Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікаціїі*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти *другий (магістерський)*

Дослідження засобів безпеки в мережах IoT

(тема)

Виконав:
здобувач 2 року навчання,
групи *ІМІм-23-1*
Поддельський В.М.

Спеціальність *172 Електронні комунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *Освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *доц., к.т.н. Чеботарьова Д.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2025 р.

Не містить відомостей, заборонених до відкритого публікування

Здобувач _____ *Поддельський В.М.*
(підпис) (прізвище та ініціали)

Керівник _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Електронні комунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри ІМІ_____
(підпис)
“____” _____2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Поддельському Владиславу Максимовичу*
(прізвище, ім’я, по батькові)

1. Тема роботи *Дослідження засобів безпеки в мережах IoT*

затверджені наказом університету від *28 жовтня 2024* року № *1148 Ст*

2. Термін подання студентом роботи до екзаменаційної комісії *20 січня 2025 р.*

3. Вихідні дані до роботи

Проаналізувати стан та тенденції розвітку IoT в світі та в Україні. Дослідити особливості та принципи функціонування мереж IoT. Виконати порівняльний аналіз сучасних телекомунікаційних технологій для мереж IoT. Проаналізувати проблеми безпеки в мережах IoT, зокрема загрози та вразливості в IoT. Дослідити засоби безпеки в мережах IoT. Виконати порівняльний аналіз існуючих платформ безпеки IoT. Запропонувати ефективні рішення для захисту мереж IoT та сформулювати рекомендації для організації та підтримки високого рівня безпеки.

4. Перелік питань, що потрібно опрацювати в роботі

Вступ.
1. Аналіз стану та розвитку IoT.
2. Особливості та принципи функціонування мереж IoT.
3. Аналіз проблем безпеки в IoT.
4. Рішення для захисту мереж IoT.
Висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *Слайди у форматі Power Point (назва, мета і задачі роботи, аналіз стану та розвитку IoT, особливості IoT в Україні, концепція та принципи функціонування IoT, аналіз сучасних технологій зв'язку для мереж IoT, переваги та проблеми IoT, основні проблемні області безпеки та вразливості IoT, загрози та атаки мереж IoT, аналіз засобів захисту мереж Інтернету речей, рекомендації дощо захисту мереж IoT, порівняльний аналіз сучасних платформ безпеки IoT, рішення для забезпечення безпеки IoT методом життєвого циклу, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів атестаційної роботи	Строк виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ*	*28.10.24*	*виконано*
2	*Підбір літератури за темою роботи*	*28.10 - 02.11.24*	*виконано*
3	*Виконання розділу 1*	*03.11 - 19.11.24*	*виконано*
4	*Виконання розділу 2*	*20.12 – 02.12.24*	*виконано*
5	*Виконання розділу 3*	*03.12 – 19.12.24*	*виконано*
6	*Виконання розділу 4*	*20.12 - 02.01.25*	*виконано*
7	*Оформлення пояснювальної записки*	*03.12 – 11.01.25*	*виконано*
8	*Оформлення презентаційного матеріалу,*		
	підготовка до захисту у ЕК	*12.01 - 20.01.25*	*виконано*

Дата видачі завдання *28.10.2024 р.*

Здобувач _____ *Поддельський В.М.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка 76 с., 16 рис., 5 табл., 31 джерело, 2 додатки.

Об'єкт дослідження – безпека в мережах IoT.

Мета роботи – дослідити сучасні засоби безпеки в мережах IoT, запропонувати ефективні рішення та сформулювати рекомендації для захисту мереж IoT.

Результати – у роботі проведено аналіз актуального стану технології IoT, у тому числі виділені етапи розвитку технології Інтернету речей та особливості впровадження технології в Україні. Досліджено принципи функціонування мереж IoT та виведені основні переваги та проблеми. Детально вивчені вразливості та види атак, які загрожують безпечній роботі мереж Інтернету речей. Також проаналізовано існуючі засоби захисту мереж IoT та виділені загальні рекомендації щодо їх захисту. У якості ефективного рішення для захисту мереж IoT запропоновано комплексний захист на основі використання методу життєвих циклів IoT.

БЕЗПЕКА, IoT, МЕРЕЖА, ЗАХИСТ, ЗАГРОЗА, ВРАЗЛИВІСТЬ, ПРИСТРІЙ, ТЕХНОЛОГІЯ, МОНІТОРИНГ

THE ABSTRACT

Explanatory note: 76 p., 16 fig., 5 tabl., 31 sources, 2 app.

The object of study is security of IoT networks.

The purpose of the work is to investigate modern security tools in IoT networks, propose effective solutions and formulate recommendations for protecting IoT networks.

Results - the work analyses the current state of IoT technology, including the stages of development of the Internet of Things technology and the peculiarities of technology implementation in Ukraine. The principles of functioning of IoT networks are investigated and the main advantages and problems are identified. Vulnerabilities and types of attacks that threaten the secure operation of IoT networks are studied in detail. The existing means of protecting IoT networks are also analysed and general recommendations for their protection are highlighted. As an effective solution for protecting IoT networks, the proposes a comprehensive protection based on the IoT life cycle method.

