміну даними, а складною, взаємопов’язаною системою, де кожна складова — від сенсора, що зафіксував подію, до центру, що прийняв рішення — утворює цілісний організм, подібний до людського тіла, в якому жоден елемент не є зайвим і не може бути вилучений без втрати функціональності. Від ефективності кожної ланки залежить:

— швидкість реагування;

— точність дій;

— цілісність інформаційного потоку;

— безпека учасників операції.

Військові IoT-рішення мають бути автономними, захищеними, адаптивними, здатними функціонувати у віддалених і складних умовах без потреби в сталій інфраструктурі, і саме завдяки взаємодії між сенсорами, мережами, обчислювальними модулями та інтерфейсами для кінцевих користувачів утворюється міцна технологічна основа, яка підвищує ефективність операцій у реальному бойовому середовищі.

1.4 Огляд реальних IoT-рішень у військовій сфері

Сучасні війни дедалі більше змінюють свою природу, набуваючи ознак технократичного протистояння, де перевага визначається не лише силою озброєння, а й можливістю глибокої цифрової інтеграції, збору та обробки інформації в реальному часі, застосуванням сенсорних мереж, безпілотних платформ та автономних систем прийняття рішень, що разом формують нову парадигму ведення бойових дій, наближену до умов кіберфізичного протиборства в реальному просторі. У такому контексті реальні IoT-рішення, які вже використовуються у військовій сфері, є не теоретичними моделями чи прототипами на етапі лабораторних випробувань, а повноцінними технічними системами,

випробуваними в бойових умовах і вже адаптованими до потреб сучасного поля бою, тому доречно не лише їх аналізувати, а й спиратися на них при створенні або вдосконаленні власних рішень [8-10].

Ghost Robotics Q-UGV – автономний наземний розвідник. Одним із яскравих прикладів застосування військових IoT-технологій є Ghost Robotics Q-UGV — чотириногий автономний наземний робот, розроблений американською компанією Ghost Robotics, який поєднує в собі функції розвідника, патрульного, транспортувальника спорядження та потенційного бойового учасника з можливістю адаптації під специфіку конкретного завдання. Завдяки модульній архітектурі кожен Q-UGV оснащується широким набором сенсорів, включно з відеокамерами, лідаром, GPS-приймачами та інерціальними датчиками, що забезпечують йому просторову орієнтацію й точність позиціювання навіть у складних умовах. Підключення до комунікаційних мереж здійснюється через Wi-Fi, LTE або 5G-зв'язок, що дозволяє підтримувати синхронізацію з іншими бойовими одиницями або командними центрами без втрати мобільності, а локальна обробка даних та алгоритми штучного інтелекту надають можливість автономного прийняття рішень, обходу перешкод, супроводу об'єктів і навігації на місцевості без участі людини. З огляду на бойовий контекст, така автономність критично важлива в умовах, де будь-який контакт із противником може коштувати життя (див. рис. 1.14) [8].



Рисунок 1.14 – Зовнішній вигляд автономного наземного розвідника Ghost Robotics Q-UGV

Маючи низький профіль та високу маневреність, Q-UGV здатен пересуватись у пересіченій місцевості, а конструкція передбачає можливість дооснащення додатковими антенами, модулями зв’язку, сенсорними системами чи навіть озброєнням, що перетворює його на багатоцільову платформу з високою ступінню адаптації до конкретних завдань. Такий робот здатен передавати зібрані дані до центру управління або іншим роботизованим системам, створюючи локальну інформаційну мережу без прив’язки до фіксованої інфраструктури, що суттєво розширює можливості командування в полі. Завдяки здатності виконувати патрулювання, моніторинг, охорону, участь у розгортанні сенсорних вузлів чи дослідження небезпечних територій (наприклад, мінних полів), подібні платформи фактично беруть на себе функції, які раніше виконували бійці, і таким чином знижують ризик людських втрат.

Саме подібне поєднання робототехніки, сенсорної інтеграції, комунікаційних систем і автономного управління формує новий вимір ведення бойових дій, де збереження життя, гнучкість операцій і миттєвий обмін даними стають не абстрактними цілями, а досяжними результатами впровадження конкретних технічних рішень, що вже довели свою ефективність у реальних бойових умовах.

DARPA Tactical IoT – сенсорні мережі наступного покоління. Агентство передових оборонних досліджень США (DARPA) ініціювало розробку концепції Tactical IoT як відповідь на зростаючу потребу створення розосереджених сенсорних мереж, здатних функціонувати в умовах сучасного бойового простору, де традиційні способи спостереження й комунікації втрачають ефективність. Головна ідея цієї ініціативи полягає у формуванні масштабної, адаптивної, інтелектуальної системи, яка може автоматично збирати, обробляти та передавати дані з тисяч сенсорів у реальному часі, забезпечуючи таким чином ситуаційну обізнаність без необхідності постійної присутності військ на місці. Розгортання мережі базується на застосуванні мініатюрних пристроїв, які можуть бути вручну розміщені в зоні бойових дій або скинуті за допомогою дронів, створюючи розгалужену систему збору даних, що здатна покривати великі території з високою гнучкістю (див. рис. 1.15) [8].

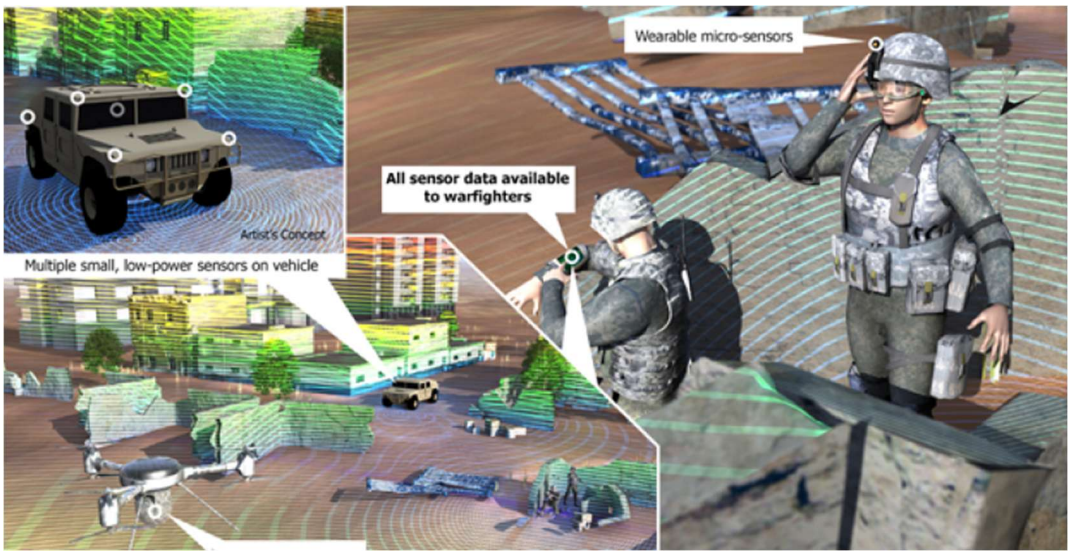


Рисунок 1.15 – Візуалізація сенсорної мережі DARPA Tactical IoT [8]

Система передбачає обробку інформації безпосередньо на рівні сенсорів завдяки вбудованим елементам edge computing, що у поєднанні з алгоритмами машинного навчання дозволяє здійснювати первинну аналітику прямо в польових умовах, автоматично фільтруючи некритичну інформацію та передаючи лише важливі сигнали про потенційні загрози, такі як звук техніки, вибухи або переміщення. Мережева архітектура передбачає самовідновлення — навіть у разі втрати окремих вузлів інформаційний обмін не припиняється, а система самостійно прокладає нові маршрути для передачі даних, що суттєво підвищує живучість та надійність у нестабільних умовах.

Зібрана інформація виводиться у вигляді тактичної візуалізації, інтегруючись у карти або AR-інтерфейси, що дає змогу оперативно приймати рішення на основі актуальних даних. Масштабованість такої системи дозволяє забезпечити контроль над значними ділянками території, а її автономність — зменшити навантаження на операторів і зосередитись на стратегічних рішеннях. Особливо важливою перевагою стає низька латентність, завдяки якій критичні повідомлення негайно надходять до командних пунктів, зберігаючи час реагування в межах секунд. Використання цієї концепції формує свого роду електронну павутину, яка безперервно моніторить ситуацію, дозволяючи своєчасно виявляти загрози,

координувати дії між підрозділами та адаптувати тактику відповідно до змін у бойовій обстановці.

БПЛА Furia та Leleka-100 – українські рішення з телеметрією. На тлі глобальних технологічних трендів важливо усвідомлювати, що сучасні технологічні рішення з успіхом реалізуються не лише провідними західними оборонними структурами, а й на рівні національних ініціатив. Українські безпілотні літальні апарати, такі як Furia та Leleka-100, стали прикладами ефективного впровадження телеметричних систем у бойових умовах, де технологічна автономність і гнучкість у використанні мають вирішальне значення. Розроблений компанією «Атлон Авіа» БПЛА Furia виконує функції розвідки, коригування артилерійського вогню та ретрансляції сигналів, маючи високоточну GPS-навігацію, передачу відео й телеметрії у реальному часі, а також систему шифрування для захисту даних від перехоплення. Автопілот з алгоритмами стабілізації маршруту на основі штучного інтелекту дозволяє апарату функціонувати автономно навіть в умовах перешкод і складної географії [9].



Рисунок 1.16 – Зовнішній вигляд БПЛА Furia зі системою телеметрії

Іншим прикладом вітчизняної розробки є БПЛА Leleka-100 від компанії «Девіро», який відзначається здатністю до автономного польоту за заздалегідь заданими точками з постійним зворотним зв’язком через телеметричні канали, що передають стан системи, рівень заряду акумулятора, координати, сигнал зв’язку, а також фото- й відеодані до командних пунктів для оперативного аналізу. У загальному розумінні ці платформи виконують роль мобільних сенсорів, які

можуть вільно змінювати положення у просторі, виконувати розвідку, виявляти цілі, координувати атаки та здійснювати ретрансляцію сигналів від інших пристроїв у тил, що надзвичайно важливо у зонах з нестабільним або ворожим радіочастотним середовищем (див. рис. 1.17) [9].



Рисунок 1.17 – Зовнішній вигляд БПЛА Leleka-100 зі системою телеметрії

Подібні рішення довели свою ефективність у реальних умовах бойових дій, ставши органічною складовою військової інфраструктури. У контексті обмеженого доступу до високотехнологічного імпортного обладнання, впровадження таких систем локального виробництва значно пришвидшує їхню адаптацію до умов конкретного театру бойових дій, а також забезпечує оперативну модернізацію відповідно до зворотного зв’язку з фронту. Такі БПЛА виступають не просто як платформи для збору інформації, а як інтегровані елементи військової екосистеми, де телеметрія, штучний інтелект та сенсорна інтеграція поєднуються у єдину функціональну систему, здатну оперативно реагувати на виклики сучасного збройного конфлікту.

Starlink – супутниковий інтернет для бойових підрозділів. Система Starlink, розроблена компанією SpaceX, забезпечує супутниковий інтернет через мережу тисяч низькоорбітальних супутників, і з 2022 року її активно застосовують українські військові підрозділи, зокрема в умовах, коли традиційна інфраструктура зв’язку або сильно пошкоджена, або повністю знищена. Завдяки супутниковому

інтернету стало можливим утримувати стабільний зв’язок у найвіддаленіших та найнебезпечніших районах, де звичайні засоби комунікації втрачають ефективність. Забезпечення глобального покриття, включно з зонами, що позбавлені мобільного сигналу, дає змогу безперервно отримувати й передавати дані навіть у найскладніших обставинах, а висока пропускна здатність дає змогу обробляти відеопотоки, телеметричну інформацію, а також дані з дронів та сенсорних мереж, зокрема у реальному часі (див. рис. 1.18).



Рисунок 1.18 – Зовнішній вигляд супутникового інтернету Starlink

Завдяки інтеграції з польовими шлюзами, такими як мобільні точки доступу Wi-Fi, або мікросерверами на базі Raspberry Pi, Arduino чи інших мікроконтролерах, забезпечується передача зібраної інформації до командних центрів, що дає змогу формувати повну картину ситуації на місці (див. рис. 1.19) [10].

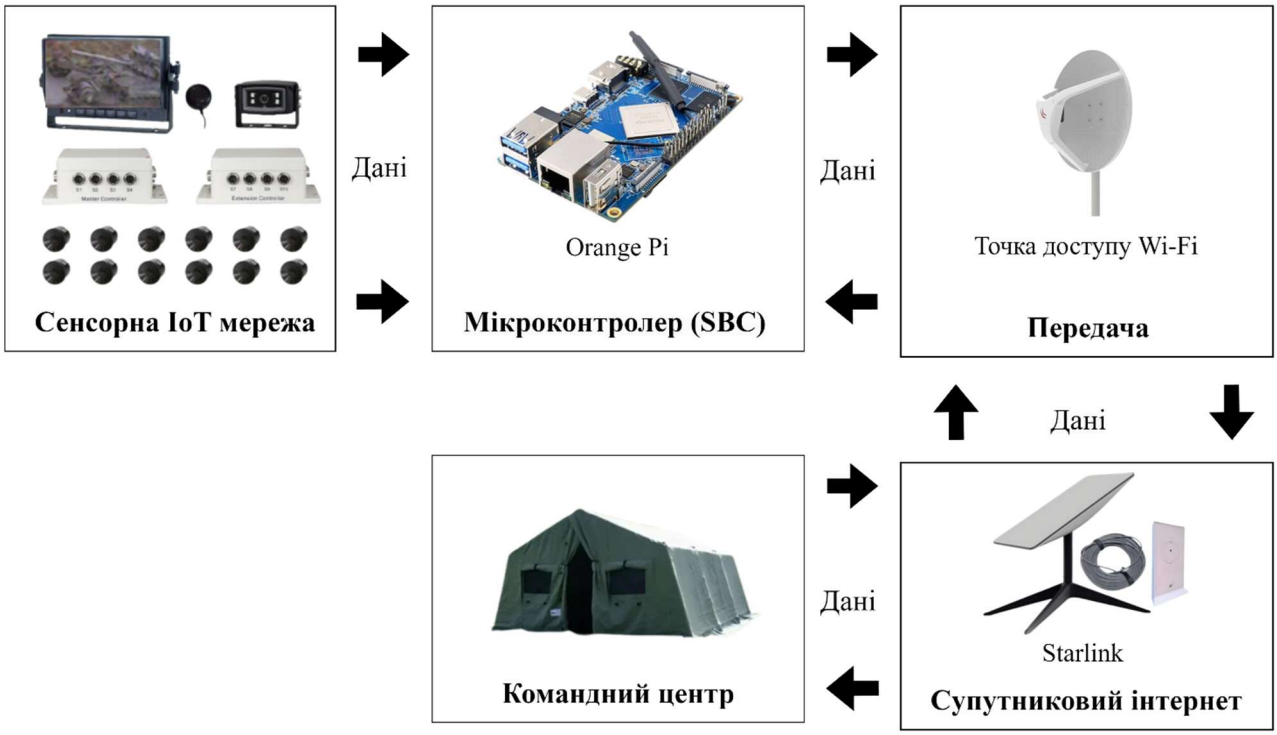


Рисунок 1.19 – Сценарій інтеграції Starlink з військовими IoT-пристроями

Незалежність від локальної інфраструктури надає цій технології додаткової гнучкості — вона є мобільною, легко розгортається в польових умовах, адаптується до змін обстановки, підвищує швидкість прийняття рішень і загальну ефективність управління підрозділами. У реальному часі надходять карти, зведення, зображення з безпілотників, дані з сенсорів, що дозволяє коригувати маршрути, виявляти загрози, передавати оновлення моделей штучного інтелекту для автономних платформ і координувати дії з мінімальною затримкою. У підрозділах ЗСУ Starlink активно використовується для передачі відео з камер, обміну телеметрією, підтримки роботи безпілотних систем і модулів спостереження, що критично важливо для збереження безперервного інформаційного потоку на передовій і в тилу. Таке рішення довело свою цінність і стало одним з ключових чинників, що дозволяє зберігати координацію у хаотичних умовах фронту, навіть тоді, коли фізичні канали зв’язку більше не доступні.

Сукупність описаних технологій, включно з DARPA Tactical IoT, українськими БПЛА Furia та Leleka-100 і супутниковою системою Starlink, не є лише проєктами майбутнього, а вже сьогодні діють у реальних умовах, змінюючи

хід бойових операцій щогодини. Вони створюють нову парадигму ведення війни, де вирішальним стає не лише озброєння, а й здатність швидко збирати, аналізувати, передавати й використовувати дані для оперативного прийняття рішень. Кожне з таких рішень — автономне, мобільне, адаптивне — дає змогу своєчасно реагувати на загрози, мінімізувати втрати, посилювати захист особового складу і наносити точкові удари з високою ефективністю (див. табл. 1.2) [8-10].

Таблиця 1.2 – Приклади реальних IoT-рішень у військовій сфері

№	**Назва рішення**	**Розробник / Країна**	**Призначення**	**IoT-складова**	**Військове значення**
1	Ghost Robotics Q-UGV	Ghost Robotics (США)	Патрулювання, розвідка, транспортування спорядження, бойові задачі	Камери, LiDAR, GPS, ІЧ-датчики, mesh-мережі, локальна обробка даних	Заміна людини в небезпечних зонах, мобільні сенсорні вузли, нічне патрулювання
2	DARPA Tactical IoT	DARPA (США)	Масштабована сенсорна мережа для бойових умов	Розосереджені сенсори, AI-аналітика, edge computing, mesh-топологія, AR-візуалізація	Створення "електронної павутини" для постійного моніторингу, раннього виявлення загроз, координації

Продовження таблиці 1.2 – Приклади реальних IoT-рішень у військовій сфері

№	Назва рішення	Розробник / Країна	Призначення	IoT-складова	Військове значення
3	БПЛА Furia	Атлон Авіа (Україна)	Розвідка, коригування вогню, ретрансляція сигналів	GPS-навігація, відео/телеметрія в реальному часі, шифрування, автопілот з AI-стабілізацією	Збір і передача даних у тил, координація дій, забезпечення розвідки в складних умовах
4	БПЛА Leleka-100	DeViRo (Україна)	Автоматизований розвідник з передачею телеметрії та відео	Автономний політ, телеметрія систем, передача зображень до командних пунктів	Мобільний сенсор, ретрансляція сигналів, підвищення ефективності артилерії та ППО
5	Starlink	SpaceX (США)	Супутниковий інтернет у зонах без покриття	Глобальне покриття, висока пропускна здатність, інтеграція з IoT-шлюзами та сенсорами	Координація на передовій, передача даних з дронів і камер, оновлення карт, робота IoT-мереж у бойових умовах

Усе це підкреслює, що інформаційна перевага дедалі більше визначає успіх на полі бою, а технології, створені як у межах міжнародних ініціатив, так і безпосередньо в Україні, уже стали основою сучасного воєнного ландшафту та наближають завершення війни, трансформуючи традиційне бачення безпілотних, сенсорних і комунікаційних систем.

1.5 Порівняльна характеристика технологій зв'язку

У військовому середовищі зв'язок має критичне значення, оскільки від його стабільності та надійності залежить координація, оперативність, ефективність і безпека виконання бойових завдань. У той час як традиційні засоби комунікації часто не відповідають вимогам мобільності, стійкості до перешкод і енергоефективності, виникає необхідність у впровадженні сучасних безпровідних технологій зв'язку, здатних працювати у складних і динамічних умовах поля бою. Розгляд таких технологій, як Wi-Fi, LoRa та Mesh, дозволяє оцінити їх потенціал у різних сценаріях використання — як у тилу, так і безпосередньо на передовій, з урахуванням особливостей роботи, переваг і обмежень кожної з них [11].

Wi-Fi – висока швидкість, але вразливість до перешкод. Wi-Fi як стандарт безпровідного зв'язку зазвичай використовується для передавання великих обсягів даних на короткі відстані, тому в умовах бойових дій його застосовують здебільшого для локального підключення до польових серверів, планшетів, шлюзів або безпілотних літальних апаратів. Висока пропускна здатність, що для новітніх стандартів, як-от Wi-Fi 6, досягає кількох гігабіт за секунду, а також широка доступність і сумісність з великою кількістю пристроїв, робить цю технологію зручною для створення тимчасових точок зв'язку в обмежених умовах, зокрема всередині укриттів, командних пунктів або мобільних центрів управління. Завдяки вже сформованому ринку обладнання Wi-Fi є простим у розгортанні й

налаштуванні, що дозволяє швидко інтегрувати його в існуючі системи передачі даних, зокрема в симбіозі з супутниковими каналами, такими як Starlink.

Разом із тим низка технічних характеристик обмежує сферу ефективного застосування цієї технології у бойових умовах. Обмежена дальність дії, яка в реальних польових умовах рідко перевищує 100 метрів, робить Wi-Fi малопридатним для відкритої місцевості або взаємодії між мобільними підрозділами на значній відстані. Спроби збільшити дальність шляхом підсилення сигналу часто супроводжуються втратою пропускної здатності та стабільності, що може призвести до затримок або повного обриву зв’язку у критичні моменти. Високе енергоспоживання значно знижує автономність польових пристроїв, а чутливість до перешкод і поганий рівень роботи у складному рельєфі або в умовах щільної забудови додатково звужують коло його можливостей. Саме тому Wi-Fi рідко розглядається як основний протокол зв’язку в активній фазі бойових дій, але зберігає свою доцільність у закритих та контрольованих просторах, де є потреба у швидкому передаванні відео, телеметрії чи карт, або для підключення польової техніки до глобальних мереж через ті ж самі супутникові шлюзи.

LoRa – енергоефективність і дальність, але мінімальні обсяги. LoRa, або Long Range, являє собою технологію вузькосмугового безпровідного зв’язку, що орієнтована на передачу невеликих обсягів даних на значні відстані, при цьому забезпечуючи вкрай низьке енергоспоживання. Саме завдяки цим властивостям вона стала надзвичайно актуальною в межах застосування для пристроїв Інтернету речей, які функціонують у віддалених або польових умовах, де автономність та тривалість роботи від батареї відіграють вирішальне значення. Дальність дії LoRa у відкритому просторі може сягати 10–15 км, що дає змогу використовувати її у зонах бойових дій для побудови інфраструктури передачі даних від сенсорів, встановлених на позиціях або в тилу. Підтримка роботи пристроїв на акумуляторах протягом кількох років робить LoRa придатною для розгортання мереж у місцях, де фізичне обслуговування вкрай ускладнене або неможливе. Особливу користь у військових умовах приносить її стійкість до радіозавад завдяки використанню технології розширення спектру CSS, що дозволяє зберігати стабільність зв’язку

навіть за умови інтенсивного електромагнітного впливу. Попри низьку пропускну здатність у межах 0,3–50 кбіт/с, цього вистачає для передачі телеметрії, координат або сповіщень, що не потребують миттєвого оновлення. Затримки передачі, що властиві LoRa, не дозволяють використовувати її для трансляції відео чи обробки великих потоків даних, однак в умовах, де необхідна лише періодична передача простих пакетів інформації, вона залишається ефективним інструментом. Застосування включає сенсорний моніторинг температури, вібрацій, звуків або руху, віддалене розміщення розвідувальних пристроїв і передачу координат від автономних модулів, що дозволяє формувати надійне середовище контролю ситуації на розосереджених ділянках фронту.