SECURITY, IoT, NETWORK, PROTECTION, THREAT, VULNERABILITY, DEVICE, TECHNOLOGY, MONITORING

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) – стандарт взаємодії по протоколу IPv6 для малопотужних пристроїв;

AMQP (Advanced Message Queuing Protocol) – протокол для передачі повідомлень між компонентами системи;

API (Application Programming Interface) – інтерфейс програмування застосунків;

AR (Augmented Reality) – доповнена реальність;

BLE (Bluetooth Low Energy) – технологія Bluetooth з низьким енергоспоживанням;

CoAP (Constrained Application Protocol) – протокол обмеженого застосування;

DoS/DDoS ((Distributed) Denial-of-Service Attack) – кібератака типу «відмова в обслуговуванні»;

HSM (Hardware Security Modules) – апаратні модулі безпеки;

HTTP/2 (HyperText Transfer Protocol/2) – друга версія мережного протоколу HTTP;

IAM (Identity and Access Management) – система керування ідентичністю й доступом;

IDC (International Data Corporation) – міжнародна дослідницька та консалтингова компанія;

IIoT (Industrial Internet of Things) – промисловий Інтернет речей;

IPS/IDS (Intrusion Prevention System / Intrusion Detection System) – системи виявлення та попередження вторгнень;

IP-адреса (Internet Protocol address) – числовий ідентифікатор мережного рівня;

LoRaWAN (Long Range Wide Area Network) – бездротовий мережний протокол;

LPWAN (Low-power Wide-area Network) – бездротова технологія передачі невеликих за обсягом даних;

MAC-адреса (Media Access Control) – унікальний ідентифікатор для устаткування в комп'ютерних мережах;

MDM (Mobile Device Management) – управління мобільними пристроями;

MitM (Man-In-The-Middle) – вид кібератаки типу «людина посередині»;

MQTT (Message Queue Telemetry Transport) – спрощений мережний протокол;

NAC (Network Access Control) – контроль доступу до мережі;

NB-IoT (Narrow Band Internet of Things) – стандарт стільникового зв'язку для пристроїв з низьким енергоспоживанням;

NGFW (Next-Generation Firewall) – міжмережний екран для фільтра трафіку;

RFID (Radio Frequency Identification) – технологія автоматичної ідентифікації;

SIEM (Security Information and Event Management) – інформація про безпеку та управління подіями;

SQL-ін'єкції – спосіб злому сайтів та програм, що працюють з базами даних;

UBA (User Behavior Analytics) – аналіз поведінки користувачів;

UDP (User Datagram Protocol) – протокол користувальницьких датаграм;

Wi-Fi (Wireless Fidelity) – технологія бездротової локальної мережі;

XSS (Cross-Site Scripting) – підтип атаки на веб-системи;

IoT (Internet of Things) – інтернет речей;

ІШІ – штучний інтелект.

ВСТУП

Швидкість розвитку технологій, яка стрімко збільшилася у світі протягом останніх десятиліть, поставила перед суспільством ряд непростих та хвилюючих питань. У нестримному бажанні спростити та автоматизувати власний побут і буденні заняття, людство розпочало нову інформаційно-технологічну гонку. Її передумовами були потреби в збереженні часу, економії ресурсів, необхідність у створенні зручного простору, куди могли бути інтегровані усі необхідні системи для повноцінного функціонування як окремої людини, так і групи людей, для забезпечення комфортного життя та можливостей зосереджуватися на головному, маючи змогу не відволікатися на дрібні побутові справи. Одним із визначних рушіїв четвертої промислової революції стало впровадження цифрової технології – Інтернету речей.

Інтернет речей (Internet of Things, IoT) – технологія, що трансформує процеси взаємодії між системами, оптимізуючи та автоматизуючи їх в одному цифровому просторі. IoT сприяє підвищенню ефективності виробничих процесів та спрощує процес побуту людини. Створення подібного простору дозволило людству впроваджувати технології «розумних будинків», використовувати IoT у сільськогосподарський діяльності, промисловості, логістиці, медицині, що розширило можливості людства у розвитку цих сфер діяльності.

За прогнозами міжнародної дослідницької компанії IDC, до 2026 року глобальні інвестиції в IoT складуть близько 1 трильйона доларів США [1].

Проте, враховуючи швидкість розвитку IoT та стрімкість її впровадження, перед технологічним світом постає нове складне питання – безпека. Ризики, що зростають, пов’язані з особливостями архітектури IoT-мереж, які включають в себе велику кількість розподільних пристроїв, адже чим їх більше, тим складніше захистити цифрові дані. Вразливості IoT-системи можуть мати серйозні наслідки, наприклад, такі як порушення приватності кінцевого користувача, відкриття його фінансових таємниць або навіть загрожувати життю людей, якщо мережі IoT використовуються для процесів життєзабезпечення або на об’єктах критичної інфраструктури.

Дослідження показали, що у 2023 році кількість кібератак на пристрої Інтернету речей збільшилися на 37%, а 98% трафіку між пристроями не має

належного захисту, що може призвести до того, що у наступні роки більшість IoT-пристроїв будуть піддаватися серйозним кібератакам через відсутність регулярних оновлень [2].

Актуальність даної роботи полягає у дослідженні засобів безпеки в мережах IoT, зокрема ризиків, яким можуть піддаватися мережі Інтернету речей, та методів захисту цих мереж.