Mesh-зв'язок – гнучкість, самовідновлення, адаптивність. У контексті гнучких топологій зв'язку особливу увагу привертає технологія Mesh, яка не є окремим стандартом зв'язку, а радше підходом до побудови мереж, що реалізується на базі рішень на кшталт Zigbee чи ESP-NOW. У таких мережах кожен пристрій функціонує як вузол, здатний приймати, передавати й ретранслювати сигнали інших вузлів, що дає змогу створювати динамічні, самовідновлювані системи без фіксованого центру управління. У разі виходу з ладу одного з вузлів мережа автоматично перебудовується, забезпечуючи передачу даних через альтернативні маршрути, що особливо важливо в умовах бойових дій, де пошкодження інфраструктури є очікуваним явищем. У випадку використання Zigbee чи ESP-NOW, пристрої залишаються мініатюрними, що спрощує їхнє маскування в полі, серед руїн або в лісистій місцевості, а також дозволяє встановлювати їх у великій кількості для покриття широких територій. Дальність передачі між вузлами складає від 100 до 500 метрів, однак ця відстань може бути збільшена завдяки розміщенню додаткових ретрансляторів, що сприяє масштабуванню мережі. Пропускна здатність таких рішень становить приблизно 100–500 кбіт/с, чого достатньо для обміну даними між сенсорами, модулями керування та командними пунктами. Основними перевагами Mesh-зв'язку є гнучкість розгортання, адаптивність до змін у середовищі, відсутність єдиної точки відмови, що дає змогу системі продовжувати функціонування навіть при втраті окремих компонентів [11].

Зокрема, у випадку Zigbee застосовується поняття координатора, який слугує центральним вузлом, однак мережу можна структуризувати у вигляді кількох кластерів із різними координаторами, що знижує ризики збоїв у роботі всієї системи. Попри наявність технічних викликів, пов’язаних із налаштуванням маршрутизації та усуненням несумісностей між пристроями, така модель залишається актуальною в сучасному бойовому середовищі. Проблеми можуть виникати через збільшення затримок при зростанні кількості вузлів у маршруті або внаслідок поганої якості сигналу, однак оптимізація розміщення пристроїв дозволяє звести до мінімуму ці ризики. Живлення таких мереж зазвичай здійснюється від батарейок типу CR2032 або невеликих акумуляторів, а в разі використання ретрансляторів, що потребують більшої енергії, можна застосовувати рішення з резервним живленням. Mesh-системи дозволяють створювати мобільні сенсорні мережі в складних умовах — у лісах, гірських районах, серед міських руїн, де критично важлива оперативна передача інформації без залежності від інфраструктури.

Реалізація подібних мереж може включати взаємодію з автономними наземними роботизованими системами або дрібними дронами, які потребують стабільного локального зв’язку з наземними пристроями, а також використовуватись у персональних рішеннях для відстеження життєво важливих параметрів солдатів, де сенсори, інтегровані у бронежилети або шоломи, здатні передавати дані про температуру, пульс чи інші показники. Навіть у разі втрати зв’язку з центральною точкою, мережа продовжує взаємодію між сусідніми вузлами, забезпечуючи функціонування мінімального інформаційного контуру (див. рис. 1.20).

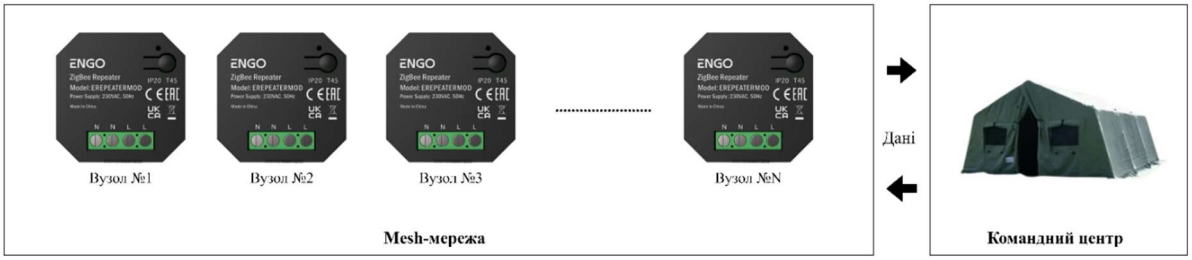


Рисунок 1.20 – Mesh-мережа для військового застосування

Усе це дозволяє Mesh-технологіям залишатися релевантними в умовах сучасної цифрової війни, де мережі мають бути адаптивними, стійкими до пошкоджень і максимально автономними.

Безпека переданих даних у військових умовах. У військових умовах забезпечення безпеки переданих даних є критично важливим, адже перехоплення навіть найпростіших координат або телеметричних показників може спричинити фатальні наслідки, зокрема загибель особового складу чи втрату техніки на передовій, і саме тому кожна з використовуваних технологій повинна максимально ефективно реалізовувати засоби шифрування, автентифікації та захисту переданої інформації, оскільки нехтування цими аспектами безпосередньо впливає не лише на успішність бойових дій, а й на життя конкретних військовослужбовців. У ситуації, коли протокол зв'язку дозволяє використання певного рівня криптографічного захисту, важливо задіювати його повною мірою, особливо з урахуванням сучасного рівня кіберзагроз та технологічних можливостей супротивника, який активно шукає способи втручання в комунікаційні системи.

Наприклад, безпровідна технологія Wi-Fi має підтримку сучасних стандартів безпеки, таких як WPA2 і WPA3, що дозволяє забезпечити відносно надійне шифрування трафіку, а також можливість тунелювання даних через VPN або HTTPS-з'єднання, що створює додаткові рівні захисту при передачі інформації між пристроями або мережами. Однак, разом із цим, Wi-Fi є вразливим до атак типу глушіння сигналу та потребує постійного оновлення прошивок для уникнення відомих CVE-уразливостей, тому використання цієї технології в бойових умовах передбачає постійний контроль за її конфігурацією та технічним станом. На відміну від Wi-Fi, технологія LoRa, що працює в умовах вузькосмугового зв'язку, передбачає застосування AES-128 шифрування на рівні LoRaWAN і забезпечує значно більшу стійкість до глушіння сигналу завдяки своїй низькій пропускній здатності та здатності проходити перешкоди, що робить її ефективною для моніторингу на великих відстанях із мінімальним енергоспоживанням. Особливість LoRa полягає також у тому, що вона здебільшого використовується для односторонньої передачі даних, що ускладнює активне втручання в

комунікацію, проте збільшує ризик підміни сигналів, оскільки базові конфігурації не передбачають складних механізмів автентифікації без використання додаткових шлюзів [11].

Окрему увагу заслуговують сіткові технології, побудовані на основі протоколів типу Zigbee та Thread, які використовуються для створення самовідновлюваних мереж, здатних до динамічного переналаштування маршрутизації у разі втрати окремих вузлів або пошкодження інфраструктури. Такі мережі зазвичай використовують симетричне шифрування, що дозволяє захистити передані пакети від простого перехоплення, проте вони залишаються вразливими до складніших атак, зокрема на маршрутизатори або точки ретрансляції в динамічному середовищі. Проте головною перевагою таких мереж є відсутність центральної точки зосередження трафіку, оскільки кожен вузол може виступати як ретранслятор, що ускладнює централізоване перехоплення або знищення всієї мережі одночасно. Така розподілена структура забезпечує функціонування системи навіть при виході з ладу окремих компонентів, що надзвичайно важливо в умовах бойових дій, де постійно змінюється доступність комунікаційних засобів (див. рис. 1.21).

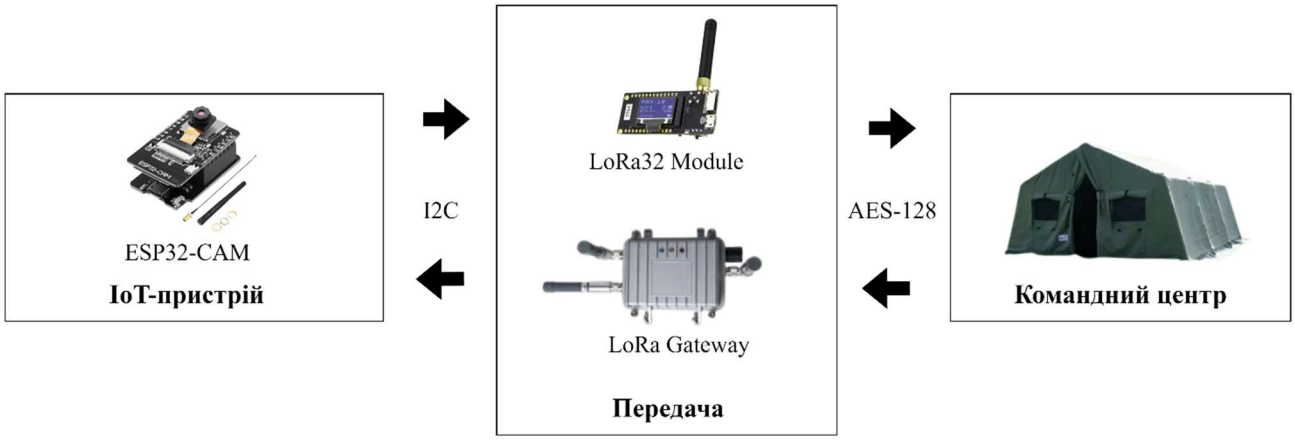


Рисунок 1.21 – Захист переданих даних у військових IoT-системах

Узагальнюючи специфіку технологій, можна зробити висновок, що у військових IoT-рішеннях не існує єдиного універсального протоколу зв’язку, здатного задовольнити всі вимоги одночасно, адже ефективність тієї чи іншої

технології залежить від конкретного сценарію її використання, зокрема відстані передачі даних, потреби в енергоефективності, стійкості до завад, здатності до адаптації в умовах пошкодженої інфраструктури, а також рівня бажаної конфіденційності. У випадку передачі інтенсивного трафіку на короткі відстані, наприклад, при передачі зображень, відео або телеметрії з дронів або інших тактичних платформ, найбільш доцільним буде використання Wi-Fi із належним захистом і шифруванням, особливо якщо такі передачі здійснюються через базові станції або супутникові канали, зокрема через Starlink. Натомість, у випадках, коли необхідно організувати моніторинг великих територій при мінімальному енергоспоживанні і відносній захищеності від перешкод, більш прийнятною є технологія LoRa або LoRaWAN, яка дозволяє здійснювати передачу даних на великі відстані з низькою швидкістю, але високою стабільністю. Що ж до адаптивних, стійких до збоїв мереж, то технології типу mesh, побудовані на базі Zigbee, Thread чи подібних протоколів, дають змогу створювати гнучкі комунікаційні структури, які автоматично переналаштовуються у разі пошкодження інфраструктури та можуть забезпечити безперервність передачі даних навіть за умов втрати окремих вузлів (див. табл. 1.3) [11].

Таблиця 1.3 – Порівняння основних характеристик технологій зв’язку

Параметр	**Wi-Fi**	**LoRa**	**Mesh (на основі Zigbee/ESP-NOW)**
Дальність передачі	до 100 м	до 15 км (відкрите поле)	100–500 м (між вузлами)
Енергоспоживання	Високе	Дуже низьке	Низьке-середнє
Пропускна здатність	До 1 Гбіт/с	До 50 кбіт/с	~100–500 кбіт/с
Стійкість до перешкод	Низька	Висока	Висока

Продовження таблиці 1.3 – Порівняння основних характеристик технологій зв’язку

Параметр	**Wi-Fi**	**LoRa**	**Mesh (на основі Zigbee/ESP-NOW)**
Надійність у бою	Помірна	Висока (одноразові пакети)	Висока (при правильному розгортанні)
Затримка сигналу	Мінімальна	Висока	Помірна
Захищеність передачі	Висока (з WPA3)	Середня (AES-128)	Середня–висока (з шифруванням)

РОЗДІЛ 2 АНАЛІЗ АРХІТЕКТУР ТА СЦЕНАРІЇВ ЗАСТОСУВАННЯ ІОТ-СИСТЕМ

2.1 Архітектура IoT-системи для військових задач

Побудова архітектури IoT-систем для військових задач формується не лише на основі загальних технічних вимог, а й значною мірою зумовлена суворими обмеженнями та викликами, притаманними бойовим умовам. Архітектура таких систем не є стандартизованою чи однозначною, а навпаки — гнучко адаптується до різних сценаріїв застосування, що залежать від:

— специфіки завдань;

— середовища використання;

— рівня доступності інфраструктури;

— очікуваної автономності.

У військовому середовищі застосовуються переважно гібридні рішення, де поєднуються кілька технологій і протоколів, що уможливлює ефективне функціонування систем в умовах порушення зв’язку, втрати живлення, або фізичного ураження окремих елементів, що обумовлює формування певного умовного базового шаблону архітектури, на який можуть спиратись інженери, адаптуючи його до конкретних бойових задач і оперативних потреб. Такий шаблон не є фіксованим і не може повністю відповідати всім можливим сценаріям, однак на його основі легко формувати різні модифікації систем, ураховуючи потребу в модульності, масштабованості, децентралізації та адаптації до динамічної тактичної ситуації [12-13].

Загальні принципи побудови військових IoT-систем. У бойовому контексті архітектура IoT-систем завжди має враховувати ймовірність:

— втрати каналів зв’язку;

— часткову або повну недоступність електроживлення;

— складність фізичного доступу до окремих вузлів;

— високу вірогідність ураження технічних засобів противником.

Усі ці фактори автоматично виключають можливість використання класичних централізованих архітектур, характерних для цивільних рішень, де вузли слугують лише датчиками чи виконавцями, передаючи всі дані на центральний сервер. У військових умовах кожен вузол має виконувати функції не лише збору, але й автономної обробки, зберігання та, за необхідності, ретрансляції інформації. Такий підхід забезпечує живучість системи у разі втрати комунікації з іншими вузлами або центральними модулями, а також дозволяє реалізувати більш адаптивну реакцію на зміну умов, зокрема шляхом самоконфігурації або автоматичного перерозподілу функцій між елементами мережі. Модульність виступає основою такої архітектури, де кожен блок системи — окремий функціональний модуль із чітко визначеним завданням, але здатний діяти незалежно або в складі групи вузлів, формуючи тимчасову або постійну мережеву структуру з підтримкою як синхронної, так і асинхронної взаємодії [12].

У рамках таких архітектур критичною залишається здатність систем працювати у децентралізованому режимі, коли відсутність зв’язку з центральним вузлом не призводить до повної втрати функціональності. Кожен окремий пристрій у системі має не лише мінімальне енергоспоживання і базову здатність до обчислень, а й потенціал для виконання завдань локального прийняття рішень, що особливо важливо для умов, де ризик блокування або глушіння сигналів високий, а час на прийняття рішень обмежений. У таких випадках ефективність IoT-системи вимірюється не лише її пропускною здатністю чи точністю вимірів, а й здатністю зберігати функціональність навіть при частковому порушенні мережі, що й зумовлює необхідність використання технологій побудови мереж з ознаками самовідновлення, самоорганізації та динамічного перепланування маршрутів передачі даних [12].

Унаслідок цього зростає значення мережевих топологій, що не базуються на жорсткій ієрархії, натомість використовують принципи рівноправної взаємодії між вузлами з можливістю тимчасового або постійного делегування функцій обробки

даних та прийняття рішень. Такий підхід дозволяє будувати стійкі до втрат системи, в яких знищення окремих вузлів не призводить до критичної деградації всієї архітектури. У поєднанні з використанням надійних методів шифрування, контролю доступу, автентифікації та мінімізації радіовипромінювання це дозволяє сформувати високозахищене середовище передачі інформації навіть у надзвичайно агресивних умовах. У результаті архітектура IoT-систем для військових задач має розглядатися як багаторівнева, гнучка і динамічна структура, здатна до адаптації в реальному часі з урахуванням як технічних параметрів, так і оперативної обстановки [12].

Структурні компоненти військової IoT-системи. Архітектура військової IoT-системи базується на сукупності спеціалізованих структурних компонентів, які повинні функціонувати автономно, стійко до зовнішніх впливів і бути адаптованими до надзвичайно складних умов. Основою кожного вузла такої системи є кілька функціональних блоків, що забезпечують сенсорну, обчислювальну, комунікаційну, енергетичну та захисну функціональність. Центральним елементом є блок збору даних, який реалізується у вигляді набору сенсорів, здатних працювати в екстремальних умовах — від температурних сенсорів і датчиків руху до магнітометрів, тискомірів і модулів GPS — причому всі вони мають вирізнятися низьким енергоспоживанням і широким температурним діапазоном роботи, що критично важливо в бойових умовах. Зібрана інформація надходить до обчислювального блоку, який представлений мікроконтролерами типу ESP32, STM32, RISC-V, здатними самостійно виконувати базову обробку даних, аналізувати ситуацію, виявляти аномалії, генерувати сигнали тривоги, виконувати шифрування та мінімізувати обсяг переданої інформації шляхом попередньої фільтрації [12-13].

У військових умовах централізовані обчислювальні моделі зазнають суттєвих обмежень, тому більшість рішень проєктується на основі децентралізованої обробки даних, де вузли виконують логіку автономно. Для забезпечення зв’язку між елементами використовується комунікаційний модуль, до складу якого входять безпровідні інтерфейси на основі LoRa, LoRaWAN, NB-IoT,

Zigbee або вузькосмугового радіозв’язку, що дозволяє мінімізувати ймовірність виявлення. Значну роль відіграє підтримка peer-to-peer взаємодії, а також маршрутизація даних у межмережевих (mesh) топологіях, що забезпечують стійкість до знищення окремих вузлів і дозволяють даним передаватися через кілька проміжних точок. Структура системи також передбачає енергетичний блок, який базується на використанні автономних джерел живлення з можливістю підзарядки від сонячних панелей і реалізацією енергозбереження через використання режимів сну та інші методи оптимізації споживання енергії. У випадках відсутності стабільного живлення така автономність дозволяє зберігати функціональність вузлів без зовнішньої інфраструктури [12].

Особливої уваги потребує блок захисту, що має включати як фізичну оболонку, стійку до вологи, пилу та механічних пошкоджень, так і засоби інформаційної безпеки. У корпусах реалізується відповідність стандартам IP65 або IP68, а внутрішні протоколи забезпечують автентифікацію, шифрування, верифікацію даних, захист від повторного відтворення пакетів (replay attack), що дозволяє зберігати безпечність комунікацій навіть у разі перехоплення сигналу (див. рис. 2.1).

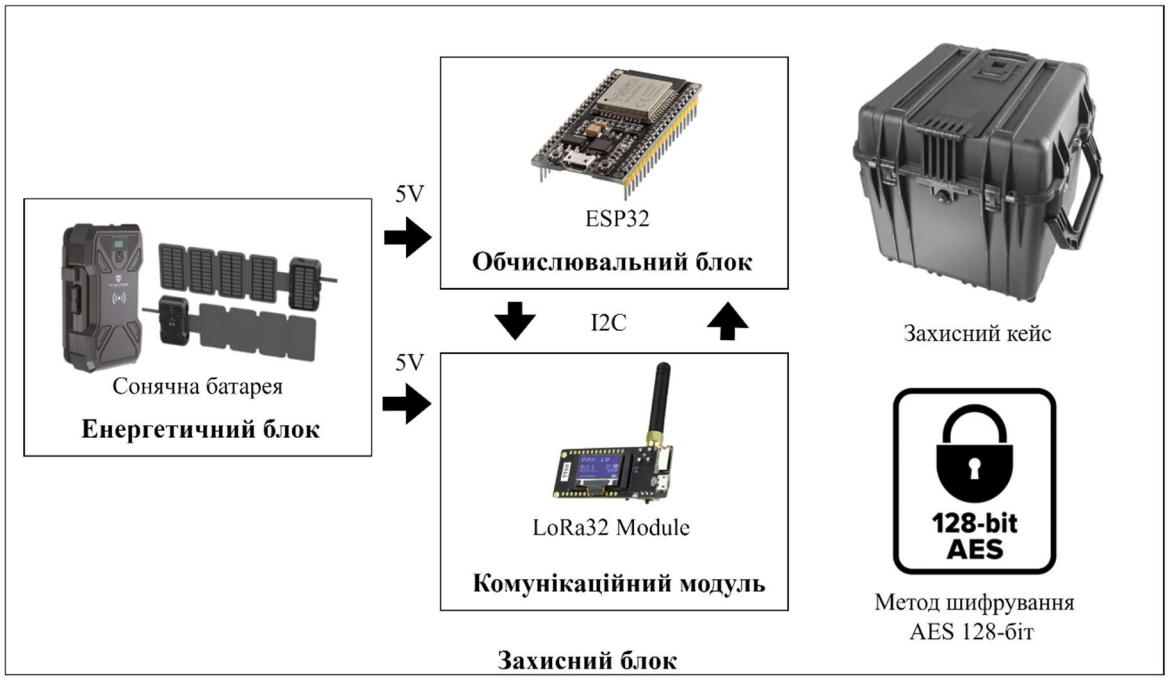


Рисунок 2.1 – Типова структура військової IoT-системи

Така компонентна структура відкриває шлях до побудови гнучких, модульних IoT-рішень для військових цілей, що можуть адаптуватися під конкретні задачі, швидко оновлюватися та відновлюватися навіть після часткових втрат або в разі втручання противника [12].

Децентралізація та взаємодія в умовах обмеженого зв'язку. Коли архітектура будується з урахуванням обмеженого або нестабільного зв'язку, зникає можливість постійної прив'язки до центрального сервера чи хмарної платформи, як це зазвичай відбувається у цивільних IoT-рішеннях. У таких умовах критично необхідною стає повна децентралізація функцій і здатність кожного вузла працювати самостійно, включно з обробкою, збереженням та прийняттям рішень. На практиці реалізація таких вузлів здійснюється за допомогою одноплатних комп'ютерів — Raspberry Pi, Orange Pi, NVIDIA Jetson, Arduino або подібних платформ, які поєднують у собі доступну обчислювальну потужність та можливість інтеграції з іншими модулями. Однією з найдоцільніших концепцій у цьому контексті стає архітектура DTN (Delay-Tolerant Network), у якій вузли здатні накопичувати дані локально і передавати їх далі тільки тоді, коли з'являється стабільний зв'язок із іншим вузлом чи релейною станцією. Такий підхід забезпечує життєздатність системи навіть у випадках повного глушіння або втрати каналу зв'язку, що особливо актуально в зонах бойових дій, де традиційні мережеві підходи виявляються неефективними або взагалі недієздатними [13].

Завдяки моделі, де кожен вузол не залежить від одного центра обробки чи зберігання, забезпечується повна стійкість до втрати окремих компонентів. Вузли взаємодіють між собою в сітчастій мережі, що дозволяє автоматично змінювати маршрути даних залежно від ситуації на полі бою, не потребуючи переналаштування всієї системи. У разі втрати окремого елементу інший вузол може швидко перебрати його функції за допомогою резервних конфігурацій, що дозволяє уникнути потреби у повному розгортанні мережі з нуля. Така гнучкість, самовідновлюваність і здатність до адаптації визначають ефективність військової IoT-системи в умовах реальної загрози, мінімізації людського втручання та високих ризиків (див. рис. 2.2).

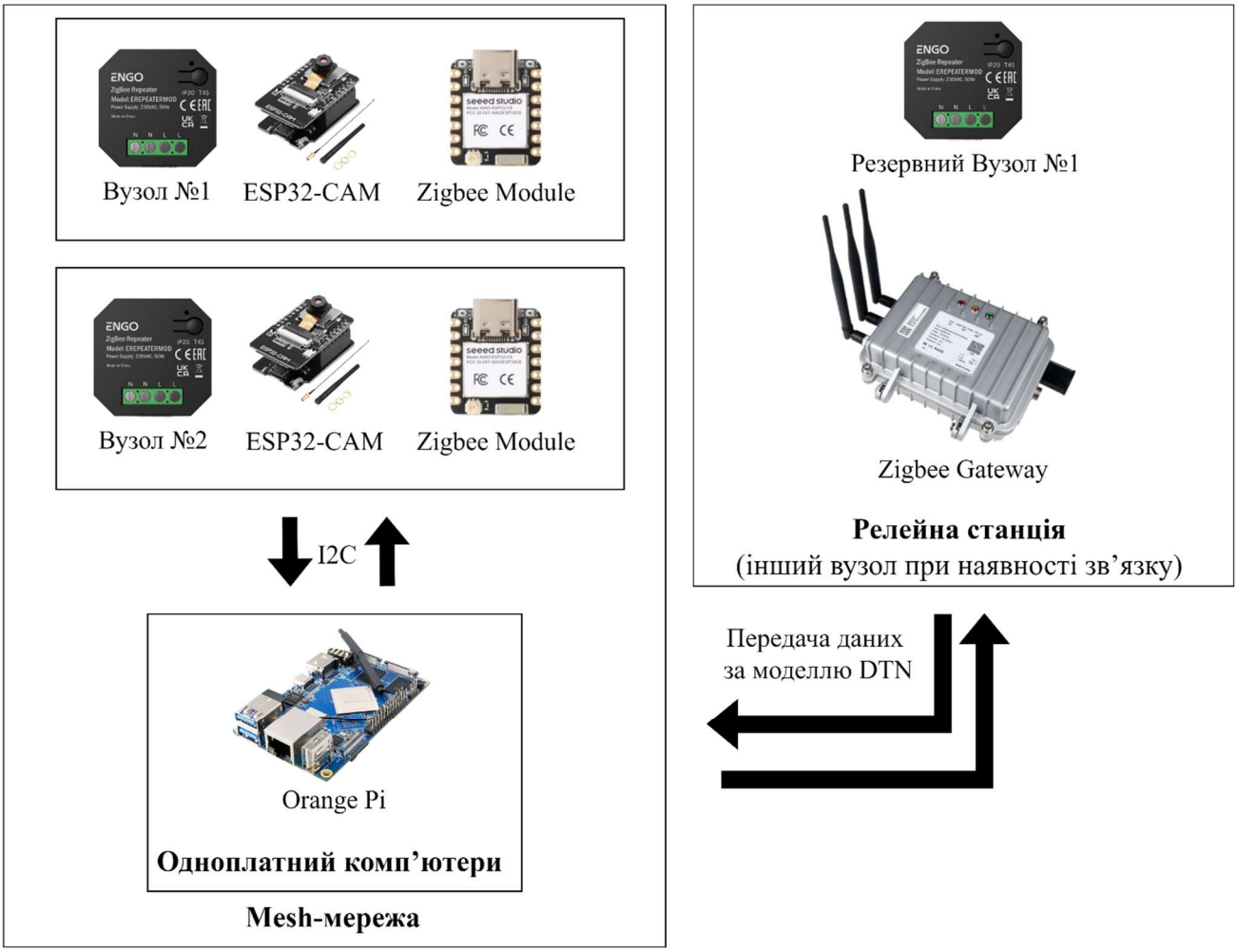


Рисунок 2.2 – Децентралізована архітектура в умовах обмеженого зв'язку

У результаті побудова децентралізованих IoT-архітектур з підтримкою DTN, peer-to-peer і mesh-моделей дозволяє створювати високостійкі інформаційні мережі, здатні функціонувати навіть у найбільш ворожих середовищах, залишаючись максимально ефективними у виконанні завдань.

Узагальнена модульна архітектура IoT-системи. На основі розглянутих принципів, що реалізуються у військових умовах з урахуванням потреби в автономності, захищеності, енергоефективності й децентралізації, можливо побудувати узагальнену модульну архітектуру IoT-системи для військових задач, яка поєднує в собі:

— гнучкість застосування;

— стійкість до зовнішніх впливів;

— здатність адаптуватися до широкого спектра сценаріїв бойового використання.

Така архітектура, орієнтована на гібридні підходи, дозволяє розгортати системи в умовах нестабільного або повністю відсутнього інфраструктурного середовища, забезпечуючи при цьому ефективний збір, обробку, зберігання та передачу даних. У своїй основі архітектура включає сенсорні вузли — так звані "sensor nodes", які є автономними пристроями з низьким енергоспоживанням та базовою логікою обробки, що здатні розгортатися у великій кількості, утворюючи сенсорні мережі, призначені для фіксації активності, змін в оточенні, проникнень, вібрацій, температурних коливань або інших параметрів, залежно від типу місії. Такі вузли не потребують постійного зв’язку, можуть працювати в режимах періодичної активності та передавати лише релевантні дані до вищих рівнів архітектури.

Передача даних і формування мережевої структури забезпечується маршрутизуючими вузлами — "relay nodes", які мають підвищену обчислювальну потужність порівняно з сенсорними елементами, здатні тимчасово зберігати інформацію, виконувати попередню обробку, шифрування або маршрутизацію даних до наступного вузла. Розміщення таких вузлів дозволяє реалізовувати сітчасті структури типу mesh, які забезпечують самовідновлення маршрутів у разі втрати окремих елементів. Дані, зібрані з різних джерел, передаються до тактичного центру або мобільного серверного вузла — Tactical Gateway або Edge Server, що уособлює більш потужний обчислювальний елемент системи, здатний виконувати глибший аналіз, агрегацію, зберігання та подальше поширення інформації. Такий вузол може бути реалізований у вигляді захищеного ноутбука, мобільного командного пункту або переносного сервера з супутниковим чи високочастотним каналом зв’язку для інтеграції з ширшими мережевими структурами або центрами прийняття рішень. Він також відповідає за синхронізацію окремих фрагментів IoT-мережі, формування загальної ситуаційної картини та забезпечення віддаленого керування окремими елементами [12-13].

Ключовим аспектом архітектури є модульність, що означає можливість адаптації кожного вузла до конкретної місії шляхом варіативної комплектації.

Наприклад, в одному випадку достатньо сенсорного вузла з базовим безпровідним передавачем, тоді як в іншому — необхідне розгортання вузла з додатковими модулями шифрування, розпізнавання, інерційної навігації, збереження даних на накопичувачах чи захисту від фізичного втручання. Гнучкість архітектури дозволяє швидко масштабувати систему як у горизонтальному (збільшення кількості вузлів), так і вертикальному (посилення функціональності окремих елементів) напрямках, що особливо критично в польових умовах, де оперативність розгортання напряму впливає на ефективність операцій. У цьому контексті важливо враховувати, що завдяки використанню mesh-архітектур, наприклад на основі Zigbee, Thread, LoRa Mesh, можлива реалізація мереж, які самостійно адаптуються до змін у структурі, автоматично переналаштовують маршрути й залишаються працездатними навіть у разі виходу з ладу частини елементів. Розгортання таких мереж може здійснюватися за допомогою мобільних підрозділів, безпілотних літальних апаратів, або розміщення попередньо запрограмованих пристроїв у критичних точках простору (див. рис. 2.3) [12-13].

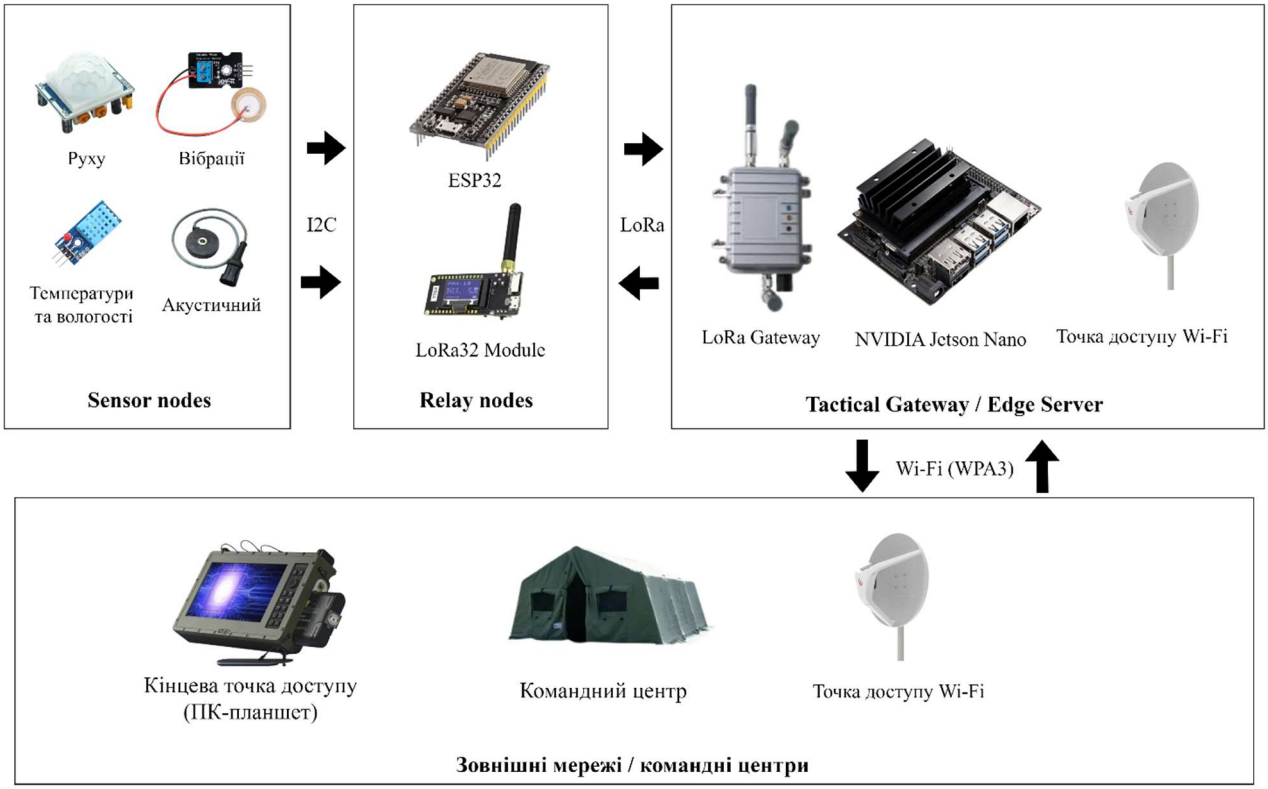


Рисунок 2.3 – Узагальнена модульна архітектура IoT-рішення

У підсумку, модульна IoT-архітектура військового призначення, побудована на принципах децентралізації, енергоефективності, захищеності й адаптивності, дає змогу створювати системи, які не тільки відповідають вимогам до надійності та автономності в бойових умовах, але й забезпечують довготривалу життєздатність у змінному середовищі. Відмова від централізованих моделей на користь децентралізованих рішень, які оперують без постійного зв'язку із сервером, дозволяє мінімізувати вразливість до атак, забезпечити автономну обробку даних та збільшити стійкість системи до зовнішнього впливу. Кожен елемент архітектури функціонує як частина більшої структури, але з повною здатністю до виконання завдань навіть у відриві від мережі (див. рис. 2.4).

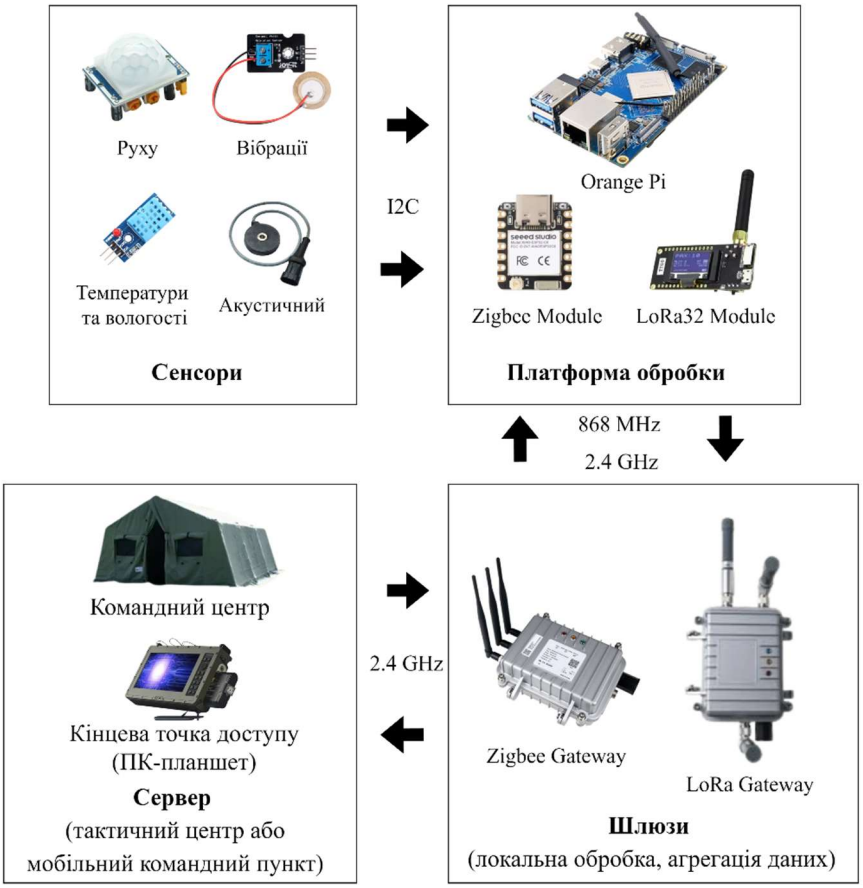


Рисунок 2.4 – Взаємодія між сенсорами, шлюзами та сервером

У підсумку така система може підтримувати критично важливі функції — від моніторингу переміщень, виявлення небезпек, до тактичного планування — на основі об'єднаних даних з різнорідних сенсорів, включаючи візуальні, акустичні,

температурні, радіочастотні, магнітні та інші типи, що робить архітектуру не лише функціонально повною, а й стратегічно гнучкою та надзвичайно стійкою в умовах бойових дій.

2.2 Сценарії використання та варіанти побудови

Окрім реалізації архітектури IoT-системи для військових потреб, важливо усвідомлювати, що така система повинна мати чіткі сценарії використання, у яких вона здатна ефективно функціонувати, тобто її проєктування не обмежується лише структурою — необхідно також окреслити ті умови та випадки, де ця система реально застосовується, зокрема варіанти її практичного впровадження на різних рівнях бойового управління, в умовах динамічно змінюваної тактичної ситуації. На основі побудованої модульної архітектури створюються конкретні рішення, які адаптуються до потреб військових операцій, і ці рішення формуються відповідно до контексту бойового завдання, що дозволяє проєктувати гнучкі та масштабовані застосування IoT, які ефективно інтегруються в існуючі системи [14]:

— командування;
— розвідки;
— безпеки;
— логістики.

Сценарії використання IoT у військових умовах. У військовому контексті Інтернет речей розглядається як сукупність взаємопов’язаних технологій, здатних у реальному часі збирати, передавати та обробляти дані в умовах обмежених ресурсів, високих ризиків та швидкоплинних подій. Одним із найтиповіших сценаріїв такого використання є моніторинг навколишнього середовища, де сенсорні вузли оснащуються відповідними сенсорами — температури, вологості, акустики, газу або радіації — для виявлення змін, які можуть свідчити про небезпеку для особового складу або сигналізувати про підхід супротивника. Такі

мережі можуть бути встановлені поблизу потенційно загрозливих ділянок, в тилу або безпосередньо в зоні бойових дій, і працювати автономно протягом тривалого часу (див. рис. 2.5).

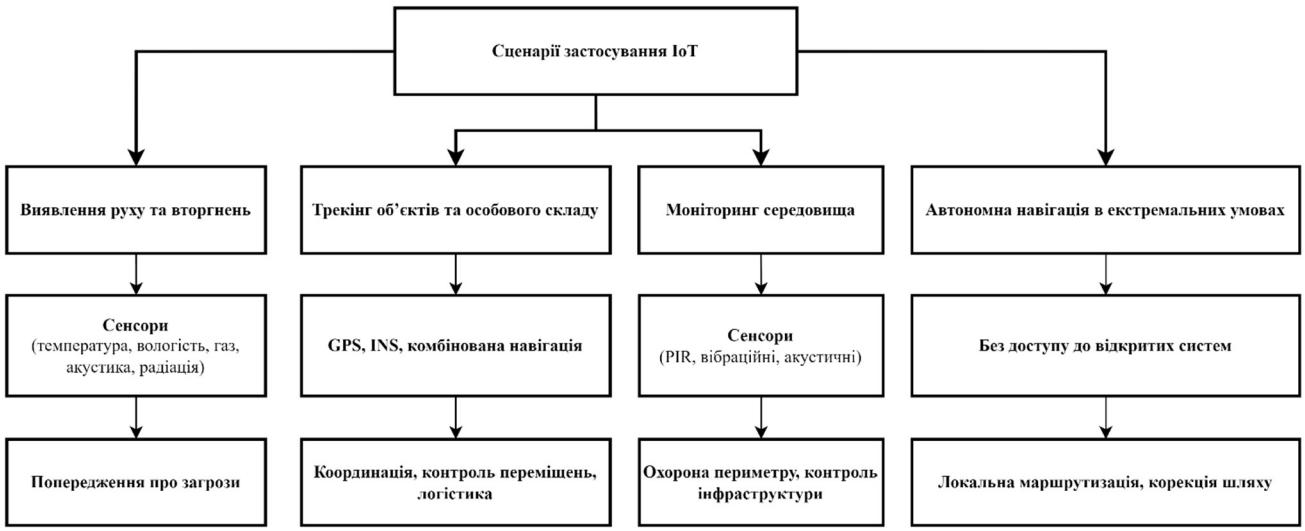


Рисунок 2.5 – Сценарії застосування IoT у зоні бойових дій

Ще одним критично важливим сценарієм є трекінг об'єктів і особового складу — на основі GPS-модулів, інерційних навігаційних систем або комбінованих методів геопозиціонування можна інтегрувати IoT-вузли у спорядження військовослужбовців або військову техніку для фіксації місцезнаходження, маршруту переміщення, а також для координації логістики. Такий підхід забезпечує постійний контроль за мобільними підрозділами, дає змогу реагувати у випадку втрати зв'язку з окремим солдатом чи одиницею техніки, забезпечує ефективне управління пересуванням у складній місцевості або в ситуаціях, де швидкість і точність мають критичне значення.

Окремий сценарій стосується виявлення руху та вторгнень, що реалізується завдяки встановленню сенсорних мереж з PIR-датчиками, акустичними сенсорами або сенсорами вібрації, які здатні виявляти наближення або переміщення сторонніх об'єктів. Подібна система використовується для організації охорони периметру, контролю тимчасових опорних пунктів, охорони інфраструктури або обладнання, розміщеного у зоні підвищеної небезпеки. У поєднанні з візуальними або

тепловізійними сенсорами, такі рішення можуть працювати навіть у нічний час або в умовах обмеженої видимості.

Ще один важливий сценарій — навігаційна підтримка в умовах порушеної інфраструктури або відсутності доступу до загальнодоступних навігаційних систем, коли групи можуть орієнтуватися за допомогою власних IoT-вузлів, які не використовують відкриті канали зв'язку і не можуть бути заблоковані або перехоплені противником. У подібних випадках забезпечується автономність навігації, а також можливість корекції маршруту в реальному часі без потреби в централізованих запитах чи зовнішньому втручанні.

Усі вказані сценарії об'єднує необхідність у високому рівні автономності, стійкості до втрати зв'язку, здатності працювати в умовах активного застосування засобів радіоелектронної боротьби, мінімального споживання енергії та гнучкості розгортання навіть у складних польових умовах. Саме на цих вимогах базується необхідність створення модульних IoT-рішень, які не залежать від централізованої інфраструктури та можуть бути адаптовані для різних завдань — від моніторингу навколишнього середовища до комплексної координації операцій у зоні бойових дій.

Варіанти побудови IoT-систем. Побудова IoT-систем для військових потреб тісно пов'язана з конкретними сценаріями їхнього застосування, оскільки саме реальні приклади використання визначають вимоги до архітектури та функціональності таких рішень. Різноманіття задач, які виникають у межах військових місій, формує потребу в адаптивності IoT-системи до різних умов і обмежень, що, у свою чергу, вимагає розробки кількох підходів до її побудови. Варіанти реалізації можуть суттєво відрізнятися в залежності від:

— розміру операцій;
— наявної інфраструктури;
— вимог до мобільності;
— джерел живлення;
— характеру середовища.

Так, одним із можливих варіантів побудови є стаціонарна архітектура, що розгортається в межах постійних або тимчасових баз, командних пунктів чи об’єктів довготривалого перебування. У таких випадках існує можливість розміщення потужніших сенсорних вузлів, забезпечення підключення до локальних мереж живлення, а також встановлення підсилювачів сигналу для покращення комунікації між компонентами системи. Подібна конфігурація дозволяє розмістити велику кількість сенсорів, виконувати локальну обробку даних та здійснювати централізовану аналітику, що особливо важливо для організації керування великими підрозділами або забезпечення захищеного зберігання даних.

Інший варіант пов’язаний із використанням мобільних вузлів, які можуть бути вбудовані безпосередньо в спорядження особового складу, бойову техніку або інші рухомі об’єкти. Такі рішення відрізняються більшою гнучкістю, проте потребують особливої уваги до енергоефективності, компактності та здатності до самоконфігурування у русі. В умовах постійного переміщення, обмеженого доступу до джерел живлення та необхідності уникати зайвого виявлення, мобільні вузли повинні працювати автономно та з мінімальними витратами енергії. Такі системи також мають підтримувати адаптивну маршрутизацію даних для уникнення втрати зв’язку при зміні просторового розташування вузлів.

Третій можливий варіант – гібридна архітектура, яка поєднує як стаціонарні вузли, що формують опорну мережу та забезпечують зв’язок із командним центром, так і мобільні елементи, які збирають дані на місцях та передають їх до стаціонарних точок через проміжні ретранслятори. Така структура дозволяє балансувати між охопленням великої території, стабільністю мережі, гнучкістю реагування та стійкістю до ворожих впливів (див. рис. 2.6).



Рисунок 2.6 – Варіанти побудови мережі з урахуванням обмежень

Кожен з описаних варіантів обов’язково повинен враховувати можливість автономного живлення, здатність до самовідновлення при втраті вузлів і надійність у ситуаціях, де можливі перебої через фізичні або кіберзагрози, адже в умовах бойових дій системи можуть опинитися під безпосереднім впливом ворожих атак, або ж просто втратити частину функціоналу через знищення окремих вузлів чи втрату енергозабезпечення.

Обмеження середовища застосування. На відміну від цивільного середовища, військове застосування накладає низку додаткових обмежень, які значною мірою формують специфіку архітектурних і технологічних рішень. Однією з найсуттєвіших проблем є повна або часткова відсутність інфраструктури, зокрема систем енергопостачання, фіксованих мереж зв’язку та центрів обробки даних, що змушує проєктувати IoT-системи як повністю автономні рішення, які повинні мати власні механізми комунікації, накопичення і обробки даних, з можливістю функціонувати у відриві від глобальних чи публічних мереж. Така автономність особливо важлива в умовах активної фази бойових дій, де будь-яка зовнішня залежність може бути використана ворогом для виявлення або знищення системи (див. рис. 2.7).

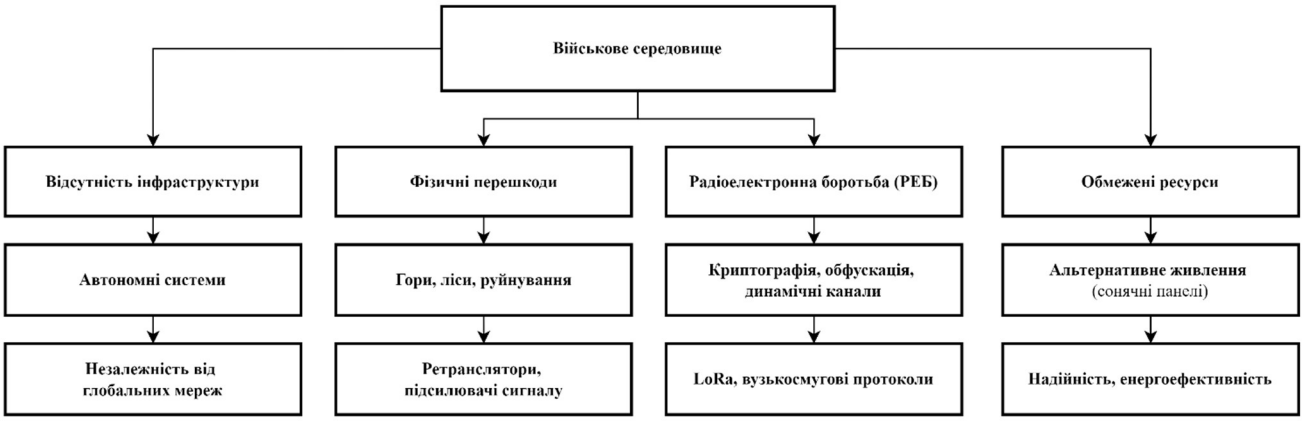


Рисунок 2.7 – Вплив середовища на вибір технології зв’язку

Додатково до цього існують фізичні перешкоди, як-от гористий рельєф, густі ліси, зруйновані міські квартали чи несприятливі погодні умови, які ускладнюють поширення сигналу, потребуючи впровадження підсилювачів або використання

самовідновлюваних мереж із ретрансляторами, які формують маршрути передачі динамічно залежно від умов. Ретранслятори також повинні мати окреме джерело живлення, бути енергоефективними та надійними, оскільки від їхньої роботи залежить цілісність мережі.