1 АНАЛІЗ СТАНУ ТА РОЗВИТКУ IoT

1.1 Еволюція IoT

Інтернет речей – одна із найбільш перспективних технологій сучасності, що поклала початок четвертої промислової революції. Технологія, що стрімко розвивається, трансформуючи різноманітні сфери людської діяльності. Концепція мережі IoT полягає у взаємопов'язаній між собою системі пристроїв, із вбудованим програмним забезпеченням та модулями, що забезпечують взаємодію між ними та зовнішнім середовищем. IoT-мережа спрощує економічні, суспільні та побутові процеси, виключаючи з «ланцюга» необхідність в них участі людини.

Інтернет речей, як концепцію, було запропоновано у 1999 р. засновником дослідницької групи Auto-ID Center Массачусетського технологічного інституту Кевіном Ештоном під час його презентації для компанії Procter & Gamble [3]. В наш час мережі IoT подолали значний шлях розвитку та трансформувалися від ідеї до складної системи взаємопов'язаних пристроїв, що автономно функціонують між собою та навколишнім середовищем.

Історія розвитку IoT-технології бере свій початок від ідеї створення об'єднаної мережі фізичних об'єктів, що з'явилася завдяки винаходу першого електромагнітного телеграфу у 1832 році, який поклав початок створення глобальної мережі зв'язку.

Процес еволюції IoT-мереж представлено в табл. 1.1.

Проте, перший інтернет-пристрій – тостер, під'єднаний до мережі, який міг дистанційно вмикатися та вимикатися - експериментальний винахід Джона Ромкі у 1990-му році, можна вважати справжнім початком еволюції IoT-мереж [4]. Експеримент Ромкі сприйняли як жарт, але вчений першим продемонстрував можливості підключення фізичних об'єктів до інтернету.

Подальший розвиток IoT-мереж протягом наступних десятиліть прискорювався завдяки деяким технологічним досягненням. Ключовим внеском у процвітання Інтернету речей було розробка мініатюрних електронних компонентів та зниження їхньої собівартості на ринку, адже поява ефективних, проте недорогих процесорів, які могли обробляти великий обсяг

інформації, суттєво розширило можливості для подальшого початку масового виробництва «розумних» пристроїв.

Таблиця 1.1 – Етапи еволюції IoT-мереж

№	Період	Зміст
1	1960 – 1999 роки	Етап характеризується появою ідей та перших автоматизованих пристроїв
2	2000 – 2010 роки	Відбувається процес масштабування IoT, з'являються перші «розумні» пристрої
3	2010 – 2020 роки	Відбувається активна інтеграція із хмарними технологіями та з'являються перші «розумні» міста
4	2020 – 2025 роки	Відбувається процес злиття IoT-мереж з технологіями штучного інтелекту, 5G-зв'язку та активно розширюються сфери подальшого застосування технології
5	Після 2025 р.	Етап, що прогнозується орієнтовно з 2030-го року характеризується появою повноцінних інтелектуальних автономних IoT-систем, цифрових двійників та процесом масштабування технології до глобальних мереж

Технологічним проривом у процесі еволюції IoT став паралельний розвиток безпровідних технологій, зокрема, Wi-Fi, Bluetooth та ZigBee, які змогли забезпечити необхідну структуру з'єднання між пристроями.

У 2010-х роках кількість підключених пристроїв росла за експонентою, розширюючи сфери можливого застосування. У широкий загал випускалися перші масові продукти: термостати Nest та системи безпеки, які у подальшому використовувалися як перші IoT-пристрої систем «розумного» будинку. Одночасно з тим, такі сфери як промисловість, сільське господарство, охорона здоров'я та логістика також почали активно застосовувати IoT-технології з

метою оптимізації власних виробничих процесів, моніторингу стану здоров’я та керуванням транспортних маршрутів.

У 2012 році створення протоколу IPv6, впроваджений для розширення адресного простору глобальної мережі, був вирішенням проблеми обмеженої кількості IP-адрес, що суттєво загальмовувала розвиток IoT. Застосування цього протоколу дає можливість присвоювати унікальні IP-адреси великій кількості пристроїв, що дозволило розгорнути масштабне застосування IoT-мереж [5].

Розробка хмарних технологій відіграла одну з ключових ролей в еволюції IoT-технології, адже хмарні сховища та платформи створили необхідний простір для збереження і обробки величезних обсягів різноманітної інформації, що продукувати пристрої Інтернету речей. Інтеграція технологій штучного інтелекту та машинного навчання розширило можливості аналізу інформації та відкрило шлях для процесу прийняття автономних рішень. Впровадження цих технологічних рішень поклало початок сучасному етапу еволюції IoT-мереж, який характеризується розвитком мереж від простого збору та аналізу даних до структурних інтелектуальних систем. Завдяки цьому процесу IoT-пристрої стають автономними одиницями мережі, а інтеграція в них парадигми крайових обчислень (англ. edge computing) дозволяє їм обробляти дані безпосередньо на пристроях, що розвантажує мережу та прискорює реакцію системи на змін.

Сучасний Інтернет речей – це цільна система, що включає в себе програмне забезпечення, розподільні пристрої, комунікаційні модулі, сенсори та процесори обробки даних. Особливу роль у функціонуванні IoT-мережі відіграють сенсори, які збирають різноманітну інформацію як внутрішнього, так і зовнішнього середовища: освітленість, рух, тиск вологість, температуру, тощо, а потім передають зібрані дані через комунікаційні модулі до процесорів обробки даних, де вони аналізуються, щоб зрештою використатись в якості сигналу для актуаторів – пристроїв, які мають фізичний вплив на середовище.