Крім того, серйозною загрозою виступає перехоплення та глушіння сигналів із боку засобів радіоелектронної боротьби противника, що вимагає реалізації спеціальних механізмів криптографічного захисту, обфускації даних, динамічного перестроювання каналів зв’язку, а також використання вузькосмугових протоколів типу LoRa, які дозволяють уникати виявлення та забезпечують передачу навіть у складних умовах. У цьому контексті важливо забезпечити також низьке енергоспоживання, особливо в режимі очікування, і можливість перемикання вузлів у більш енергозберігаючі стани, що дозволяє підтримувати роботу системи тривалий час без зовнішнього втручання.

Значну роль відіграє і обмеженість ресурсів, пов’язана з ускладненою логістикою або неможливістю обслуговування системи в бойових умовах, тому компоненти повинні бути максимально надійними, мати тривалий термін роботи на одному заряді або бути здатними заряджатися від альтернативних джерел енергії, таких як сонячні панелі. Всі описані обмеження прямо впливають на вибір конкретних протоколів, типів сенсорів, методів комунікації та способів обробки даних, що вимагає глибокого аналізу кожного з факторів на етапі проєктування системи, з урахуванням того, що навіть найменша помилка у виборі компонентів або технологій може призвести до критичних наслідків у реальному бойовому застосуванні.

Вимоги до мережевої топології залежно від сценарію. У контексті побудови IoT-систем для військових завдань одним із визначальних факторів є вимоги до мережевої топології, що залежать безпосередньо від сценарію використання та типу системи, яка розгортається. Мережева топологія визначає, наскільки ефективно відбувається передача даних, як надійно вузли взаємодіють між собою, а також чи здатна система адаптуватися до змін у навколишньому середовищі чи втрати окремих елементів. Саме завдання, яке стоїть перед системою, її

функціональне навантаження, кількість вузлів, їх мобільність або фіксованість, географічне розташування та рівень загроз — усе це прямо впливає на вибір топології, що буде використовуватись при її побудові.

У випадках, коли система базується на стаціонарному рішенні, доцільно використовується топологія типу «зірка», де існує один центральний вузол, який приймає дані від усіх інших. Така структура спрощує обробку інформації та централізоване управління, проте має серйозний недолік — уразливість до втрати центрального вузла, що автоматично призводить до втрати всієї системи, або її значного часткового функціоналу. У контексті мобільних або гібридних рішень актуальнішою стає mesh-топологія, в якій кожен вузол має змогу не лише передавати власні дані, але й ретранслювати пакети інших, забезпечуючи гнучке і надійне функціонування всієї мережі навіть у разі виходу з ладу окремих елементів. Завдяки цьому досягається властивість самовідновлення, що надзвичайно важливо в умовах бойових дій, коли частини мережі можуть бути знищені, відключені чи заглушені. Mesh-топологія також дозволяє зменшити залежність від конкретних точок відмови та розширює можливості маршрутизації, оскільки маршрути не є жорстко зафіксованими [14].

Ще одним підходом є peer-to-peer-топологія, яка передбачає обмін даними між вузлами без визначеного центру, де кожен елемент мережі функціонує на рівних правах з іншими. Такий підхід забезпечує високий рівень децентралізації та стійкість до атак або фізичних впливів, але ускладнює побудову загальної структури управління та маршрутизації, оскільки вимагає складніших алгоритмів синхронізації, пошуку шляхів і балансування навантаження. Таке ускладнення часто виправдане в ситуаціях, де на перше місце виходить саме гнучкість і виживання системи, а не швидкість чи простота адміністрування [14].

На практиці рідко застосовується лише один тип топології, оскільки реальні умови завжди накладають власні обмеження, зокрема змінність конфігурацій, наявність або відсутність джерел живлення, загроза перехоплення та перешкод, щільність розміщення вузлів, а також інші фактори. Тому часто реалізуються комбіновані рішення, де стаціонарні вузли можуть використовувати зіркоподібну

структуру для ефективного збору інформації та управління, тоді як периферійні або мобільні вузли між собою утворюють mesh або p2p-з’єднання, що дозволяє досягати гнучкої адаптації системи до динамічних змін на полі бою. Такий підхід забезпечує одночасно високу масштабованість, стійкість до зовнішніх впливів та здатність до функціонування навіть у частково зруйнованому або сильно зашумленому середовищі.

У підсумку, вимоги до мережевої топології тісно пов’язані з варіантами побудови IoT-систем та сценаріями їх застосування, адже саме архітектура взаємодії між вузлами визначає технічну життєздатність системи, її придатність до виконання конкретного завдання, та рівень безпеки, якого можна досягти в бойовому середовищі.

2.3 Алгоритми функціонування IoT-систем

Для реалізації сценаріїв функціонування IoT-системи важливим аспектом стає її алгоритмічна структура, яка забезпечує відповідність архітектури конкретним завданням і дозволяє досягати необхідного функціонального результату. Як і в будь-якій технічній системі, основа ефективної роботи полягає у впровадженні алгоритмів, що керують:

- логікою взаємодії елементів між собою;
- організацією процесів збору, обробки, передавання та зберігання даних.

Незважаючи на різноманітність конкретних реалізацій, більшість IoT-систем дотримуються схожих загальних принципів, адаптованих під умови середовища та тип задач, які ставляться перед мережею. У військовому контексті ці алгоритми набувають особливого значення через необхідність автономного функціонування, гнучкої адаптації до змін середовища, мінімізації енергоспоживання та підвищення

стійкості до втрати зв’язку з центральним контролером або іншими вузлами [15-16].

Основні етапи функціонування IoT-вузлів. Функціонування IoT-вузлів базується на модульному підході, що дозволяє формувати їх логіку з окремих етапів, серед яких основними є:

— збирання інформації сенсорами;

— первинна обробка та агрегація;

— локальне або проміжне зберігання;

— передача даних;

— подальше обслуговування вузла.

Спершу, на етапі збору даних, сенсори, що інтегровані в структуру вузла, здійснюють регулярні або подійно активовані вимірювання, які можуть залежати від заздалегідь заданих умов — наприклад, сенсори руху спрацьовують лише у відповідь на зміну інфрачервоного фону, що дозволяє суттєво скоротити споживання енергії та підвищити автономність у польових умовах. Далі, після фіксації події або набору значень, відбувається агрегація даних, яка може здійснюватися як безпосередньо на вузлі, так і на проміжному агрегуючому елементі, що дозволяє провести первинну фільтрацію, усереднення, виявлення аномалій або логічну інтерпретацію подій ще до того, як інформація буде передана далі по мережі (див. рис. 2.8).

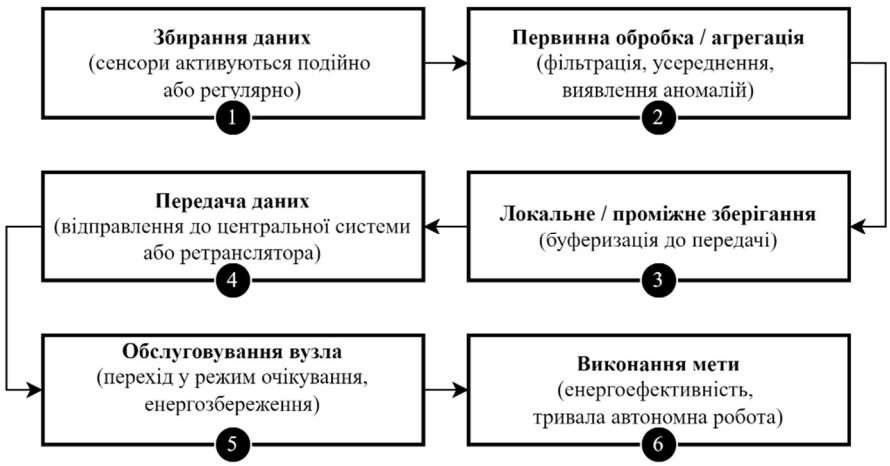


Рисунок 2.8 – Етапи функціонування типового IoT-вузла

Такий підхід не тільки розвантажує загальний трафік, а й дозволяє зменшити ризик перевантаження центрального вузла інформацією, що не має стратегічного значення [15].

Передача даних, як наступний етап алгоритму, реалізується за допомогою побудови гнучких маршрутів, що можуть динамічно змінюватися залежно від топології, наявності або відсутності сусідніх вузлів, рівня сигналу та загального стану мережі. У ситуаціях, коли вузол знаходиться на значній відстані від головного вузла або шлюзу, застосовується ретрансляція через інші елементи мережі, що дозволяє уникати сліпих зон і підтримувати стабільну взаємодію навіть у розподілених структурах. У мережах з динамічною маршрутизацією особливо важливим є врахування затримок і можливих втрат пакетів, тому вузли можуть здійснювати вибір оптимального шляху на основі метрик типу RSSI, часу затримки, або кількості проміжних хопів [15].

Завершальним етапом у логіці функціонування вузлів є оновлення та обслуговування, яке включає періодичну самодіагностику, оцінку поточного стану системи, включаючи рівень заряду батареї, внутрішню температуру, працездатність окремих модулів і наявність помилок у попередніх транзакціях. У разі виявлення аномалій або несприятливих умов вузол може автоматично переходити у сплячий режим, обмежувати активність, відключати другорядні компоненти або перебудовувати логіку взаємодії з іншими елементами системи, що особливо критично в умовах обмеженого доступу до джерел живлення або високого ризику ураження.

Узгоджене функціонування всіх цих етапів забезпечує стабільність системи у відсутність централізованого керування, дозволяє їй зберігати працездатність у режимі автономної дії, адаптуватися до зовнішніх умов та зберігати здатність до виконання поставлених завдань, навіть якщо частина її елементів вийшла з ладу або тимчасово втратила зв’язок із загальною інфраструктурою. Така структура алгоритмів дозволяє забезпечити стратегічну надійність IoT-рішень у бойових сценаріях, де централізована координація не завжди можлива або доцільна [15].

Оптимізація енергоспоживання. Однією з головних задач при створенні алгоритмів функціонування для військових IoT-систем стає мінімізація енергоспоживання, оскільки технічне обслуговування вузлів у польових умовах або є надзвичайно ускладненим, або взагалі неможливим, що вимагає реалізації ефективних підходів до збереження енергії на рівні програмної логіки. Серед таких підходів особливе місце займає застосування режимів глибокого сну, у яких вузол більшість часу перебуває в енергозберігаючому стані та активується лише за наявності певного тригера, наприклад, сигналу від сенсора або запиту від іншого вузла. Така поведінка дозволяє зменшити загальну активність радіомодуля та істотно скоротити витрати живлення. Додатково, алгоритм може включати зниження частоти передачі даних, що базується на логіці передачі лише у випадках, коли нові значення виходять за встановлені порогові межі, ігноруючи незначні коливання, які не мають стратегічного значення.

Іншим важливим підходом є реалізація енергоефективної маршрутизації, коли маршрути обираються з урахуванням мінімізації витрат енергії, зокрема, коли вузли з вищим зарядом батареї можуть брати на себе більшу кількість функцій, пов’язаних із ретрансляцією, тоді як вузли з низьким рівнем живлення зменшують свою активність. Підтримка обробки даних безпосередньо на вузлах також забезпечує істотне зниження енергоспоживання, оскільки замість надсилання сирих даних у мережу, проводиться локальна агрегація, фільтрація або виконання базових логічних операцій на кшталт "XOR" або "AND", що дозволяє скоротити тривалість увімкнення радіомодуля, одного з найбільш енерговитратних компонентів пристрою (див. рис. 2.9).

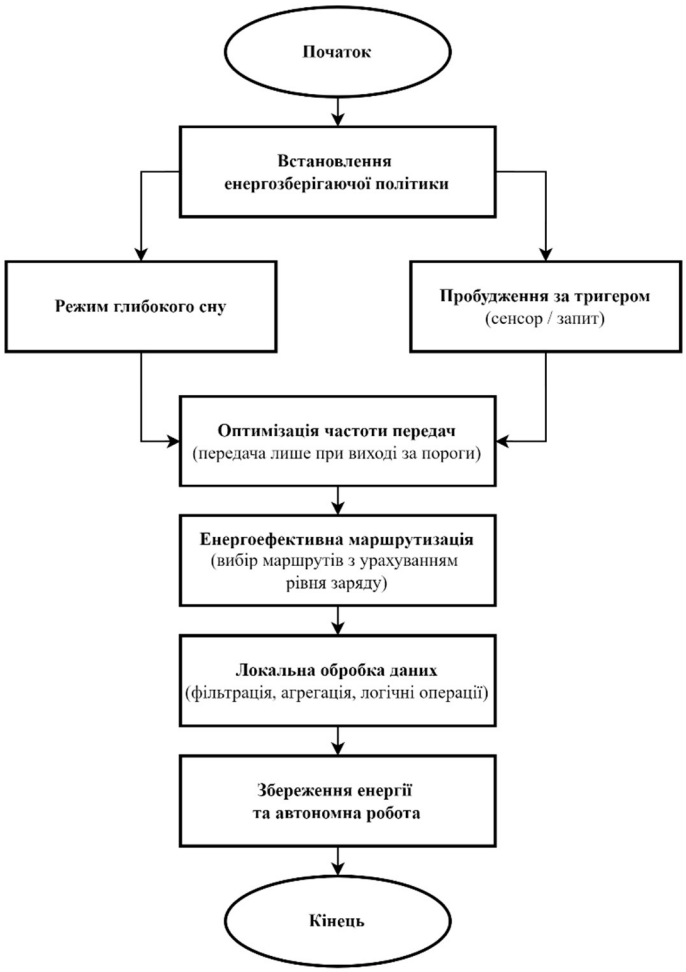


Рисунок 2.9 – Алгоритм зниження енергоспоживання у сенсорах

Завдяки поєднанню цих технік досягається суттєве подовження автономного функціонування IoT-вузлів, що особливо важливо в умовах обмеженого або нестабільного живлення, які характерні для військових операцій у складній місцевості або на територіях без інфраструктури.

Забезпечення стійкості до збоїв і втрати зв'язку. З урахуванням бойових умов особливої уваги вимагає забезпечення стійкості IoT-систем до збоїв і втрати зв'язку, що передбачає створення архітектури, здатної до самовідновлення, адаптації та підтримки функціональності навіть у випадках втрати окремих компонентів. Для цього реалізуються алгоритми, орієнтовані на підвищення стійкості до пошкоджень або перешкод. Зокрема, доцільно впроваджувати дублювання вузлів або критичних функцій, наприклад, функцій ретрансляції, що дозволяє компенсувати вихід з ладу окремих елементів без втрати загальної

працездатності мережі. Одним із основних рішень у цьому напрямку є застосування динамічної маршрутизації, коли мережа автоматично адаптується до змін, зокрема, якщо певний вузол стає недоступним, дані автоматично перенаправляються через альтернативні шляхи без необхідності втручання ззовні.

Особливу ефективність демонструє підхід "store-and-forward", у якому вузол може тимчасово зберігати дані у внутрішньому буфері, якщо поточна ситуація не дозволяє здійснити передачу, і відправляти їх пізніше при відновленні зв’язку, що є надзвичайно важливим у мобільних сітках, де порушення зв’язку є регулярним явищем. Додатково, впроваджується механізм контролю життєздатності вузлів через "Heartbeats" та "Watchdog", де вузли періодично перевіряють не лише власний стан, а й стан своїх сусідів, і в разі виявлення втрати зв’язку з одним із них активується алгоритм перебудови маршруту або ініціалізації резервного плану дій (див. рис. 2.10).

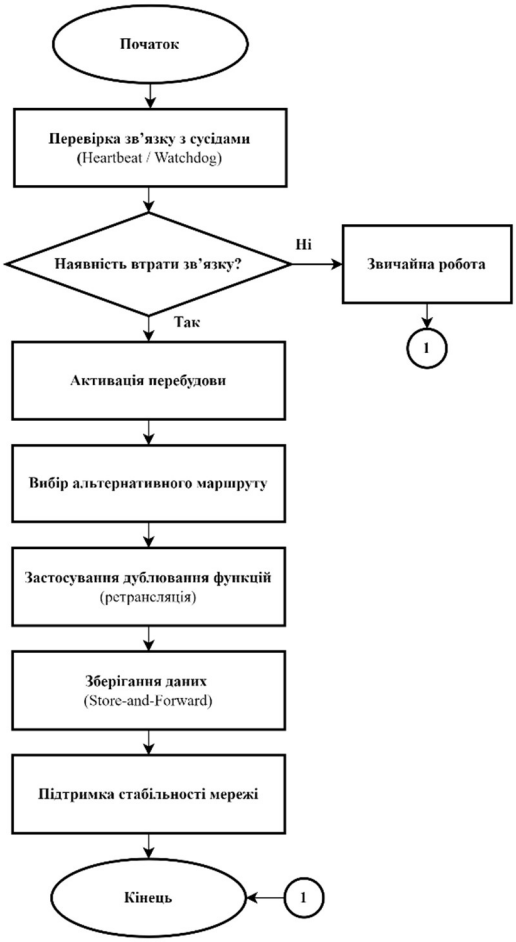


Рисунок 2.10 – Алгоритм реагування на втрату зв’язку

Завдяки такій структурі, система зберігає високу функціональну надійність навіть за умов сильного радіошуму, фізичних ушкоджень елементів мережі або повної втрати частини інфраструктури, що дозволяє зберігати цілісність комунікацій та логіки керування в реальному часі незалежно від зовнішніх обставин [15].

Протоколи безпечного обміну в IoT-системах. У процесі побудови військово-орієнтованих IoT-систем не менш важливою складовою, ніж енергоефективність чи стійкість до збоїв, є забезпечення безпечного обміну даними між вузлами, адже сам факт наявності інформаційного обміну в умовах бойових дій передбачає не лише надійність комунікації, а й захист переданої інформації від перехоплення, підміни або спуфінгу, що робить вибір відповідних протоколів безпечного обміну критично необхідним (див. рис. 2.11).

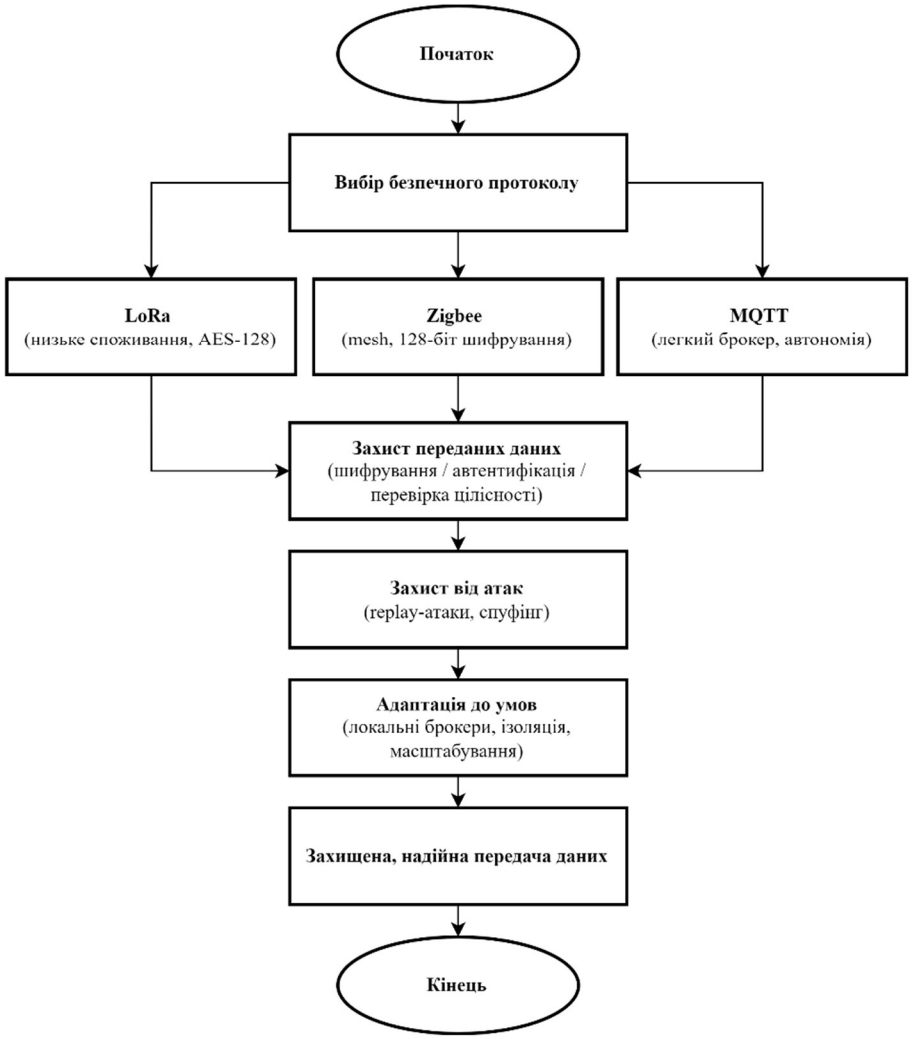


Рисунок 2.11 – Алгоритм безпечної передачі даних

Одним із найбільш придатних рішень для організації надійного зв’язку у середовищах з низьким енергоспоживанням і великою дальністю передачі є LoRa, який функціонує на субгігагерцових частотах, менш уразливих до заглушення, і вже на рівні базової архітектури містить вбудоване AES-128 шифрування, забезпечуючи необхідний рівень захисту інформації при мінімальних витратах енергії. LoRa підходить для створення децентралізованих мереж із низькою швидкістю передачі, що є характерним для багатьох військових сценаріїв, де важливі не обсяги трафіку, а стабільність і захищеність даних [16].

Іншим протоколом, що може бути ефективно використаний у подібному контексті, є Zigbee, орієнтований на роботу з великою кількістю близько розташованих вузлів, який реалізує mesh-архітектуру і також підтримує 128-бітне шифрування. Така структура дозволяє ефективно координувати взаємодію між елементами мережі навіть при втраті частини з них, хоча й поступається LoRa за максимальною дальністю дії, адже потребує розміщення більшої кількості ретрансляторів для підтримки стійкого з’єднання, проте саме це робить його придатним для використання в умовах компактно розташованих військових підрозділів або мобільних баз [16].

Особливий інтерес у рамках безпечного обміну даними становить MQTT — протокол публікації-підписки, що характеризується мінімальним навантаженням на мережу і дозволяє реалізовувати ефективний обмін повідомленнями між вузлами за участі посередника — брокера. В умовах обмеженого доступу до інфраструктури MQTT може працювати у зв’язці з локальними брокерами, розгорнутими на одноплатних комп’ютерах типу Raspberry Pi або навіть на мікроконтролерах ESP32, формуючи автономні підмережі з ізольованим або контрольованим доступом, зберігаючи при цьому функціональність і захищеність зв’язку. MQTT часто інтегрується з іншими мережевими протоколами, зокрема з тими ж Zigbee-шлюзами, що дозволяє побудувати багаторівневу інфраструктуру, яка одночасно відповідає вимогам енергозбереження та криптографічної безпеки [15-16].

Разом із вибором відповідного протоколу необхідно впроваджувати надійні механізми автентифікації вузлів, зокрема через попередньо встановлені ключі, сертифікати або інші способи перевірки справжності кожного учасника мережі, а також реалізовувати захист від атак типу «повторне відтворення повідомлень» (replay attacks), які можуть дезорганізувати роботу системи або надати ворогові доступ до критичних команд. Конкретна комбінація протоколів, засобів шифрування та способів автентифікації визначається з огляду на топологію мережі, передбачувану мобільність вузлів, рівень загроз, характерний для даного театру бойових дій, та інші чинники, що постійно змінюються в динаміці конфлікту. Такий підхід дозволяє створювати адаптивні, гібридні структури зв’язку, які можуть підтримувати безпечну взаємодію навіть за умов часткової ізоляції або порушення централізованої інфраструктури [16].