Розвиток IoT-систем відбувається в умовах прогресу інформаційних технологій, і наразі системи Інтернету речей у своїй роботі використовують різноманітні стандарти та протоколи. Впровадження єдиних протоколів та стандартів позитивно впливає на інтеграцію пристроїв, забезпечуючи їх сумісність. Зокрема, мережі IoT активно інтегруються з технологіями штучного інтелекту, що дозволяє досліджувати та впроваджувати системи, які не тільки

вміють збирати та аналізувати дані, а й враховувати результат і приймати автономні рішення.

Крім того, важливою частиною розвитку IoT полягає й у зміні підходу до безпеки, який з часом став однім із ключових аспектів при розробці та впровадженні нових технологій Інтернету речей. Наразі активно розробляються нові безпекові протоколи, зокрема, додаткові методи автентифікації та шифрування.

Наразі технології Інтернету речей інтегрується з іншими передовими технологіями, наприклад, з блокчейном, що відкриває шлях до розробки децентралізованих мережних пристроїв з підвищеним рівнем безпеки та прозорістю функціонування. Крім того, розвиток 5G-технології створює необхідну інфраструктуру для реалізації високої пропускної здатності з мінімальними затримками контакту.

Сучасні системи IoT дедалі частіше впроваджуються у різні сфери промисловості та інформаційно-комунікаційних компаній, оптимізуючи виробничі процеси. Для ефективного функціонування будь-якого процесу, штучний інтелект у IoT-просторі отримує велику кількість корисної інформації, яку обробляє через згенеровані IoT-пристроями масиви даних, та може автономно приймати рішення та керувати ними.

1.2 Актуальний стан та тенденції розвитку IoT у світі

На теперішній час Інтернет речей представляє собою технологічну галузь, що динамічно розвивається вже декілька десятиліть. Сьогодні IoT-ринок є надзвичайно успішним, а кількість підключених IoT-пристроїв стабільно зростає [6], що видно з рис 1.1. Істотна кількість застосувань технології Інтернету речей викликає суттєві зміни більшості аспектів суспільного життя та стану економіки і позитивно впливає них.

Наразі стан IoT-технології можна охарактеризувати високим рівнем інтеграції у різні галузі. Актуальні сфери застосування IoT-пристроїв [7] наведено на рис.1.2. Зокрема, однією з тенденцій розвитку є промисловість – галузь, що найбільш активно впроваджує IoT-системи, створюючи новий підхід до процедур та процесів виробництва.

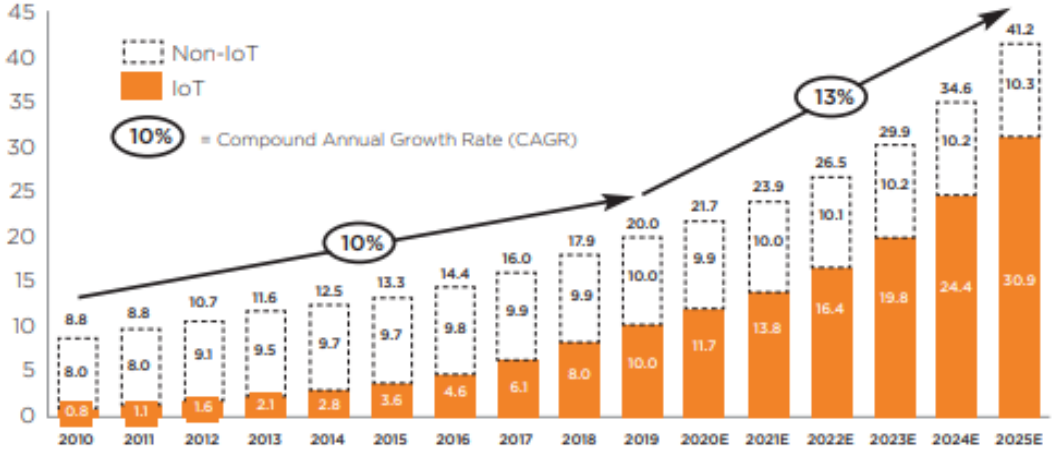

Рисунок 1.1 – Загальна кількість підключень пристроїв, включаючи не-Інтернет речей