На відміну від розглянутих рішень, класичні протоколи типу Wi-Fi у контексті військових IoT-систем не є пріоритетними через вищу вразливість до виявлення, заглушення та атак на відкриті канали передачі, що знижує їхню ефективність як бази для побудови захищених мереж, натомість зростає значення технологій, здатних забезпечити повноцінну криптографічну стійкість та енергетичну ефективність у поєднанні з автономністю та масштабованістю, що й дозволяє розглядати LoRa, Zigbee та MQTT як основні кандидати для реалізації безпечного обміну інформацією у військових IoT-мережах (див. табл. 2.1).

Таблиця 2.1 – Основні аспекти алгоритмів функціонування військових IoT-систем

Напрямок оптимізації	**Основні характеристики**
Збирання даних	Подійно-активовані сенсори, зменшення енергоспоживання
Агрегація інформації	Попередня обробка, фільтрація, зменшення навантаження на мережу
Передача даних	Динамічна маршрутизація, ретрансляція через інші вузли

Продовження таблиці 2.1 – Основні аспекти алгоритмів функціонування військових IoT-систем

Напрямок оптимізації	**Основні характеристики**
Енергозбереження	Режими сну, мінімізація передач, локальна обробка, адаптивна маршрутизація
Стійкість до збоїв	Дублювання, зберігання даних, автоматичне відновлення маршрутів
Безпечний обмін	Протоколи LoRa, Zigbee, MQTT, шифрування AES, автентифікація вузлів

2.4 Аналіз можливостей реалізації та обмежень

Розглядаючи можливості реалізації побудованої модульної архітектури IoT-систем для військових задач, необхідно враховувати як потенціал її практичного впровадження, так і спектр технічних, логістичних та концептуальних обмежень. Аналіз охоплює як базові переваги використання відкритих апаратних і програмних компонентів, так і перешкоди, які виникають на етапі адаптації цивільних технологій до фронтових умов, особливо з урахуванням реального польового середовища. Створена на відкритих рішеннях архітектура передбачає:

— можливість масштабування;

— гнучкого перепрофілювання;

— підтримки сценаріїв (орієнтованих на конкретні бойові завдання).

У цьому контексті ключовими стають питання технічної сумісності, стійкості до впливу зовнішніх факторів, стабільності енергозабезпечення та здатності до автономного функціонування в умовах радіоелектронної боротьби чи фізичної ізоляції від мережевих джерел [17].

Переваги використання відкритих компонентів у військових IoT-системах. Розробка військових IoT-рішень на базі відкритих компонентів типу ESP32, Raspberry Pi, Arduino та подібних модулів, які доступні на цивільному ринку, відкриває шлях до значного зниження витрат у порівнянні з традиційними військовими аналогами. Комерційна доступність дозволяє швидко формувати як прототипи, так і обмежено серійні системи без потреби у великих фінансових чи логістичних вкладеннях. За умов високої динаміки бойових дій це особливо цінно, оскільки створює можливість оперативного розгортання рішень навіть в умовах обмеженої інженерної підтримки. При цьому такі компоненти мають відкриту технічну документацію, широке коло прикладів реалізації, активну спільноту розробників і готові бібліотеки, що дозволяє не лише скоротити час на розробку, а й суттєво спростити процес інтеграції змін у вже існуючі системи. Наявність цієї підтримки також відкриває шлях до гнучкої адаптації під конкретні умови — з можливістю заміни сенсорних модулів, налаштування алгоритмів, оптимізації протоколів зв’язку чи додавання нових логічних блоків у загальну структуру.

В умовах війни, де фактор часу і стабільності систем має критичне значення, архітектура, що базується на відкритих та модульних компонентах, дозволяє швидко адаптуватися до змін тактичної обстановки. Наприклад, у випадку втрати зв’язку з центральним вузлом, система може бути перебудована в режимі mesh-з’єднання для забезпечення самостійного функціонування вузлів та підтримки локального обміну даними. Завдяки модульності, адаптація може здійснюватися без повного перепроєктування, шляхом локального втручання, що забезпечує перевагу в умовах обмеженого часу чи ресурсів. Відкритий код дозволяє розробникам з різних підрозділів оперативно ділитися рішеннями та досвідом, забезпечуючи горизонтальне поширення технологічних інновацій без централізованого узгодження або бюрократичних процедур.

Попри це, технічні та експлуатаційні обмеження таких рішень вимагають уважного аналізу, особливо у фронтових умовах. Відкриті платформи не завжди забезпечують належний рівень захисту від механічного впливу, екстремальних температур, вологи або електромагнітних завад, що виникають у результаті

радіоелектронної боротьби. Значна частина компонентів спроєктована для побутових або індустріальних умов, а не для застосування в зоні бойових дій, тому підвищується ризик виходу з ладу при тривалому використанні без зовнішнього захисту. Енергетичне забезпечення також є критичним фактором — хоча деякі вузли підтримують енергоефективні режими, як-от "Deep Sleep", забезпечення стабільної роботи вимагає резервних акумуляторів або альтернативних джерел енергії, таких як сонячні панелі, що можуть бути вразливими до зовнішнього впливу або недоступними в певних умовах.

Серед обмежень варто враховувати і залежність від зовнішньої інфраструктури, зокрема для обміну даними або оновлення прошивок. В умовах повної ізоляції або знищення каналів зв’язку, вузли, які не передбачають повну автономність, стають нефункціональними або обмежено корисними. Проблемою є також обмеженість обчислювальних ресурсів відкритих апаратних платформ, що накладає обмеження на складність обробки даних безпосередньо на вузлі. У системах, що мають працювати з потоковим відео, високочастотними сенсорами або алгоритмами машинного навчання, стандартні рішення можуть не забезпечити достатньої продуктивності без додаткових модулів або переорієнтації задач на хмарну або серверну обробку.

Важливо також усвідомлювати логістичні труднощі, які супроводжують закупівлю компонентів в умовах обмежень імпорту, нестабільного постачання або санкцій. Попри доступність на глобальному ринку, доставка комплектуючих може бути ускладнена або затримана, особливо якщо йдеться про стратегічні компоненти, які контролюються виробниками з країн, що не підтримують пряму допомогу, що спонукає до пошуку локальних альтернатив або формування складів із запасами критичних модулів, що потребує додаткових зусиль із боку розробників та логістичних структур.

Незважаючи на ці виклики, загальна концепція побудови військових IoT-систем на основі відкритих технологій залишається перспективною та адаптивною. Навіть з урахуванням вразливостей, вона дозволяє вивчати нові сценарії, моделювати бойові ситуації, реалізовувати експериментальні функції та проводити

тестування в реальних умовах, що створює середовище, у якому інженерна ініціатива, волонтерський ресурс і низький поріг входження у розробку здатні компенсувати обмеження традиційних підходів. І хоча ці рішення не завжди можуть слугувати повноцінною заміною для промислових військових платформ, у межах гібридної архітектури вони відіграють критичну роль як гнучкий, швидкий і масштабований засіб реагування на нові виклики, що постають перед оборонною технологічною екосистемою.

Основні технічні бар'єри впровадження. Розробка IoT-рішень для військового застосування, особливо на основі відкритих компонентів, передбачає не лише аналіз потенційних переваг, а й детальне врахування низки технічних бар'єрів, які виникають під час практичного впровадження таких систем у бойових умовах.

Однією з найвагоміших проблем є обмеженість енергетичних ресурсів, оскільки більшість поширених мікроконтролерів, таких як ESP32 або Raspberry Pi, мають доволі обмежені можливості енергозбереження й не забезпечують достатньої автономності для тривалого функціонування без підзарядки чи заміни живлення, що в умовах фронту є критично недоступним. Рішення, які потребують частого технічного обслуговування, не відповідають вимогам мобільності, непомітності та автономності, тому їх використання вимагає ретельної модифікації або розробки альтернативних енергетичних схем [17].

Крім проблем із живленням, значну загрозу становить низька завадостійкість комерційних пристроїв, адже більшість з них не розраховані на роботу в умовах радіоелектронної боротьби, не мають захисту від спрямованих електромагнітних імпульсів і легко піддаються глушінню або перехопленню, особливо при використанні стандартних протоколів безпровідного зв'язку, таких як Wi-Fi або Bluetooth. Ці протоколи через відкриту архітектуру є вразливими, і тому потребують або повної заміни на більш захищені системи зв'язку, наприклад, LoRa чи Zigbee з додатковим криптографічним захистом, або ж інтеграції зі спеціалізованими військовими засобами зв'язку, які відповідають вимогам безпечного передавання інформації в умовах заглушення чи перехоплення.

Іншою перешкодою, яка має не меншу вагу, є низький рівень фізичного захисту відкритих платформ, оскільки більшість з них постачаються без захищених корпусів, що унеможливлює їх використання в агресивному середовищі, характерному для активної фази бойових дій. Пил, волога, механічні удари та вібрації швидко виводять з ладу неінкапсульовану електроніку, тому вимагається створення нових, стійких до впливу довкілля корпусів з додатковим екрануванням, герметизацією, термозахистом і вандалозахисними елементами, що забезпечують відповідність стандартам IP67 і вище або навіть військовим специфікаціям.

Проблематика також охоплює питання інформаційної безпеки, оскільки відкриті системи часто не мають вбудованих механізмів шифрування, автентифікації чи захисту на рівні прошивки, що створює серйозні ризики витоку або підміни даних у разі компрометації вузла. Для запобігання таким загрозам необхідне:

— програмне шифрування;
— налаштування протоколів безпечної передачі інформаці;
— реалізація функцій самознищення або автоматичного стирання даних (при втраті або захопленні пристрою).

Усе це стає особливо актуальним при використанні IoT-рішень безпосередньо на передовій.

Адаптація цивільних рішень до вимог фронтової експлуатації. Всі вищезазначені фактори не виключають доцільності використання відкритих компонентів, однак зумовлюють необхідність їх глибокої адаптації до фронтової експлуатації, що відбувається у кількох напрямках. Одним із ключових аспектів адаптації є зміцнення апаратної частини, що передбачає повну заміну типового комерційного корпусу на спеціалізовані варіанти, здатні витримувати агресивні умови бойового застосування. Пристрої потребують додаткового захисту за допомогою термостійких матеріалів, посиленого корпусу, герметизації, а також використання антивандальних рішень для збереження функціональності навіть у разі прямого фізичного впливу.

Інтеграція з військовими засобами зв’язку є ще одним напрямком адаптації, що передбачає використання сумісних радіомодулів, які працюють у дозволених діапазонах частот та підтримують військові протоколи, забезпечуючи надійність і безперебійність передачі даних у тактичних мережах. Для забезпечення безпеки інформації необхідно реалізовувати надійне шифрування та резервне зберігання даних, а також запроваджувати функції автоматичного знищення інформації, що дозволить запобігти її захопленню у разі втрати обладнання.

Адаптація також передбачає розробку програмного забезпечення, орієнтованого на фронтову експлуатацію, з простими й ефективними інтерфейсами, які дозволяють швидко налаштовувати пристрої навіть за відсутності спеціальних навичок, з використанням мобільних застосунків або веб-інтерфейсів з базовими функціями моніторингу, оновлення, перевірки стану або передавання повідомлень (див. рис. 2.12).

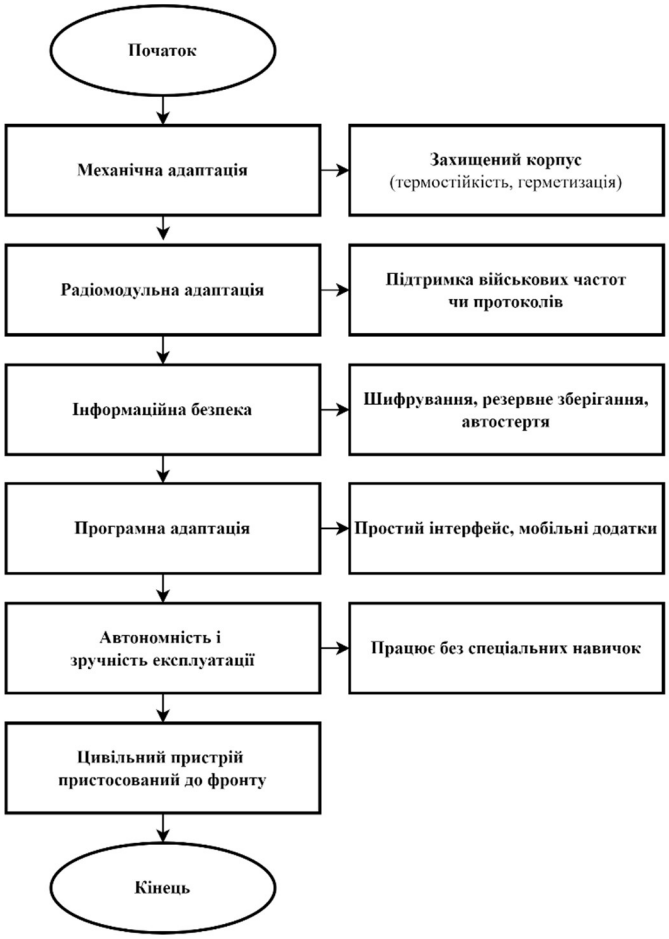


Рисунок 2.12 – Модель адаптації цивільного IoT-пристрою

За умови належної технічної підготовки, навіть доступні на ринку цивільні IoT-рішення можуть бути ефективно модифіковані для використання у складних тактичних місіях, що значно скорочує час розробки, дозволяючи зосередитися на адаптації програмної частини та забезпеченні надійної фізичної оболонки, що дозволяє пристроям виконувати поставлені завдання в умовах війни.

Можливості реалізації концептуальних моделей та польового тестування. У нинішніх умовах навіть без серійного виробництва можлива розробка демонстраційних моделей, здатних забезпечити практичну оцінку доцільності будь-якої запропонованої IoT-системи незалежно від того, чи перебуває вона ще лише на стадії концепції, чи вже проходить початкові етапи реалізації. Основна увага при цьому спрямовується на створення прототипів, які можуть бути зібрані на базі відкритих апаратних платформ, таких як ESP32, із застосуванням LoRa-модулів або простих сенсорів — температури, руху, GPS тощо, що дозволяє сконструювати діючий зразок, здатний емулювати роботу повноцінного пристрою або елементу мережі, з подальшим проведенням випробувань у контрольованих умовах. Такі тестування, що виконуються у навчальних зонах, дозволяють виявити потенційні технічні недоліки, серед яких можуть бути недостатній рівень покриття, обмежений час автономної роботи, низька завадостійкість або ненадійна точність переданих даних, що в комплексі визначає відповідність пристрою критеріям, які закладались у технічному завданні [17].

Після оцінки у польових умовах доцільно застосовувати також емуляційні середовища, що дозволяє моделювати складні сценарії без ризику для обладнання чи особового складу. Використання таких програмних рішень, як SLSim або Contiki-NG, забезпечує можливість віртуального розгортання мереж із десятками вузлів, що імітують навантаження, зміну топології та реакцію системи на зовнішні впливи, дозволяючи прогнозувати її поведінку в реальних умовах бойових дій або при раптових змінах ситуації. На основі отриманих результатів, навіть без завершеного продукту, можна сформувати концептуальне бачення системи, яке подається як демонстраційна модель для оборонного планування, дозволяючи військовому командуванню:

— оцінити технічні можливості;

— сформувати вимоги до майбутніх рішень;

— визначити пріоритети у впровадженні певних функціональностей.

Відкриті платформи при цьому забезпечують необхідну гнучкість, щоб швидко втілювати запропоновані зміни, орієнтуючись на конкретні вимоги фронту, та в окремих випадках дозволяють сформувати реалістичні очікування від майбутніх розробок на закритих або спеціалізованих платформах (див. рис. 2.13) [17].

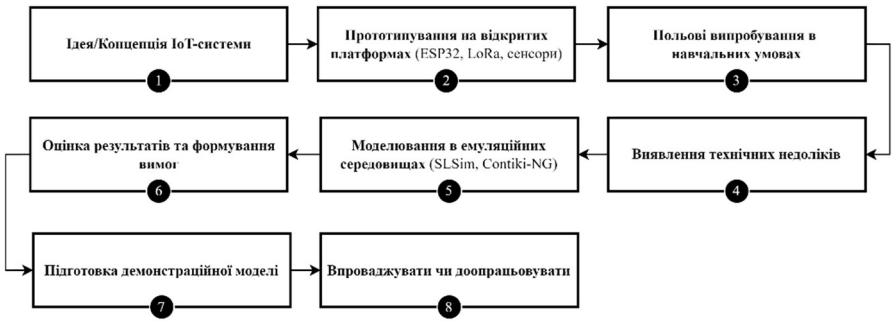


Рисунок 2.13 – Етапи розробки та тестування прототипу у польовому випробуванні

Таблиця 2.2 – Напрями реалізації та тестування концептуальних моделей військових IoT-рішень

Напрям	**Суть реалізації**	**Очікувана користь**
Розробка прототипів	Створення зразків на базі ESP32, LoRa, сенсорів	Оцінка функціональності та архітектури
Польове тестування	Випробування в тренувальних умовах	Виявлення технічних недоліків
Емуляція	Моделювання поведінки мережі у середовищах типу Cooja	Тестування складних сценаріїв без ризиків
Концептуальна демонстрація	Візуалізація ідей без готових пристроїв	Підтримка планування та прийняття рішень

Підсумовуючи, незважаючи на наявні обмеження щодо використання відкритих IoT-компонентів у військових цілях, їх застосування залишається перспективним напрямом (див. табл. 2.2), особливо на етапах ранньої розробки в умовах обмежених ресурсів. Водночас ефективне впровадження таких рішень потребує:

- глибокої технічної адаптації;
- врахування реалій бойового застосування;
- розробки захищених корпусів;
- стійких протоколів зв’язку;
- надійного програмного забезпечення.

Саме завдяки проходженню етапів прототипування та польового тестування створюється основа для формування повноцінних тактичних IoT-систем, які можуть бути масштабовані та інтегровані в сучасну оборонну інфраструктуру.

РОЗДІЛ 3 ОЦІНКА ІСНУЮЧИХ ПІДХОДІВ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

3.1 Методи покращення систем IoT

Ефективність IoT-систем у військовому середовищі значною мірою залежить від здатності працювати автономно, забезпечувати стабільний зв’язок та гарантувати безпечний обмін даними, що є критичним у складних і змінних умовах бойових дій. Серед основних напрямів удосконалення таких систем доцільно виділяти методи, спрямовані на:

- зниження енергоспоживання;
- забезпечення захищеності передачі інформації;
- підвищення стійкості до впливів зовнішнього середовища;
- адаптацію архітектури систем до постійних змін і загроз.

Ці напрямки взаємодіють між собою, створюючи комплекс рішень, здатний істотно підвищити практичну ефективність існуючих систем у військових застосуваннях навіть без докорінної перебудови їхньої структури [18].

Застосування енергозберігаючих режимів та альтернативних джерел живлення. Один із першочергових аспектів полягає у впровадженні енергозберігаючих режимів та альтернативних джерел живлення, адже в умовах обмеженого доступу до централізованого електропостачання критично важливо мінімізувати споживання енергії. Сучасні мікроконтролери та сенсори, навіть у своїх цивільних варіантах, здатні переходити у глибокі енергозберігаючі стани на кшталт deep sleep, у яких енергоспоживання знижується до одиниць мікроамперів. Активізація системи відбувається лише у випадку зовнішніх тригерів, як-от виявлення руху, зміна температури чи інші зміни середовища, що дозволяє пристрою залишатися більшість часу неактивним, споживаючи мінімальну

кількість енергії. У поєднанні з подійно-орієнтованими механізмами, такими як "wake-on-interrupt", забезпечується значна економія без шкоди для функціональності, що критично важливо при тривалому розгортанні в полі без змоги швидкого доступу до технічного обслуговування (див. рис. 3.1).

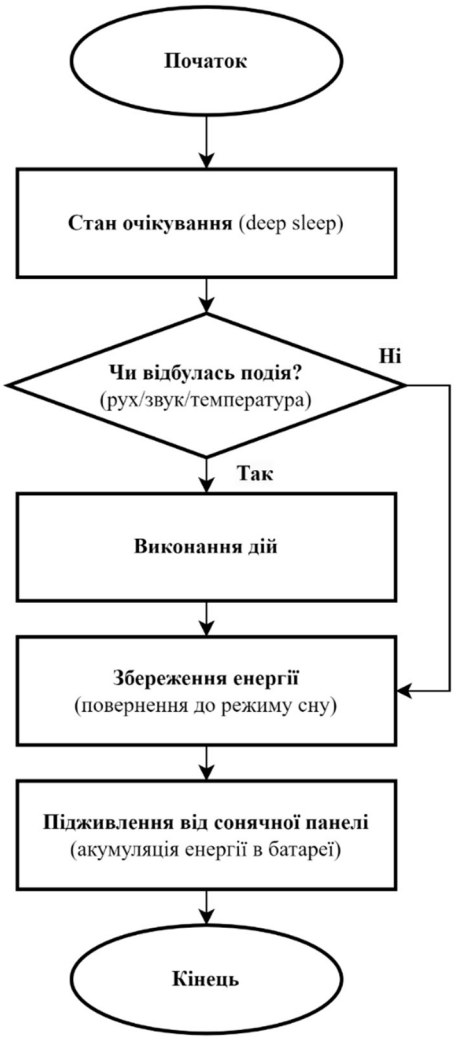


Рисунок 3.1 – Метод перемикання енергозберігаючих режимів

Додатково доцільно використовувати альтернативні джерела живлення, зокрема сонячні панелі, які здатні не лише підтримувати роботу пристрою впродовж дня, а й поповнювати енергетичний запас акумуляторів (див. рис. 3.2).



Рисунок 3.2 – Приклад використання сонячного живлення

Такий підхід дозволяє уникати залежності від міських мереж або польових генераторів, забезпечуючи стабільну роботу навіть у повній ізоляції. У разі відсутності сонячного випромінювання або настання ночі накопичена енергія може використовуватись із акумуляторів, батарей або суперконденсаторів, що забезпечує безперервність функціонування. Зменшення частоти втручання технічного персоналу для заміни або підзарядки живлення дозволяє підвищити живучість систем у бойових умовах, де кожне фізичне наближення до пристрою пов’язане з ризиками або логістичними труднощами.

Вбудоване шифрування, автентифікація та захист проти атак. Захист переданої інформації є однією з базових вимог для будь-якої IoT-системи, що функціонує в умовах потенційно ворожого, динамічного та непередбачуваного середовища, де ризики перехоплення або маніпуляцій із даними залишаються постійно високими. У такому контексті особливого значення набуває вбудоване шифрування даних безпосередньо на рівні пристрою, де загальноприйнятим стандартом для малопотужних систем є AES-128, що забезпечує достатній рівень криптостійкості за мінімального навантаження на обчислювальні ресурси. Разом із цим для захисту каналів зв’язку можуть застосовуватись транспортні рівні протоколи безпеки, зокрема TLS або його спрощені версії на кшталт mbedTLS, спеціально оптимізовані для вбудованих систем з обмеженою обчислювальною

потужністю. Такий рівень шифрування, однак, не є достатнім без впровадження автентифікації між пристроями, що дозволяє гарантувати достовірність учасників обміну [18].

Автентифікація може бути реалізована через попередньо встановлені сертифікати, симетричні ключі з обмеженим терміном дії або ж гібридні підходи, які враховують баланс між безпекою та продуктивністю системи. В окрему групу загроз належать атаки типу replay, коли зловмисник повторно надсилає перехоплені раніше пакети з метою викликати некоректну реакцію системи, тому для протидії таким діям доцільно застосовувати часові мітки, унікальні ідентифікатори сесій та нонси, які гарантують одноразовість використання кожного переданого пакета. У сукупності такі підходи дозволяють формувати більш стійке до втручання середовище, де пристрої не лише здійснюють обмін даними, але й постійно підтверджують свою приналежність до системи, що має вирішальне значення в умовах активних бойових дій, коли загроза проникнення у внутрішній периметр залишається постійною [18].