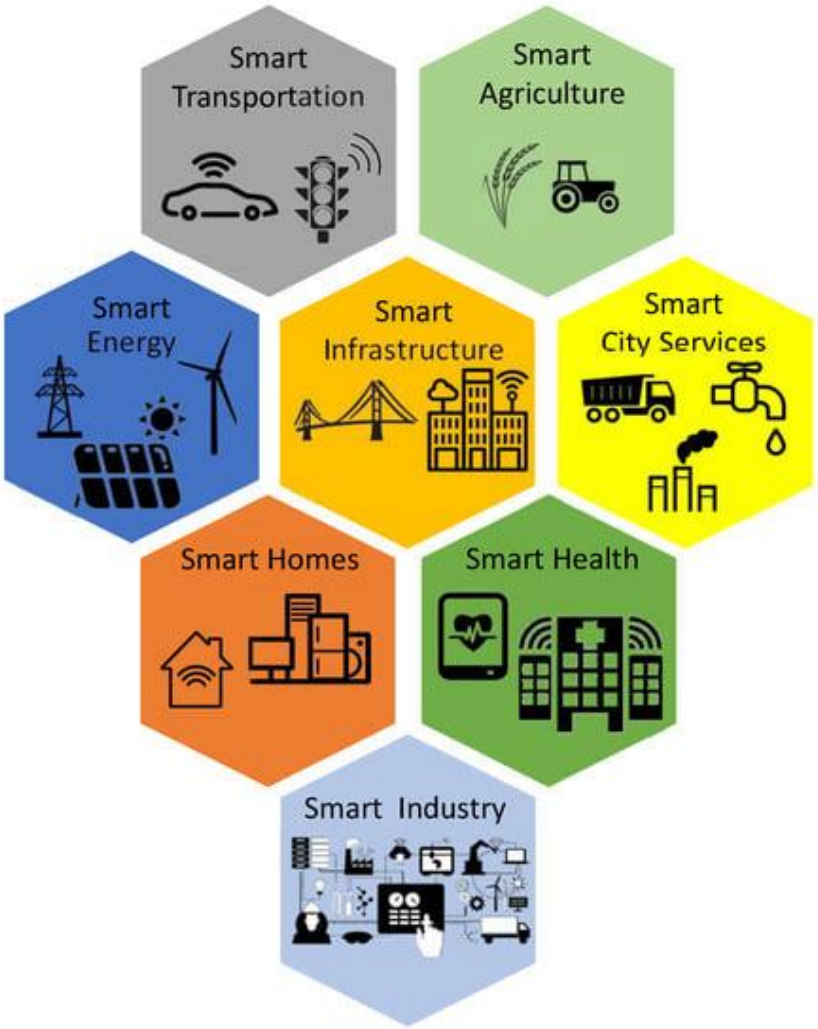

Рисунок 1.2 – Актуальні сфери застосування Інтернету речей

Промисловий Інтернет речей (Industrial IoT, IIoT) – один із найперспективніших напрямків розвитку IoT. Індустріальні IoT-системи активно використовуються для автоматизації та оптимізації процесів виробництва, моніторингу його етапів, превентивного обслуговування обладнання. Ці системи підвищують ефективність виробництва, дозволяють знизити витрати на обслуговування обладнання та мінімізувати ризики виникнення позаштатних ситуацій. Найбільш корисною функцією є моніторинг обладнання та можливість передбачення його потенційних несправностей, що позитивно впливає на динаміку попередження та реагування на аварійні ситуації.

Застосування підприємствами IIoT (промислового Інтернету речей) знижує витрати виробництва, поліпшує якість обслуговування обладнання та прискорює виробничі процеси. За останніми прогнозами експертів, інтеграція IIoT-систем потенціально підвищить ефективність виробництв не менше ніж на 30% [8].

IIoT-системи також значною мірою слугують базою для розроблення та впровадження концепцій «розумних» міст, де використовуються у логістичних цілях, для моніторингу екологічної ситуації, регулюванні енергоспоживання та забезпеченні громадського правопорядку і безпеки.

Дедалі більше міст у різних куточках світу впроваджують у свій повсякденний ритм мегаполісу IoT-технології, використовуючи їх для керування транспортом та логістикою, в енергетичному секторі, переробці і утилізації відходів тощо (рис. 1.3). Подібні автоматизовані системи поліпшують якість життя містян та стають помічником для туристів, знижають кількість викидів і зменшують негативний вплив на екологію, оптимізуючи кількість використання корисних копалин та ресурсів.

Інтеграція технологій штучного інтелекту, розвиток edge computing, 5G-мережі відкривають шлях для подальшого розвитку IoT. Ці технології дозволяють створювати більш інтелектуальні систем зі зниженим рівнем затримок та зменшеним навантаженням, які мають високу пропускну здатність і можливість підключення великої кількості пристроїв, що дають потужний поштовх для розвитку у сферах транспорту, промисловості, медицині.

Не зважаючи на суттєві перспективи розвитку IoT-мереж, що пов’язані з їхньою подальшою інтеграцією у все більшу кількість сфер суспільного,

промислового та побутового життя людей, питання безпеки не врачають актуальності. У подальшому очікується зростання кількості підключених до мереж пристроїв, впровадження нових технологій та сфер їх застосування, що автоматично створить велику кількість нових вразливостей для IoT-систем, якими можуть скористатися зловмисники.

Рисунок 1.3 – Приклади використання IoT технологій в різних галузях

Питання безпеки та стандартизації IoT наразі є найбільш важливим у контексті розвитку технології. Єдині протоколи та стандарти роботи, над якими активно ведуться роботи, забезпечать необхідний рівень сумісності між пристроями від різних виробників та спростить їхню експлуатацію. Розробка та ефективне впровадження блокчейну або криптографії суттєво підвищує захищеність вразливих блоків системи. Крім того, відбувається розробка інших передових технологій захисту.

Технологія Інтернету речей продовжує свій активний розвиток, дедалі частіше знаходячи собі застосування у різноманітних аспектах життя людства. Постійне розширення сфер використання, вдосконалення технології та розрішення нових викликів і питань створюють сприятливі умови для зросту подальшого впливу IoT на економіку та суспільство. Наразі більшість досліджень та апгрейдів Інтернету речей зосереджені на питаннях безпеки, подоланнях обмежень використання нових розробок і створення більш ефективних технологій.