Ретрансляція та побудова mesh-мереж для покращення дальності і надійності зв'язку. У ще складніших умовах, де класичний прямий зв'язок між пристроями або з базовими станціями ускладнений через фізичні перешкоди, радіоелектронні засоби придушення або велику відстань, ефективним рішенням є впровадження ретрансляційних механізмів та побудова mesh-мереж, у яких кожен вузол здатний виконувати функцію проміжного передавача сигналу. У такій мережевій топології забезпечується автоматичне перенаправлення трафіку навіть у разі виходу з ладу окремих вузлів, оскільки структура постійно адаптується до змін, дозволяючи знайти альтернативні маршрути передачі даних. Вузли, які розміщені в енергетично стабільних точках або мають доступ до додаткових джерел живлення, можуть брати на себе більшу частину навантаження, функціонуючи як магістральні ретранслятори, що підвищує загальну гнучкість і життєстійкість мережі.

Mesh-архітектура демонструє також здатність до самовідновлення, оскільки втрата одного або кількох елементів не порушує загальну комунікаційну структуру,

а маршрути миттєво перебудовуються без зовнішнього втручання чи централізованого контролю. Такий підхід дозволяє зберігати зв’язок між мобільними об’єктами, спостережними пунктами та командними центрами навіть у розосереджених і динамічно змінних умовах, які характерні для сучасного театру бойових дій. Завдяки високій масштабованості mesh-системи можуть покривати великі території, функціонуючи незалежно від централізованої інфраструктури, що суттєво підвищує їхню надійність і стійкість до кібератак, оскільки децентралізований характер мережі унеможливлює централізоване виведення її з ладу або перехоплення керування (див. рис. 3.3).

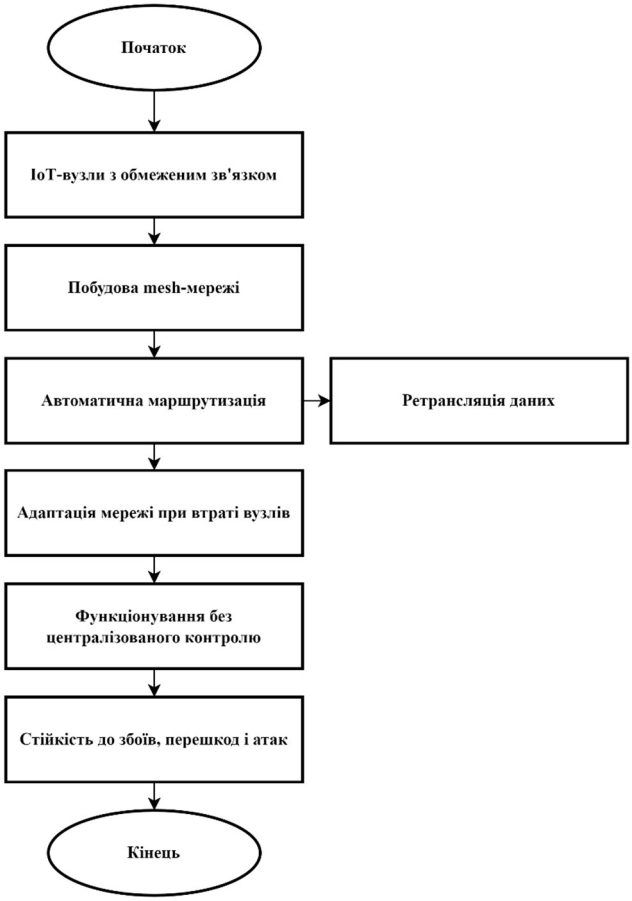


Рисунок 3.3 – Метод побудови mesh-мережі для збільшення дальності

Така мережа здатна продовжувати функціонувати навіть у разі компрометації окремих вузлів, що є важливим фактором під час реалізації польових операцій або розгортання IoT-рішень у зоні бойового контакту.

Модульність, адаптивність та відмовостійкість архітектури. Таким останнім, але не менш значущим аспектом удосконалення IoT-систем у військовому контексті залишається побудова архітектури, здатної до адаптації, масштабування і збереження працездатності навіть у випадках часткових пошкоджень або втрати окремих компонентів. Модульність у цьому випадку означає, що система має складатися з окремих функціональних блоків, кожен з яких виконує свою специфічну роль і при цьому може бути замінений, оновлений або модифікований без необхідності зупинки всієї інфраструктури. Один модуль може бути відповідальним за збір даних, інший — за їх передачу, ще один — за локальну обробку, що дає змогу підтримувати роботу навіть у випадках деградації або втрати частини мережі. Такий підхід також дозволяє легко масштабувати систему, додаючи нові функціональні вузли в залежності від потреб, без серйозного втручання в основну структуру.

Високий рівень адаптивності дозволяє змінювати маршрути передачі, пріоритети обробки або логіку роботи в реальному часі, залежно від конкретної ситуації. У разі втрати з’єднання з центральним вузлом можлива автоматична переорієнтація системи в автономний режим із локальним збереженням критичних даних, щоб забезпечити їх подальшу передачу після відновлення зв’язку. Усі ці функції стають особливо важливими в бойових умовах, де пристрої можуть бути зруйновані або фізично пошкоджені, виведені з ладу радіоелектронними засобами або захоплені противником. Для таких ситуацій надзвичайно важливо забезпечити відмовостійкість системи шляхом дублювання критичних компонентів — джерел живлення, передавачів, вузлів обробки або елементів зберігання, а також застосування механізмів автоматичного виявлення та ізоляції несправних компонентів, з подальшим обходом проблемних ділянок мережі (див. рис. 3.4).

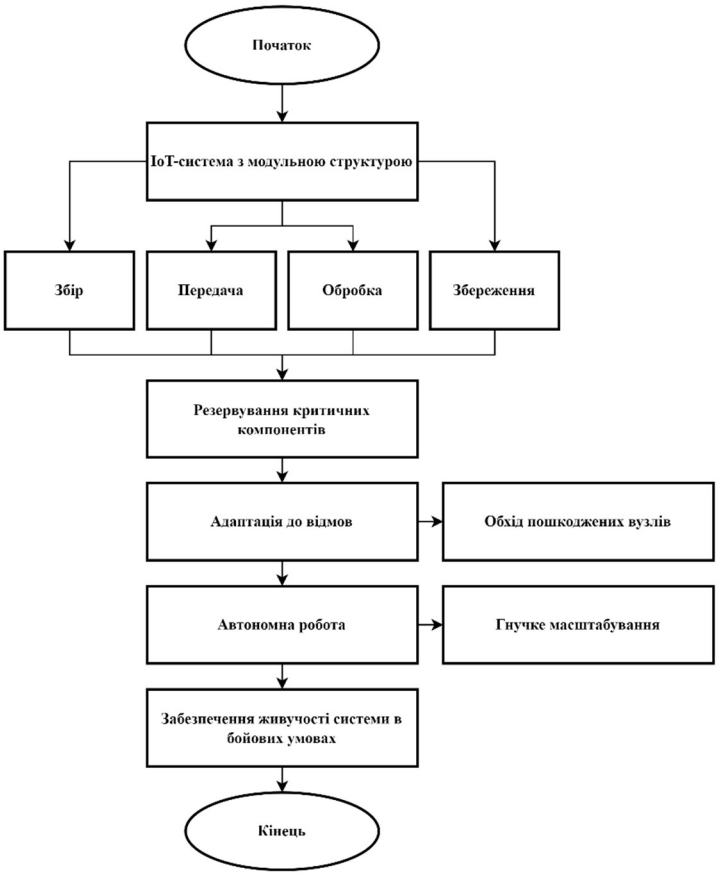


Рисунок 3.4 – Метод використання адаптивної модульної архітектури з резервуванням

У поєднанні з самовідновлюваними мережевими структурами, захищеним шифруванням даних і гнучкими каналами передачі така архітектура створює життєздатну платформу для роботи в динамічному, агресивному середовищі, де постійно змінюються умови, а стабільність — це виняток, а не норма. Реальне застосування таких систем у військових умовах потребує максимальної гнучкості, швидкої адаптації до загроз і наявності резервних сценаріїв на всіх рівнях. Саме тому архітектурна модульність у поєднанні з адаптивною логікою обробки і наявністю вбудованих механізмів захисту стає не лише технічною перевагою, а фактично обов’язковою умовою для створення дієздатної системи в умовах бойового середовища, де не можна передбачити всі сценарії, але необхідно бути готовим до будь-якого з них [18].

Таблиця 3.1 – Порівняння методів покращення IoT-систем

Метод	**Економія енергії**	**Безпека**	**Дальність зв’язку**	**Стійкість**	**Впровадження**	**Вартість**
Deep Sleep (режим сну)	Висока	—	—	Середня	Легка	Низька
Акумулятор	Висока	—	—	Добра	Легка	Середня
Сонячні панелі	Висока	—	—	Висока	Середня	Вища
TLS / MQTT захист	—	Висока	—	Середня	Середня	Низька
AES шифрування	—	Висока	—	Середня	Легка	Низька
Mesh-мережа	Середня	Середня	Далека	Добра	Складна	Середня
LoRa / LoRaWAN	Висока	Середня	Дуже далека	Висока	Складна	Вища
Ретранслятори	Низька	—	Далека	Середня	Легка	Середня
Модульна конструкція	Середня	—	—	Висока	Середня	Низька
Локальна обробка (Edge)	Висока	Висока	—	Висока	Середня	Середня
Захищений корпус (IP65+)						

У підсумку реалізація таких методів удосконалення (див. табл. 3.1) дозволяє формувати IoT-рішення, здатні ефективно функціонувати навіть у найбільш складних умовах, де традиційні системи часто виявляються непридатними. Поєднання енергоефективних технологій, багаторівневого захисту інформації, самовідновлюваних мереж і адаптивної, модульної архітектури створює основу для сучасних, надійних і стійких рішень військового призначення, що мають потенціал перевершити існуючі реалізації та забезпечити новий рівень функціональності і стійкості в реальних умовах застосування.

3.2 Порівняння з іншими IoT-рішеннями

Розробка військових IoT-систем часто базується на адаптації або переосмисленні існуючих рішень, створених для цивільного використання, однак суттєві відмінності в умовах експлуатації, вимогах до безпеки, автономності та стійкості до зовнішніх впливів не дозволяють безпосередньо перенести комерційні технології у військовий контекст без серйозних доопрацювань, адже більшість із них створювалися з урахуванням середовища з прогнозованими ризиками та контрольованою інфраструктурою, тоді як військові умови є вкрай нестабільними, агресивними та непередбачуваними, що висуває зовсім інший набір вимог як до апаратної, так і до програмної складової IoT-рішень [19].

Відмінності за ключовими критеріями. Оцінювання ефективності таких рішень у військовому застосуванні вимагає детального порівняння за основними технічними критеріями, одним із яких є безпека — в умовах цивільного середовища зазвичай використовуються базові засоби захисту, такі як WPA2 для Wi-Fi, які є достатніми в більшості випадків, однак у бойовій обстановці навіть найменше порушення цілісності або конфіденційності переданих даних може мати катастрофічні наслідки, тому реалізація багаторівневого захисту на основі сучасних криптографічних протоколів, взаємної автентифікації пристроїв,

шифрування з підтримкою захисту від перехоплення, підміни та повтору повідомлень стає обов’язковою вимогою, що значною мірою ускладнює як розробку, так і тестування систем, особливо в умовах постійної загрози з боку засобів радіоелектронної боротьби.

Не менш важливою є автономність, оскільки якщо у побутових IoT-рішеннях живлення зазвичай забезпечується через стаціонарне підключення до електромережі або стабільні канали зв’язку типу Wi-Fi, то у польових умовах військові вузли часто розгортаються у віддалених або недоступних районах, де немає можливості для регулярного обслуговування, тому пристрої повинні функціонувати безперервно протягом тривалого часу, використовуючи обмежені ресурси живлення з глибокими режимами сну, енергозберігаючими протоколами та можливістю самостійного переходу у пасивний або економний режим в залежності від активності та сценарію використання, що вимагає значно складнішої логіки прошивок, ніж у звичайних споживчих пристроях.

Ще одним критичним параметром, який не можна ігнорувати, є дальність зв’язку — якщо комерційні рішення здебільшого розраховані на роботу в межах десятків метрів з використанням Bluetooth або Wi-Fi, то в умовах розосередженого розгортання військових підрозділів це є абсолютно неприйнятним, оскільки необхідно забезпечити стійке з’єднання на значні відстані, включаючи зони з нерівномірним рельєфом, відсутністю прямої видимості або перешкодами у вигляді будівель, рослинності чи перешкод радіозв’язку, тож для цього застосовуються технології з низьким енергоспоживанням та великою дальністю дії типу LoRaWAN, NB-IoT або навіть власні протоколи із побудовою щільної сітчастої мережі для підтримання зв’язку в умовах втрати центральної інфраструктури.

Ще один аспект, який часто недооцінюється у цивільних рішеннях, але має вирішальне значення у військових — енергоефективність, адже якщо в побутових системах пристрої можуть бути постійно підключені до джерел живлення і споживати енергію практично без обмежень, то в бойових умовах кожен міліампер енергії має значення, і баланс між частотою збору даних, передачею інформації,

режимами очікування та енергоспоживанням впливає безпосередньо на тривалість життєвого циклу кожного вузла, тому проєктування таких систем включає оптимізацію на рівні схемотехніки, елементної бази, прошивок та протоколів передачі даних з урахуванням сценарного планування навантаження, адже в іншому випадку вузли або будуть потребувати частого обслуговування, або перестануть працювати в найвідповідальніший момент.

Незважаючи на певну схожість у концепціях, цивільні та військові IoT-рішення відрізняються за суттю, цілями і пріоритетами настільки суттєво, що лише загальний підхід до збору, обробки і передачі даних може вважатися спільним, у той час як технічна реалізація, організаційні підходи та рівень допуску до помилки формують зовсім інше середовище, у якому військові системи повинні залишатися стабільними, безпечними і автономними незалежно від зовнішніх умов, навіть якщо доводиться діяти ізольовано, в умовах відсутності зв’язку, енергетичної підтримки або під безпосереднім ризиком фізичного знищення чи захоплення.

Приклади з реального світу – цивільні та військові рішення. Для кращого розуміння відмінностей між цивільними та військовими IoT-рішеннями з урахуванням критичних параметрів і умов експлуатації доцільно звернутися до прикладів реального використання, що на практиці демонструють принципові розбіжності між цими підходами, наприклад, у випадку з цивільними логістичними системами, які використовують GPS-трекери для моніторингу транспорту, доставок або керування автопарками, йдеться про пристрої з SIM-картами, GPS-модулями, акумуляторами і можливістю передавати координати через стільникову мережу у хмарне сховище в межах покриття операторів мобільного зв’язку, що забезпечує зручність та ефективність у нормальних умовах інфраструктури з гарантованою доступністю зв’язку, тоді як у військовому застосуванні, наприклад, для систем моніторингу артилерійських підрозділів або розвідувальних груп, GPS-модулі повинні працювати навіть у присутності радіозаглушення, з передачею даних через зашифровані канали на основі LoRa, військових УКХ або КХ-радіостанцій, із застосуванням буферизації, коли дані тимчасово зберігаються локально та передаються лише після відновлення зв’язку, що дозволяє

підтримувати працездатність системи навіть за умов повної відсутності з’єднання з базовими станціями або втрати каналів передачі.

Крім технічних характеристик, відмінність простежується в самих підходах до побудови систем, де цивільні рішення орієнтовані на зручність, дешевизну і масовість, у той час як військові потребують максимального акценту на надійність, ремонтопридатність і витривалість до екстремальних зовнішніх впливів, тобто ті якості, які часто ігноруються у комерційних пристроях як зайві або фінансово недоцільні, стають критичними в бойових умовах, що автоматично обмежує можливість використання непідготовлених рішень з масового ринку.

Обмеження комерційних IoT у бойових умовах. Розглядаючи потенційне застосування комерційних IoT-пристроїв у бойових умовах, можна дійти висновку, що, попри їхню загальну доступність і відносно низьку вартість, вони не здатні задовольнити специфічні вимоги фронту без глибокої попередньої адаптації, серед головних обмежень можна виокремити низький рівень захисту, оскільки більшість комерційних пристроїв або зовсім не мають вбудованих засобів криптографії, або передають дані у відкритому вигляді, що робить їх вразливими до перехоплення, підміни повідомлень, реверс-інжинірингу, а відповідно створює додаткові ризики для бойових підрозділів у разі компрометації технічних засобів.

Додатково важливим обмеженням є залежність від інфраструктури, адже пристрої, які потребують підключення до Wi-Fi або мобільного зв’язку, втрачають свою функціональність у зоні активних бойових дій, де така інфраструктура або повністю знищена, або перебуває під постійною загрозою з боку противника, натомість військові системи повинні бути повністю автономними, з власними засобами комунікації, здатними працювати в офлайн-режимі та не залежати від зовнішніх сервісів, що забезпечує їхню стійкість навіть у разі повної ізоляції.

Ще одним критичним обмеженням є механічна вразливість — комерційні пристрої, створені для використання в офісах, будинках чи промислових приміщеннях, часто не витримують впливу вібрацій, пилу, вологи, перепадів температур або механічних навантажень, які є звичними в бойовому середовищі, що робить їх непридатними для тривалого використання в умовах фронту, де навіть

незначна несправність може призвести до втрати каналу зв’язку або системи спостереження (див. рис. 3.5).



Рисунок 3.5 – Приклад цивільного IoT, непридатного до бойових умов

До цього додається відсутність адаптивності, оскільки більшість комерційних IoT-пристроїв мають закриту або обмежену архітектуру, яка не дозволяє легко змінювати конфігурацію, оновлювати прошивки або перепризначати функції відповідно до зміни тактичної ситуації чи бойового завдання, у той час як військові рішення повинні мати відкриту або хоча б модульну структуру, що дозволяє адаптувати систему до нових умов у максимально стислі строки.

В результаті, використання цивільних IoT-рішень у бойових умовах можливе лише як тимчасове рішення або прототип, який потребує значної модифікації як на рівні апаратного забезпечення, так і в програмній частині, з урахуванням усіх вимог до безпеки, енергоефективності, автономності та стійкості до зовнішніх впливів, тобто фактично — як базовий каркас, на основі якого вибудовується нове повноцінне військове рішення, здатне функціонувати в умовах реальної війни.

Аналіз вартості, наявності та логістичних викликів. Економічна доцільність, доступність та логістичні виклики формують ще один важливий аспект, що визначає можливість практичного впровадження тих чи інших IoT-компонентів у контексті військових систем, адже навіть базові елементи в умовах бойових дій можуть виявитися складними для отримання через перебої в ланцюгах постачання, санкційні обмеження чи інші зовнішні чинники, які здатні безпосередньо впливати на темпи створення та тестування прототипів. У плані вартості військові сертифіковані рішення зазвичай у кілька разів дорожчі — іноді

в п’ять-десять разів — порівняно з доступними комерційними компонентами на зразок Arduino, ESP-плат або сумісних модулів, і при цьому висока ціна далеко не завжди є гарантією ефективності в конкретному сценарії, де, навпаки, доцільним стає саме використання дешевших платформ, які можуть забезпечити базову функціональність, бути демонстраційною основою або стартовим варіантом для подальшого поглибленого доопрацювання [19].

Коли з’являється потреба в забезпеченні доступу до компонентів, ситуація ускладнюється через те, що імпорт електроніки під час війни стикається з труднощами, починаючи від фізичної відсутності постачальників до ризиків логістичних зупинок або зміни митних правил. Тому практично всі комерційні елементи, що використовуються в DIY-системах, нерідко надходять через альтернативні канали: волонтерські поставки, неформальні постачання з платформ типу AliExpress чи eBay, що закономірно впливає на загальний час реалізації проєкту. Водночас із 2022 року логістика вже частково адаптувалася до нових умов, що дозволило пришвидшити закупівлі та отримання деталей — у порівнянні з періодом, коли війна тільки розпочиналася, тепер реалізація певного рішення може відбуватись значно оперативніше.

Крім цього, додатковим викликом стає ремонтопридатність, яка істотно відрізняється залежно від типу обладнання, адже цивільні модулі часто є простішими для заміни, налаштування чи ремонту завдяки відкритим протоколам, широкій підтримці спільнот і загальнодоступності технічної документації, тоді як військові пристрої, маючи часто закриту архітектуру, захищене ПЗ та жорсткі ліцензійні обмеження, можуть виявитися практично неремонтопридатними у польових умовах без доступу до офіційної техпідтримки чи фірмових сервісів, що тісно пов’язано і з проблемою адаптації — комерційні платформи на кшталт ESP, Arduino або Raspberry Pi, завдяки відкритим екосистемам та підтримці прошивок зразка Tasmota, ESPHome або Home Assistant, дозволяють гнучко змінювати конфігурацію, функції та логіку роботи без суттєвих затрат, тоді як більшість закритих коробкових рішень практично не піддаються перепрошивці або переналаштуванню під інші задачі (див. рис. 3.6).

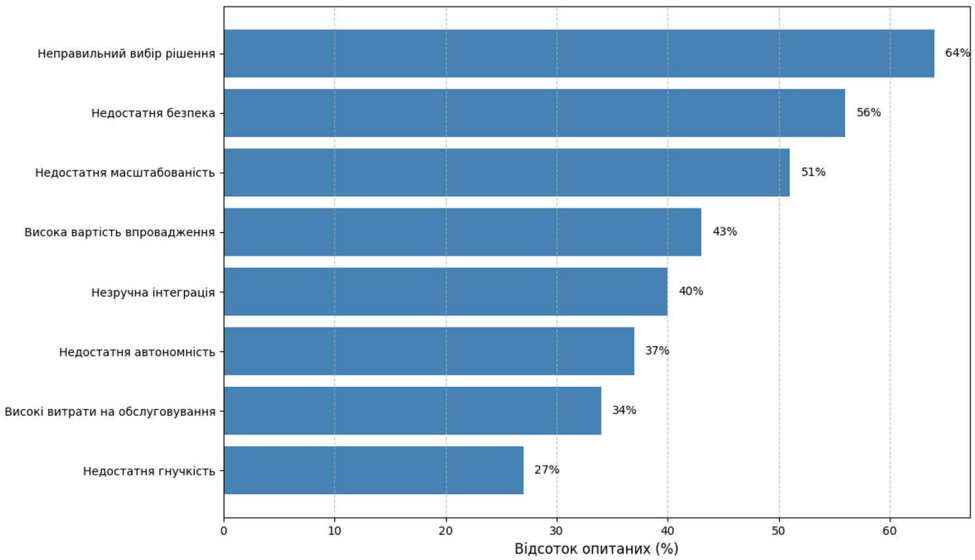


Рисунок 3.6 – Основні причини невдач IoT-проєктів при старті

З огляду на всі ці особливості, ефективною стратегією в умовах війни часто стає комбінований підхід, коли загальнодоступні цивільні модулі використовуються на етапі швидкого створення прототипу або для побудови базового функціоналу системи, що дозволяє не лише зекономити ресурси, але й значно прискорити процес реалізації, після чого відбувається поступове посилення архітектури, інтеграція додаткових засобів захисту, використання зашифрованих каналів зв’язку, покращення автономності й стійкості. Такий підхід, на відміну від повністю «військової» реалізації з нуля, дозволяє гнучко реагувати на зміну ситуації, використовувати доступні ресурси, пришвидшувати R&D і водночас залишати можливість масштабування до більш професійних конфігурацій, коли це дійсно необхідно.

У результаті аналіз за критеріями безпеки, автономності, енергоефективності, дальності зв’язку, ремонтопридатності, інфраструктурної залежності, вартості та адаптивності дозволяє чітко розмежувати дві категорії — цивільні IoT-рішення, що є дешевшими та легкодоступними, але менш витривалими й захищеними, та військові системи, які забезпечують роботу в умовах фронту, мають високу надійність і безпеку, але потребують більших затрат часу, ресурсів та відповідної підтримки (див. табл. 3.2) [19].