1.3 Особливості Інтернету речей в Україні

Особливості розвитку Інтернету речей в Україні здебільшого зумовлені економічними, соціальними та технологічними факторами, які мають суттєвий вплив на український ринок IoT. Не дивлячись на війну у країні та зниження економічних темпів, IoT-сфера демонструє стабільний ріст. Наприклад, мобільний оператор «Vodafone Україна», який є надавачем послуг для впровадження IoT-рішень повідомив, що у 2024 році компанія отримала близко 1 млрд грн прибутку за надання послуг IoT та Big Data, а кількість активованих IoT sim-карт Vodafone за останні чотири роки вирісло втричі [9].

Визначна роль у впровадженні IoT у сфери суспільно-економічного життя України відведена промисловому сектору. Так, з метою модернізації застарілого обладнання та оптимізації виробничих процесів, великі промислові підприємства, зокрема металургійні та хімічні, активно застосовують IoT-системи. Це приводить до підвищення ефективності та конкурентоспроможності на міжнародному промисловому ринку.

Значну частку економіки України займає аграрний сектор, завдяки якому країна є провідним експортером деяких видів сільськогосподарської продукції.

Тому модернізація та оптимізація сільського господарства є пріоритетним завданням. Зокрема, аграрні компанії країни впроваджують системи точного землеробства, автоматизовані системи поливу та моніторинг стану посівів. Український виробник та найбільший експортер соняшникової олії в Україні, компанія «Кернел» (Kernel), на частку якої припадає 15% від світового експорту соняшникової олії, застосовує системи GPS-моніторингу власної техніки з використанням IoT-технологій. Окрім того, користується IoT-датчиками для контролю вологості ґрунту, «розумною» системою поливу полів, а для спостерігання за посівами та з метою контролю їхнього росту – дрони [10]. IoT-рішення оптимізації власного виробництва дозволяють аграрним підприємствам підвищити якість та кількість продукції, знизити виробничу вартість та оптимізувати процеси контролю продукції на усіх етапах виробництва.

Український енергетичний сектор також є користувачем Інтернету речей, зокрема, застосування «розумних» лічильників, систем моніторингу енергоспоживання та управління мережами енергозабезпечення підвищують ефективність використання енергетичних ресурсів. Впровадження IoT-рішень в енергосектор також значно підвищує енергетичну безпеку в країні, особливо під час повномасштабної війни росії проти України, однією з цілей якої є знищення енергетики.

Однією з важливих особливостей розвитку Інтернету речей в Україні є велика кількість інноваційних проектів та ріст кількості стартапів. Згідно з звітом компанії Dealroom, що спеціалізується на керуваннями базами даних, на весну 2024 року український ринок стартапів оцінюється у 28 мільярдів євро, що ставить Україну разом із Польщею та Естонією у трійку найбільших стартап-індустрій Центральної та Східної Європи [11].

В Україні розробляють визначні та унікальні IoT-рішення, які успішно знаходять своє застосування у різноманітних сферах. У тому числі IoT-стартапи, які виходять на глобальну арену, залучаючи іноземні інвестиції та отримуючи визнання міжнародного рівня. Наприклад, фахівець із розробок програмного ПЗ, Андрій Колпаков, у 2023 році заснував стартап «Generect» і разом із командою створив платформу для маркетингових агенцій, яка автоматизує процеси створення контенту для свої клієнтів, тим самим заощаджуючи компаніям час та ресурси. Компанія уклала угоду на 1,8 мільйона

доларів США на конференції TechChill 2024, і її послугами користуються великі маркетингові агенції США, зокрема, BrightWave, LeadSync, MarVista Networks тощо [12, 13].

Крім того, технології IoTв Україні активно розвивають концепцію «розумних» міст. Великі міста, такі як Київ, Харків, Вінниця, Львів застосовують елементи «розумних» міст, у тому числі, системи управління транспортом, «інтелектуальне» освітлення, впроваджують концепцію «безпечного» міста, моніторинг навколишнього середовища, проте, порівняно з іншими країнами, масштаб подібних рішень значно обмежений [14].

У військових цілях IoT також значною мірою розвивається, адже воєнний стан в країні створив нові напрями застосування технології Інтернету речей. Наразі активно ведуться роботи щодо застосування IoT-рішень для моніторингу стану критичної інфраструктури, систем раннього попередження обстрілів, забезпечення безпеки. Також розробляються технології для відновлення пошкодженої інфраструктури та моніторингу стану пошкоджених будівель.

Не зважаючи на позитивну динаміку розвитку Інтернет речей в Україні, галузь постійно стикається з різними проблемами (рис.1.4). Повномасштабна війна в країні має значний вплив на соціально-економічні аспекти життя українців, кардинально змінивши звичний стан як суспільства, так й бізнесу, медицини, промисловості тощо. Економічне зниження, яке превалює у країні, негативно відображається й на розвитку IoT в Україні.

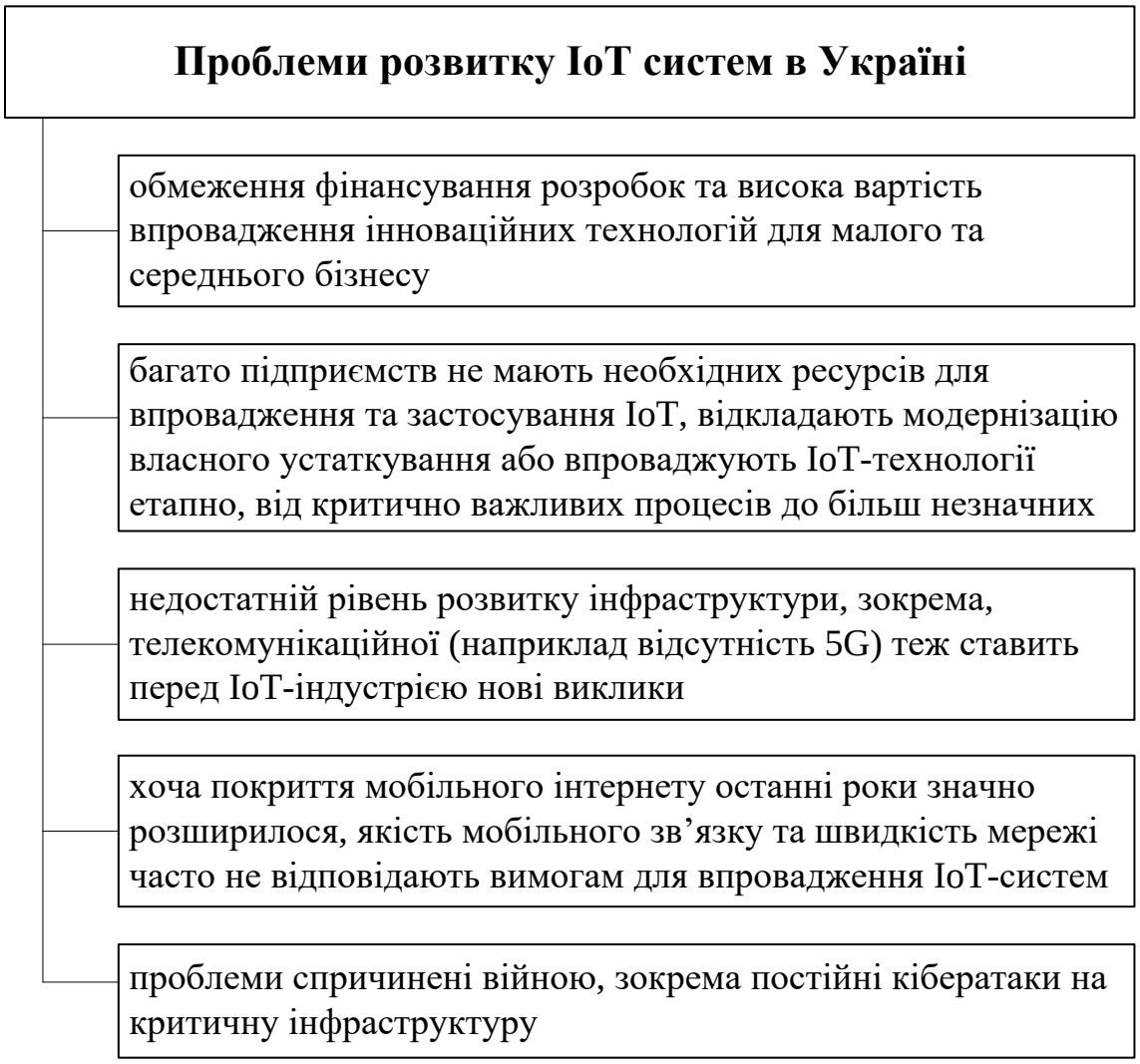

Рисунок 1.4 – Проблеми розвитку IoT в Україні

У контексті безпеки, в умовах постійних кібератак на критичну інфраструктуру, українські розробники активно застосовують додаткові заходи безпеки, проводять регулярний аудит систем, постійно вдосконалюють власні IoT-рішення, інтегрують та адаптують свої продукти до європейських протоколів і норм безпеки, стандартизуючи IoT-системи та розширюючи можливості для виходу на європейський ринок.

2 ОСОБЛИВОСТІ ТА ПРИНЦИПИ ФУНКЦІОНУВАННЯ МЕРЕЖ IoT

2.1 Концепція та принципи функціонування IoT

Від традиційних комп'ютерних мереж мережі IoT відрізняються завдяки ряду унікальних характеристик та принципів функціонування, на яких ґрунтується уся концепція. Здатність IoT-мереж забезпечувати взаємодію між великою кількістю автономних пристроїв, які можуть бути обмежені в живленні та обчислювальних ресурсах, є основною особливістю функціонування мереж Інтернету речей.

Концепція Інтернету речей (IoT) складається з обчислювальної мережі фізичних предметів (речей), які мають вбудовані технології взаємодії між собою або зовнішнім середовищем. Концепція представляє собою явище, у якому така мережа здатна перебудувати суспільні та економічні процеси, виключаючи необхідність участі людини.

Архітектура IoT наведена на рис. 2.1.