Таблиця 3.2 – Порівняння цивільних та військових IoT-рішень за ключовими критеріями

Критерій	**Цивільні IoT-системи**	**Військові IoT-системи**
Безпека	Базове шифрування або відсутність захисту	**Зашифровані канали (AES, TLS), автентифікація, захист від атак**
Автономність	Працюють від постійного живлення або акумулятора на 1–2 доби	**Тривала автономна робота (до кількох тижнів), енергозберігаючі режими**
Дальність зв’язку	Обмежена (Wi-Fi, Bluetooth — до 100 м)	**Дальнє покриття (LoRa, mesh, УКХ/КХ — до кількох км)**
Енергоефективність	Не є пріоритетом, рідко застосовується оптимізація	**Максимальна економія енергії, оптимізація частоти обміну**
Механічна стійкість	Вразливі до пилу, вологи, ударів	**Пиловологозахищені, витривалі до механічних впливів**
Інфраструктурна залежність	Потребують стабільного інтернет-зв’язку або мобільної мережі	**Працюють у відриві від інфраструктури, підтримують буферизацію даних**
Вартість і доступність	Низька вартість, висока доступність на ринку	**Вища вартість, обмежений доступ, залежність від постачальників**
Можливість адаптації	Часто закриті системи, обмежена конфігурація	**Відкриті або гнучкі рішення з можливістю модифікації**

У підсумку ефективність розгортання IoT у бойових умовах значною мірою залежить від правильного вибору початкової платформи, оцінки можливостей її адаптації, а також наявності логістичної спроможності реалізувати задумане в реальному середовищі.

3.3 Перспективи розвитку IoT-систем

Перспективи розвитку IoT-систем у військовому контексті тісно пов’язані з постійним удосконаленням вже наявних рішень, навіть якщо вони були побудовані на базі цивільних технологій, оскільки сама концепція IoT передбачає гнучкість, масштабованість і можливість інтеграції нових функцій без повного перезапуску архітектури. Багато з тих систем, які вже реалізовані або можуть бути реалізовані в умовах бойових дій, мають потенціал до подальшого вдосконалення як на рівні апаратної складової, так і в площині програмного забезпечення, де зокрема йдеться про впровадження інтелектуальних можливостей, енергоефективних протоколів та захищених каналів зв’язку. Розвиток IoT-рішень не обмежується лише фізичним розширенням функціональності, а й передбачає поступову інтеграцію новітніх технологій, таких як штучний інтелект, які можуть суттєво трансформувати принципи роботи систем як у мирний час, так і в умовах конфліктів, оскільки тенденції світового ринку прямо вказують на необхідність автономного аналізу даних і самостійного прийняття рішень у точці збору інформації [20].

Використання штучного інтелекту для локального аналізу та прийняття рішень. З огляду на це, одним із найбільш перспективних напрямів розвитку військових IoT-систем є імплементація алгоритмів штучного інтелекту безпосередньо на кінцевих вузлах, що дозволяє мінімізувати залежність від централізованої інфраструктури і забезпечити локальну обробку даних. Такий підхід є особливо актуальним у бойових умовах, де канали зв’язку часто перебувають під загрозою переривання, глушіння або перехоплення. У таких

випадках надзвичайно важливим є те, щоб вузол міг самостійно аналізувати дані з сенсорів, приймати базові рішення та реагувати у реальному часі без потреби звертатися до центрального сервера. Цього можна досягти завдяки використанню компактних моделей машинного навчання, які реалізуються через бібліотеки типу TensorFlow Lite for Microcontrollers або TinyML, що забезпечує здатність пристрою, зокрема на базі ESP32 чи STM32, розпізнавати ключові події — наприклад, за допомогою підключеного мікрофона виявляти звуки пострілів, вибухів або ж при використанні камери здійснювати базову ідентифікацію об’єктів і умов навколишнього середовища, таких як відкриті простори, ліс, урбанізована зона [20].

У результаті системи набувають можливості відправляти повідомлення або активувати тривогу тільки після детектування конкретного патерну, що знижує кількість хибних спрацювань, економить енергію, зменшує навантаження на канал зв’язку і підвищує ефективність функціонування навіть при мінімальних ресурсах (див. рис. 3.7).

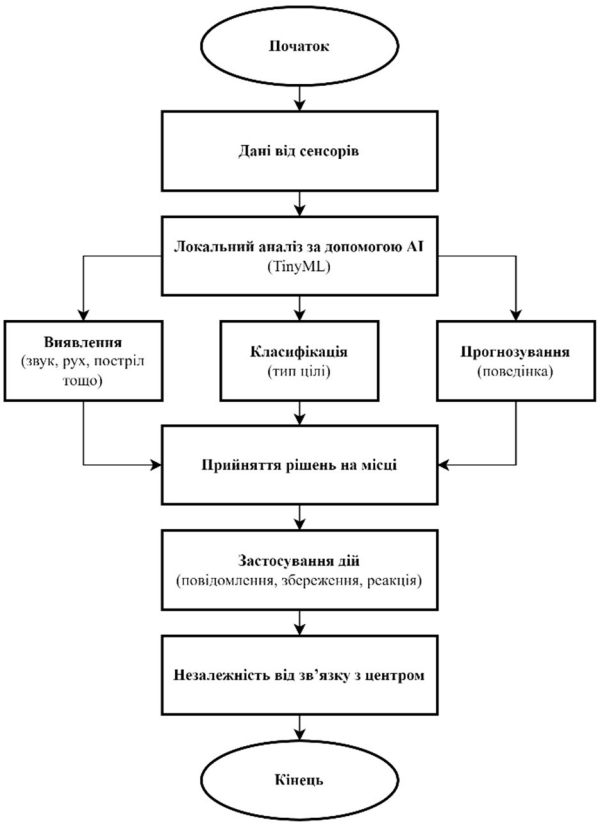


Рисунок 3.7 – Алгоритм використання AI для обробки даних на місці

Така реалізація також підвищує стійкість до кіберзагроз, адже відсутність необхідності в постійному зв’язку з центральним сервером зменшує ризики перехоплення або знищення критичної інформації. Більше того, це дозволяє створити децентралізовану мережу, де кожен вузол не є просто точкою збору даних, а виступає в ролі інтелектуального агента, здатного до адаптації та автономної роботи, що суттєво змінює парадигму проєктування військових IoT-систем загалом.

Інтеграція з супутниковими каналами зв’язку та телекомунікаційними мережами. В умовах знищення або повної відсутності традиційної мобільної інфраструктури, що є типовим у зонах активних бойових дій або на територіях, де агресор цілеспрямовано виводить з ладу критичні телекомунікаційні об’єкти, зростає потреба у створенні альтернативних каналів передачі даних, які б не залежали від наземних систем зв’язку. У цьому контексті інтеграція IoT-вузлів з супутниковими терміналами дозволяє формувати багаторівневу архітектуру, в якій дані збираються на місці події, зберігаються локально, а потім передаються до центрального командного пункту навіть із глибоко ізольованих або тимчасово недоступних регіонів. Такий підхід критично важливий у випадках, коли розгортання стандартної інфраструктури є неможливим — у гірській місцевості, на тимчасово окупованих територіях, у нових бойових позиціях або під час стрімкої зміни фронту, де мобільні вишки просто відсутні або були знищені.

Окрім супутникового каналу, стратегічно важливою стає гібридна інтеграція з існуючими телекомунікаційними мережами, зокрема з LTE і 5G, які можуть бути розгорнуті на контрольованих тилових ділянках або використовуватися для резервного зв’язку. Поєднання цих двох типів інфраструктур — супутникової та наземної — створює можливість динамічного перемикання між каналами передачі залежно від доступності, що забезпечує адаптивність і підвищену стійкість до відмов, порушень або блокування. У результаті структура обміну даними стає гнучкішою, а функціональність IoT-системи не припиняється навіть при втраті одного з типів підключення, що критично важливо у реаліях сучасної війни.

Паралельно з цим відбувається поступове зміщення фокусу з точкових, вузькофункціональних IoT-рішень до побудови масштабних мережевих архітектур, що охоплюють не лише передову, а й глибокі тилові зони — наприклад, логістичні центри, бази постачання, командні пункти та медичні підрозділи. У цьому випадку масштабування полягає не тільки у збільшенні кількості вузлів, але й у побудові системи з можливістю самоконфігурації, автоматичного відновлення зв'язку, гнучкого перерозподілу навантаження, а також із вбудованими механізмами адаптивного реагування на зміни в навколишньому середовищі. Таку систему можна реалізувати шляхом побудови mesh-мереж, де кожен вузол виконує не лише роль сенсора, а також функції ретранслятора, створюючи динамічну, відмовостійку і самовідновлювану структуру зв'язку, здатну функціонувати навіть у разі фізичного знищення окремих елементів.

Розгортання подібних мереж не обмежується лише фізичним підключенням вузлів, оскільки включає централізовану платформу для збору, аналізу і візуалізації даних у реальному часі, що дозволяє приймати стратегічні рішення на основі актуальної ситуації на полі бою. Водночас розвиток Edge-аналітики, тобто логічної обробки даних безпосередньо на вузлі, створює умови для балансу між централізованим управлінням і локальною автономією, дозволяючи системі функціонувати незалежно від центрального центру при необхідності та водночас інтегруватися у загальну структуру в разі відновлення зв'язку. Такий підхід забезпечує не тільки стабільність, а й гнучкість, ефективність та інформаційну перевагу в умовах швидкозмінної тактичної обстановки.

Роль відкритого коду та волонтерських ініціатив. Окремий напрям у розвитку екосистеми військових IoT-рішень може базуватись на ініціативах, що використовують відкритий код і залучення волонтерських спільнот, які в умовах обмеженого доступу до промислових ресурсів і централізованого фінансування фактично беруть на себе функцію розробки та впровадження нових технологій безпосередньо на практиці. В умовах війни, коли темпи змін, необхідність оперативного реагування та адаптації до нових загроз вимагають надзвичайної гнучкості, саме такі ініціативи вже демонструють ефективність, створюючи робочі

прототипи сенсорних вузлів на основі доступних і дешевих компонентів, зокрема мікроконтролерів ESP32, плат Raspberry Pi, модулів LoRa, GPS, камер та інших сенсорів, які легко інтегруються між собою завдяки відкритим протоколам і стандартам (див. рис. 3.8).



Рисунок 3.8 – Вклад волонтерських спільнот у створення рішень: PowerKit

Поєднання цих апаратних рішень з відкритим програмним забезпеченням, таким як Home Assistant для автоматизації, Node-RED для логіки обробки даних, Grafana для побудови візуальних дашбордів, дозволяє будувати повноцінні інформаційні системи, що здатні працювати автономно в умовах відсутності інтернету або централізованої інфраструктури, з можливістю налаштування прямо у польових умовах. За рахунок відкритості таких рішень забезпечується не лише мінімальна вартість реалізації, а й незалежність від дорогих комерційних платформ, що критично важливо в умовах, коли оперативність іноді важливіша за повну технічну досконалість.

Водночас можливість швидкої модифікації під конкретні потреби бойових підрозділів, передача готових конфігурацій між різними командами та підрозділами, кооперація незалежних інженерів, айтішників, технічних волонтерів — усе це формує новий тип екосистеми, що не базується на централізованому управлінні, але здатна бути в рази швидшою в реакції на нові запити і більш

гнучкою в реалізації нестандартних рішень. Відкритий код також дає можливість масштабування рішень у межах державних оборонних програм, якщо буде політична воля та технічна інтеграція з формальними структурами.

Вже зараз така екосистема підтримується переважно ентузіастами, проте з огляду на кількість і якість реалізованих рішень, очікується перехід від розрізнених ініціатив до структурованого середовища, де напрацювання будуть акумулюватися, вдосконалюватися, поширюватися, повторюватися в інших підрозділах, а в перспективі — ставати основою нових підходів до військових IoT-систем на національному рівні. Такий підхід дозволяє не лише забезпечити технологічну самостійність, але й закласти фундамент для постійно оновлюваного й адаптивного середовища, яке не потребує дорогого імпорту і здатне реагувати на запити, що виникають безпосередньо з передової.

ВИСНОВКИ

У роботі досліджено архітектурні підходи до побудови IoT-систем для військових задач із фокусом на відкриті рішення, що забезпечують автономність, надійність і гнучкість. Запропонована модульна архітектура базується на вузлах-ретрансляторах з можливістю підключення різних сенсорів, засобів зв'язку та елементів живлення залежно від умов використання, що дозволяє створювати адаптивні мережі, здатні працювати без централізованої інфраструктури, що особливо важливо в бойових умовах.

Окрему увагу приділено енергоефективності: реалізовано перемикання режимів роботи для зменшення споживання енергії, а також використано прості алгоритми безпечної передачі даних і виявлення втрати зв'язку. Розглянуто переваги mesh-топологій, що підвищують надійність обміну інформацією між вузлами. Така побудова дозволяє утримувати функціонування мережі навіть при виході з ладу окремих елементів.

Програмна частина систем розглядалась з акцентом на можливості використання відкритих інструментів, таких як MQTT-брокери, Node-RED та Home Assistant. Визначено переваги цих платформ для збору, обробки та маршрутизації даних у децентралізованих умовах, показавши, що їхнє застосування дозволяє забезпечити масштабованість, адаптивність та базовий рівень захисту переданої інформації без необхідності повноцінної інфраструктури.

Порівняння з наявними комерційними IoT-рішеннями засвідчило їхню недостатню відповідність вимогам військової сфери через обмежену автономність і слабкий рівень захисту. Натомість, запропонована система демонструє потенціал для гнучкої адаптації, резервування, захисту даних і відмовостійкої роботи, що є критичним для тактичних операцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is IoT (Internet of Things)? | TechTarget. URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (дата звернення: 27.02.2025)
2. The History of IoT: How This Technology Is Evolving - Cogniteq. URL: https://www.cogniteq.com/blog/history-iot-how-technology-evolving (дата звернення: 02.03.2025)
3. The evolution of the Internet of Things (IoT) - im it-planet blog. URL: https://blog.it-planet.com/en/the-evolution-of-the-internet-of-things-iot/ (дата звернення: 07.03.2025)
4. IoT in the military & armed forces - InfiSIM. URL: https://infisim.com/m2m-by-industry/iot-in-the-military (дата звернення: 12.03.2025)
5. Military IoT - Internet of Military Things - Defense Advancement. URL: https://www.defenseadvancement.com/suppliers/internet-of-military-things-iot/ (дата звернення: 17.03.2025)
6. Exploring Advanced Sensor Types and Their IoT Applications - Cavli Wireless. URL: https://www.cavliwireless.com/blog/nerdiest-of-things/sensors-in-iot-applications (дата звернення: 22.03.2025)
7. Information processing in Internet of Things using big data analytics - ScienceDirect. URL: https://www.sciencedirect.com/science/article/abs/pii/S0140366420311579 (дата звернення: 27.03.2025)
8. VISION 60 - Ghost Robotics. URL: https://www.ghostrobotics.io/vision-60 (дата звернення: 01.04.2025)
9. Leleka-100 Unmanned Aerial Vehicle (UAV), Ukraine - Army Technology. URL: https://www.army-technology.com/projects/leleka-100-unmanned-aerial-vehicle-uav-ukraine/ (дата звернення: 06.04.2025)
10. Pentagon Silent on Elon Musk and Starlink Risks as Military Use Expands - Military.com. URL: https://www.military.com/daily-news/2024/11/15/pentagon-silent-elon-musk-and-starlink-risks-military-use-expands.html (дата звернення: 11.04.2025)
11. The internet of battle things: a survey on communication challenges - Springer. URL: https://link.springer.com/article/10.1007/s43926-025-00093-w (дата звернення: 16.04.2025)
12. Article A Reliable and Scalable Internet of Military Things Architecture - ScienceDirect. URL: https://www.sciencedirect.com/org/science/article/pii/S1526149220002350 (дата звернення: 21.04.2025)
13. The Internet of Military Defense Things (IoMDT): State-of-the-Art - IEEE. URL: https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine/cfp/internet-military-defense-things-iomdt (дата звернення: 26.04.2025)

14. Applications of IoT in the defence industry | Issue 145 | February 2024 - Global Defence Technology. URL: https://defence.nridigital.com/global_defence_technology_feb24/case-studies-iot-defence (дата звернення: 28.04.2025)
15. Case Study: Rugged and Reliable IoT Device Integration - Object Computing. URL: https://objectcomputing.com/client-outcomes/rugged-reliable-iot-device-integration (дата звернення: 30.04.2025)
16. SBIR: Multi-factor Continuous Authentication for Wearable Defense - DARPA. URL: https://www.darpa.mil/research/programs/mcawde (дата звернення: 30.04.2025)
17. Military Leverage of Dedicated IoT Solutions - AFCEA International. URL: https://www.afcea.org/signal-media/technology/military-leverage-dedicated-iot-solutions (дата звернення: 01.05.2025)
18. ConSec: Configuration Security - DARPA. URL: https://www.darpa.mil/research/programs/configuration-security (дата звернення: 03.05.2025)
19. Innovative Internet of Military Things in Modern Defense Strategy - Number Analytics. URL: https://www.numberanalytics.com/blog/innovative-military-iot-modern-defense-strategy (дата звернення: 05.05.2025)
20. IoT and Artificial Intelligence take US military to the next level - Bitdefender. URL: https://www.bitdefender.com/en-us/blog/hotforsecurity/iot-and-artificial-intelligence-take-us-military-to-the-next-level (дата звернення:05.05.2025)
21. Бакун П.В., Жужков Д.І. Інтелектуальні IoT-рішення для задач військового призначення. «Сучасний стан та перспективи розвитку IoT» : VI Науково-техн. конф., м.Київ, 15 квітня 2025 р. (подано до публікації).
22. Бакун П.В., Жужков Д.І. Підходи до побудови надійних IoT-систем у критичних застосуваннях. «Застосування програмного забезпечення в ІКТ» : Всеукр. науково-техн. конф., м.Київ, 24 квітня 2025 р. С.503-506.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра Комп'ютерної інженерії



КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавра

НА ТЕМУ: «ІОТ-РІШЕННЯ ДЛЯ ВІЙСЬКОВИХ ЗАСТОСУВАНЬ»

Виконав студент групи КІД-41
Бакун Павло Вікторович
Керівник дипломної роботи:
Жужков Денис Ігорович
викладач кафедри КІ

Київ – 2025

Мета, об’єкт, предмет дослідження

Мета роботи – спрощення створення та підвищення стійкості розподілених IoT-систем для військових застосувань за рахунок використання принципів автономної роботи, захищеної передачі даних та енергоефективної модульної архітектури

Об’єкт дослідження – процеси побудови та функціонування IoT-систем в умовах бойових дій

Предмет дослідження – апаратно-програмні засоби захищеного зв’язку, протоколи безпровідного обміну, технології автономного живлення та конструктивної захищеності пристроїв

Актуальність роботи

У роботі розглянуто особливості побудови IoT-рішень для військового використання в умовах обмеженого зв’язку, ризику перехоплення даних та складних фізичних впливів. Проведено порівняльний аналіз архітектур цивільних та спеціалізованих IoT-систем за критеріями автономності, захищеності, дальності зв’язку, енергоефективності та вартості впровадження.

Запропоновано логічну архітектуру вузькоспеціалізованих IoT-рішень, засновану на використанні відкритих компонентів (ESP32, LoRa, GPS, автономні джерела живлення) з модульним підходом до конфігурації. Розглянуто можливі алгоритми роботи таких систем з урахуванням бойових умов і вимог до енергозбереження та безпеки. На основі аналізу зроблено висновки щодо доцільності та потенціалу подальшої адаптації відкритих технологій для військових задач без необхідності створення дорогих та складних прототипів.

Використання IoT-рішень у військових задачах



Рис. 1.4 – Основні сфери військового застосування IoT:
розвідка, логістика, моніторинг стану середовища та об’єктів



Рис. 1.7 – Бойові кейси застосування IoT

Типова архітектура військової IoT-системи

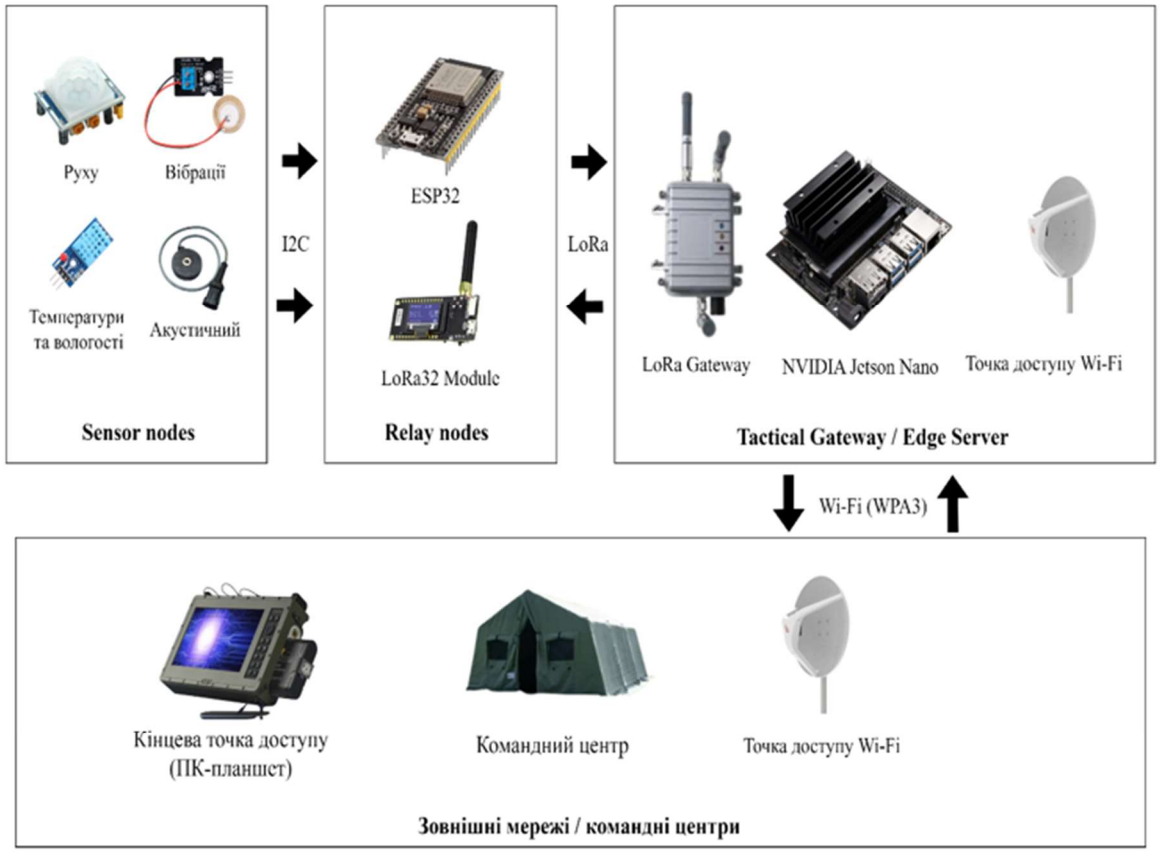


Рис. 2.3 – Узагальнена модульна архітектура IoT-рішення

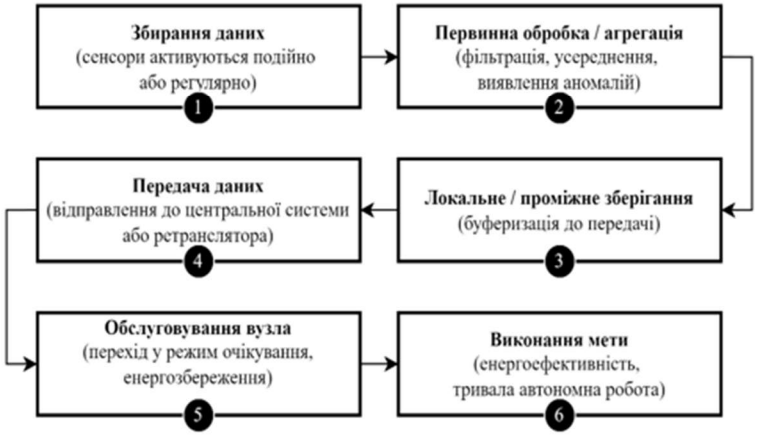


Рис. 2.8 – Етапи функціонування типового IoT-вузла

Приклади реалізації IoT-рішень



Рис. 1.14 – Зовнішній вигляд автономного наземного розвідника Ghost Robotics Q-UGV

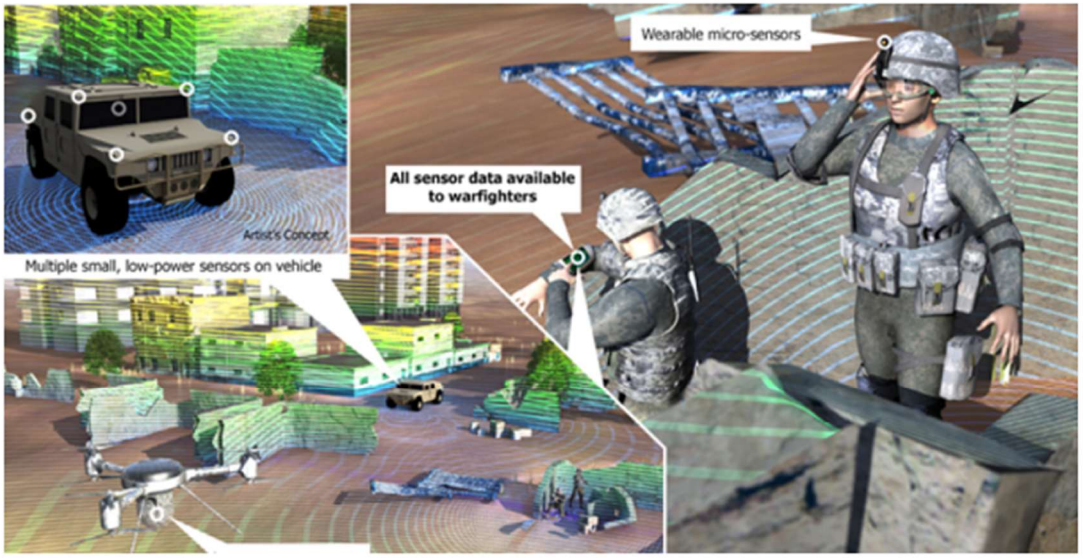


Рис. 1.15 – Візуалізація сенсорної мережі DARPA Tactical IoT [8]

Сценарії застосування в бойових умовах

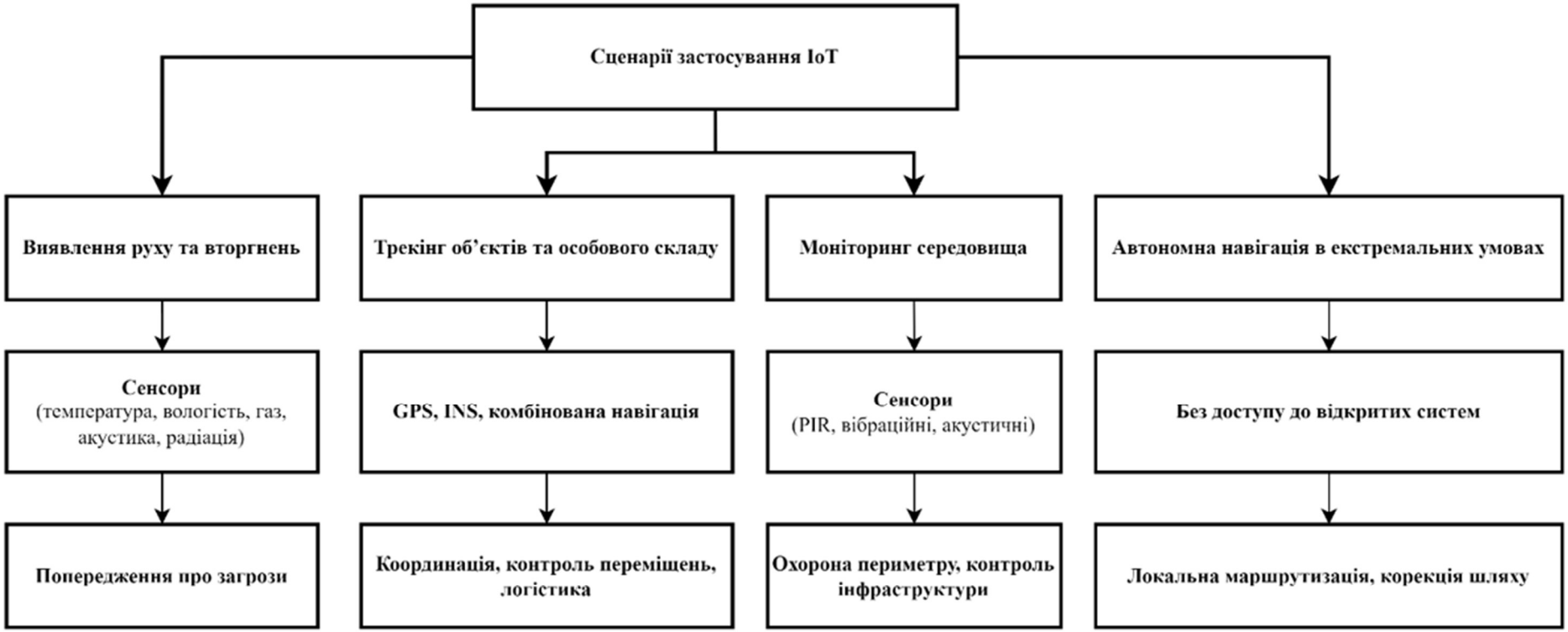


Рис. 2.5 – Сценарії застосування IoT у зоні бойових дій

Алгоритми функціонування IoT систем

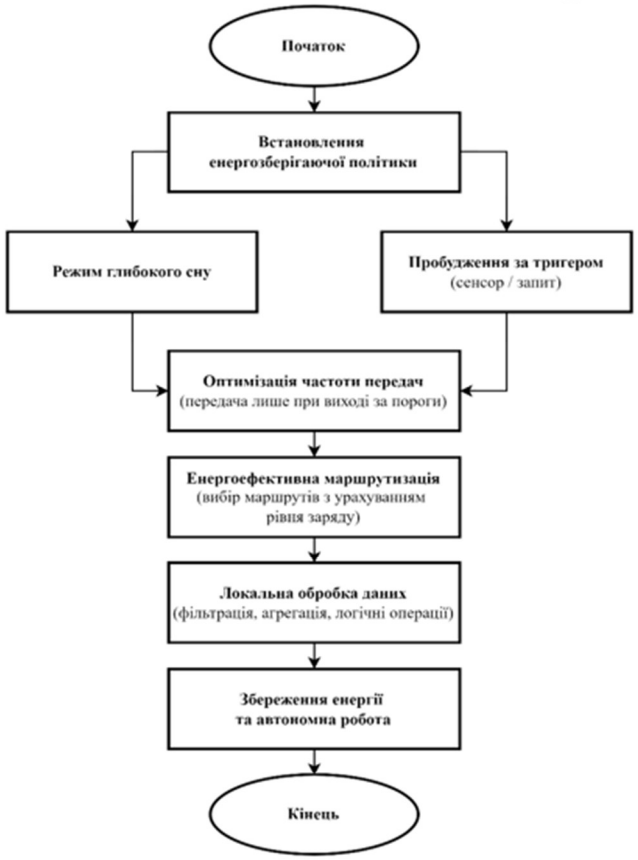


Рис. 2.9 – Алгоритм зниження енергоспоживання у сенсорах

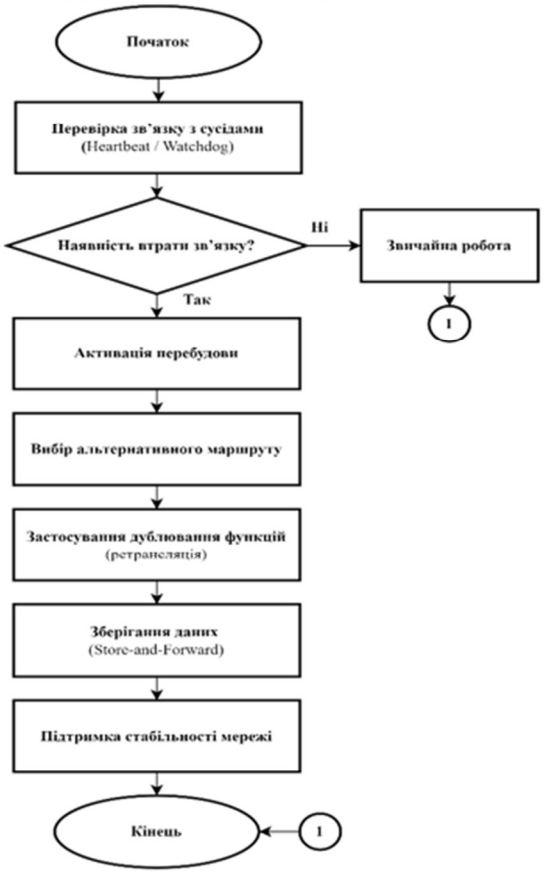


Рис. 2.10 – Алгоритм реагування на втрату зв'язку

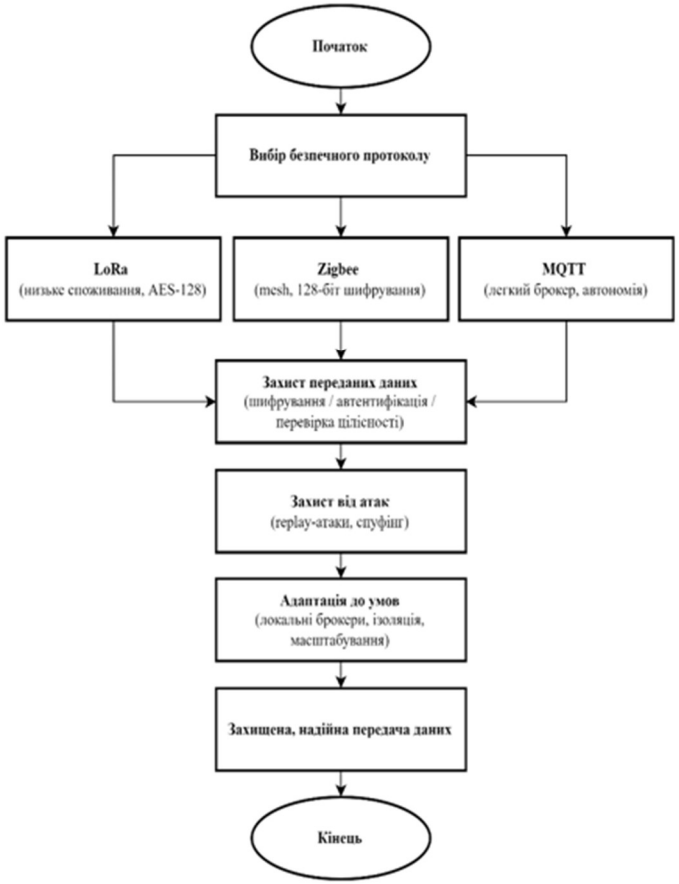


Рис. 2.11 – Алгоритм безпечної передачі даних

Методи підвищення автономності

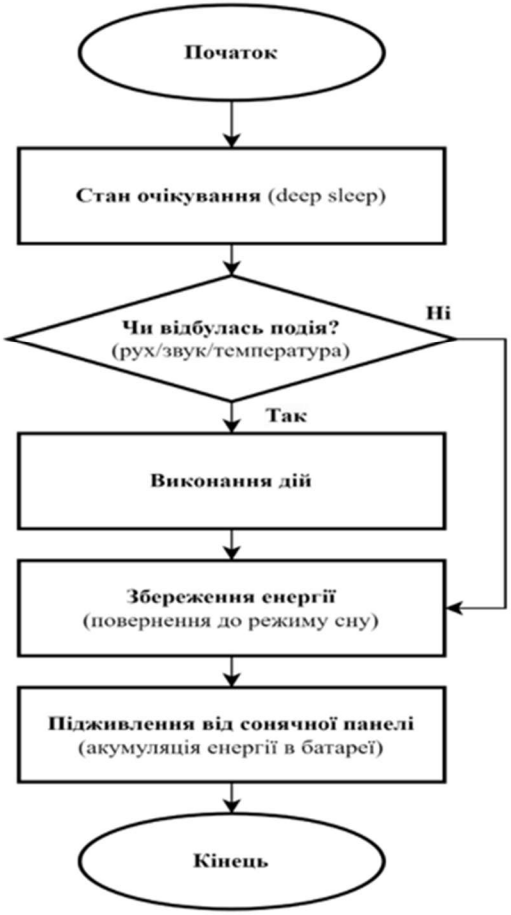


Рис. 3.1 – Метод перемикання енергозберігаючих режимів



Рис. 3.2 – Приклад використання сонячного живлення

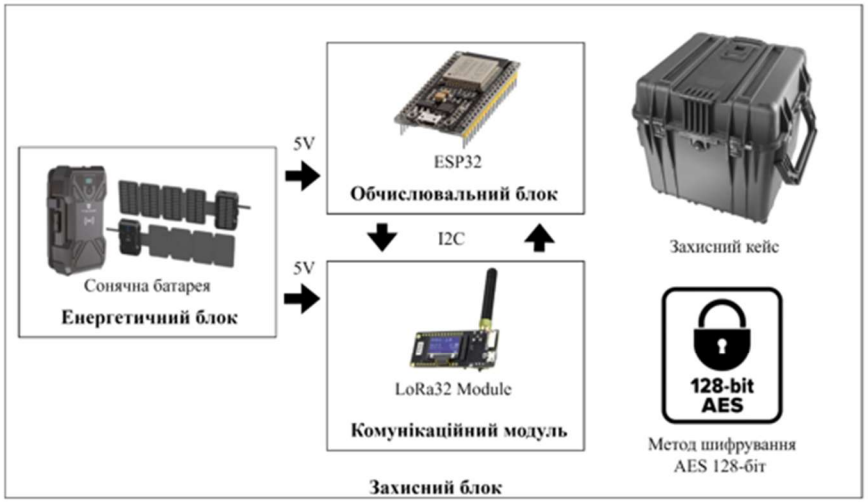


Рис. 2.1 – Типова структура військової IoT-системи

Методи підвищення автономності



Рис. 3.3 – Метод побудови mesh-мережі для збільшення дальності

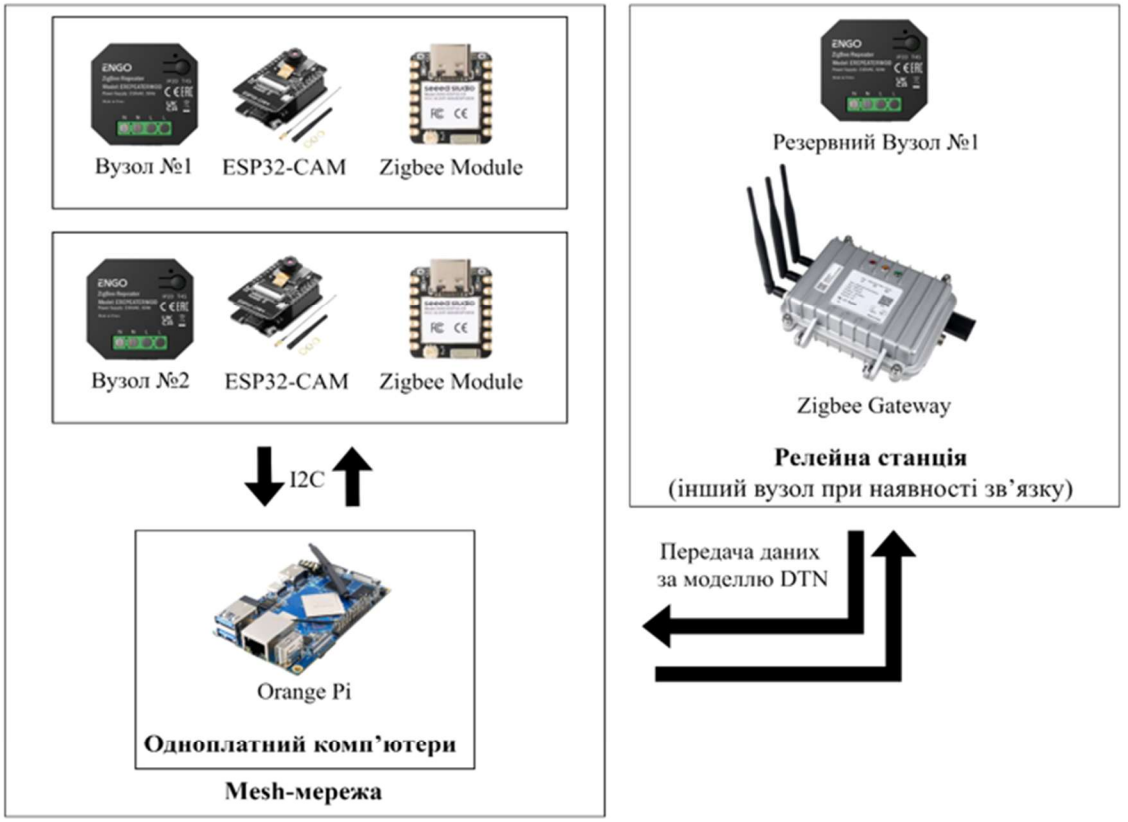


Рис. 2.2 – Децентралізована архітектура в умовах обмеженого зв'язку

Аналіз викликів щодо створення прототипів IoT-рішень

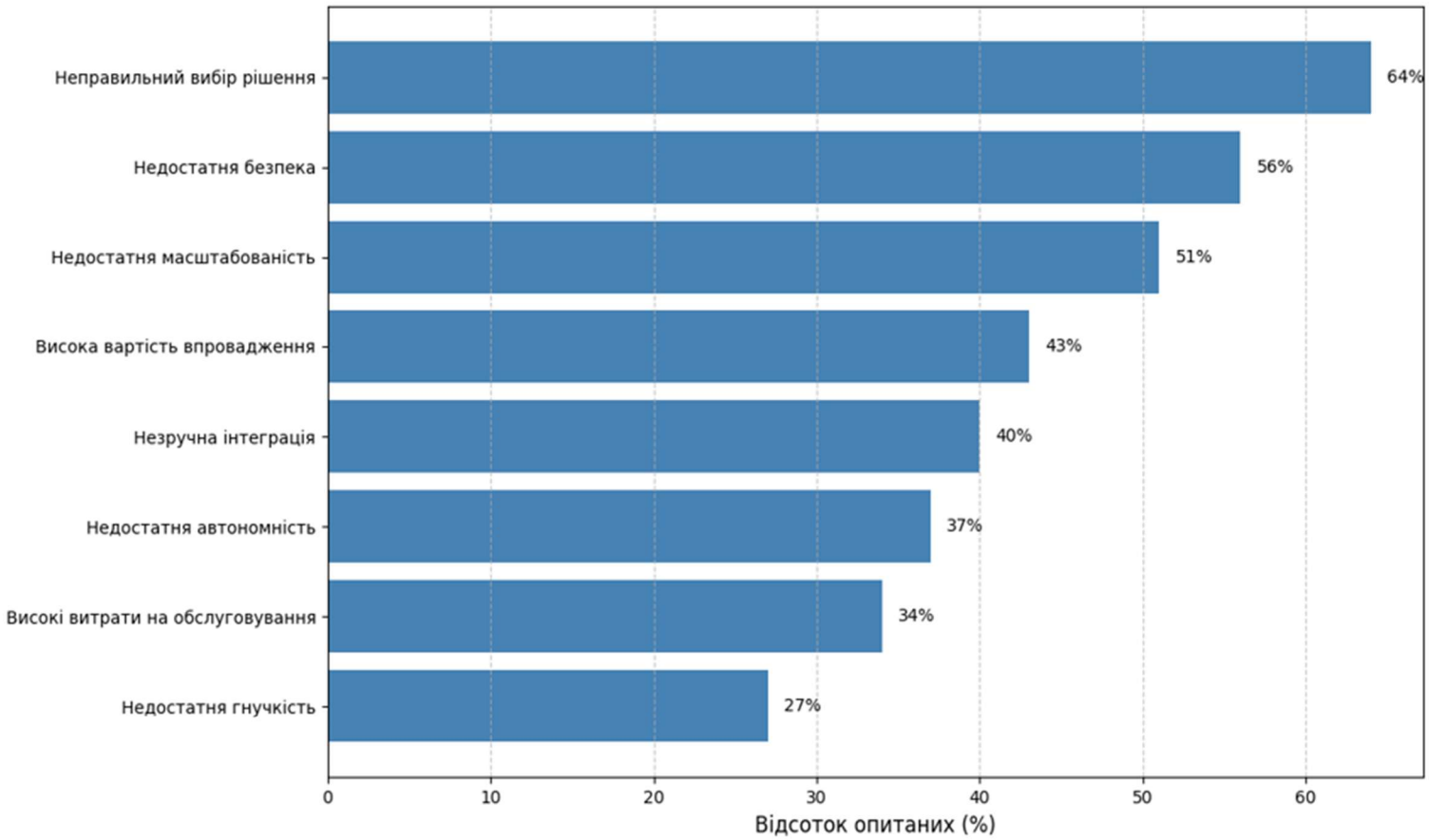


Рис. 3.6 – Основні причини невдач IoT-проєктів при старті

Порівняння з іншими IoT-рішеннями

Табл. 3.2 – Порівняння цивільних та військових IoT-рішень за ключовими критеріями

Критерій	**Цивільні IoT-системи**	**Військові IoT-системи**
Безпека	Базове шифрування або відсутність захисту	**Зашифровані канали (AES, TLS), автентифікація, захист від атак**
Автономність	Працюють від постійного живлення або акумулятора на 1–2 доби	**Тривала автономна робота (до кількох тижнів), енергозберігаючі режими**
Дальність зв'язку	Обмежена (Wi-Fi, Bluetooth — до 100 м)	**Дальнє покриття (LoRa, mesh, УКХ/КХ — до кількох км)**
Енергоефективність	Не є пріоритетом, рідко застосовується оптимізація	**Максимальна економія енергії, оптимізація частоти обміну**
Механічна стійкість	Вразливі до пилу, вологи, ударів	**Пиловологозахищені, витривалі до механічних впливів**
Інфраструктурна залежність	Потребують стабільного інтернет-зв'язку або мобільної мережі	**Працюють у відриві від інфраструктури, підтримують буферизацію даних**
Вартість і доступність	Низька вартість, висока доступність на ринку	**Вища вартість, обмежений доступ, залежність від постачальників**
Можливість адаптації	Часто закриті системи, обмежена конфігурація	**Відкриті або гнучкі рішення з можливістю модифікації**

Висновки

У роботі досліджено архітектурні підходи до побудови військових IoT-систем на основі відкритих рішень із фокусом на автономність, надійність і адаптивність. Запропонована модульна архітектура передбачає використання вузлів-ретрансляторів із можливістю підключення різних сенсорів і засобів зв'язку, що забезпечує функціонування мережі без централізованої інфраструктури. Особливу увагу приділено енергоефективності, алгоритмам безпечної передачі даних, реагування на втрату зв'язку та використанню mesh-топологій для підвищення стійкості до відмов.

Програмна частина розглядалася теоретично: проаналізовано можливості MQTT-брокерів, Node-RED і Home Assistant у децентралізованих умовах. Порівняльний аналіз показав, що наявні комерційні рішення часто не відповідають військовим вимогам, тоді як запропонований підхід демонструє потенціал до адаптації, захисту та стабільної роботи в умовах тактичної нестабільності.

Публікації та апробація роботи

1. Бакун П.В., Жужков Д.І. Інтелектуальні IoT-рішення для задач військового призначення. «Сучасний стан та перспективи розвитку IoT» : VI Науково-техн. конф., м.Київ, 15 квітня 2025 р. (подано до публікації).
2. Бакун П.В., Жужков Д.І. Підходи до побудови надійних IoT-систем у критичних застосуваннях. «Застосування програмного забезпечення в ІКТ» : Всеукр. науково-техн. конф., м.Київ, 24 квітня 2025 р. С.503-506.