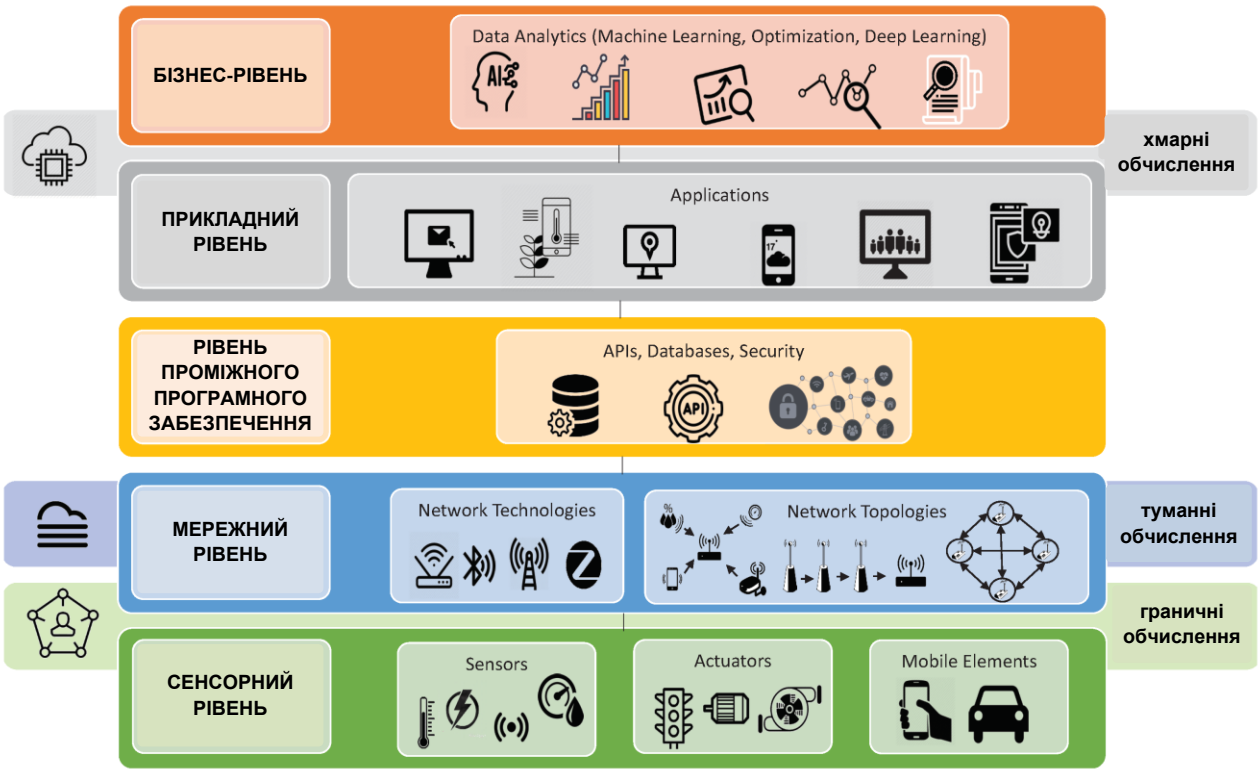

Рисунок 2.1 – Архітектура IoT

Архітектура IoT складається з п’яти рівнів (рис. 2.1) та відповідних їм елементів (програм, додатків, об’єктів ідентифікації, сенсорів та актуаторів, комунікацій та подальших обчислень). Сенсори збирають дані з навколишнього середовища або об’єкта, а актуатори виконують дії на основі проаналізованої інформації. Ідентифікація відбувається шляхом присвоєння кожному об’єкту мережі унікального ідентифікатора, які можуть бути IP-адресами, MAC-адресами, RFID-мітками тощо. Етап ідентифікації необхідний для визначення об’єктів мережі та забезпечення зв’язку між ними. Для забезпечення комунікації між компонентами мережі використовуються різноманітні протоколи зв’язку, як дротові, так й бездротові технології, наприклад, Wi-Fi, Bluetooth, ZigBee, LoRaWAN тощо, які дозволяють елементам IoT обмінюватися інформацією. Подальше обчислення отриманих даних відбувається як на самих пристроях, так і на хмарних платформах. Вибір місця обробки залежить від вимоги, які ставляться перед мережею Інтернету речей.

На сенсорному рівні відбувається процес збору даних з навколишнього середовища або фізичних об’єктів за допомогою сенсорів, датчиків, актуаторів тощо. На мережному рівні забезпечується передача даних між пристроями та хмарними платформами завдяки застосуванню різноманітних протоколів зв’язку. Прикладний рівень забезпечує обробку і аналіз вхідних даних, на основі яких згодом надається відповідних сигнал кінцевим користувачам.

Основні принципи функціонування мереж IoT наведено на рис. 2.2.

Концепція IoT представляє собою багаторівневу структуру, архітектурні принципи якої стають підґрунтям ефективної та надійної IoT-системи.

Мережі IoT використовують різноманітні протоколи зв’язку, вибір яких базується на вимогах додатків. Найпоширенішими протоколами зв’язку вважають MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) та AMQP (Advanced Message Queuing Protocol). MQTT (Message Queuing Telemetry Transport) – простий протокол, який оптимізований для використання пристроями з обмеженими ресурсами. CoAP (Constrained Application Protocol) – протокол, що застосовуються для ряду пристроїв, які функціонують через UDP (User Datagram Protocol). AMQP (Advanced Message Queuing Protocol) – надійний протокол передачі повідомлень між серверами.

Принцип масштабованості дозволяє системі адаптуватися до зростання потреб. Подібна адаптація відбувається завдяки підключенню нових пристроїв,

що відкриває можливість ефективно керувати навантаженням на систему без втрати її працездатності. Гнучкість системи, яка забезпечується шляхом масштабованості, дозволяє змінювати параметри роботи системи, адаптуючи її під нові потреби користувачів.

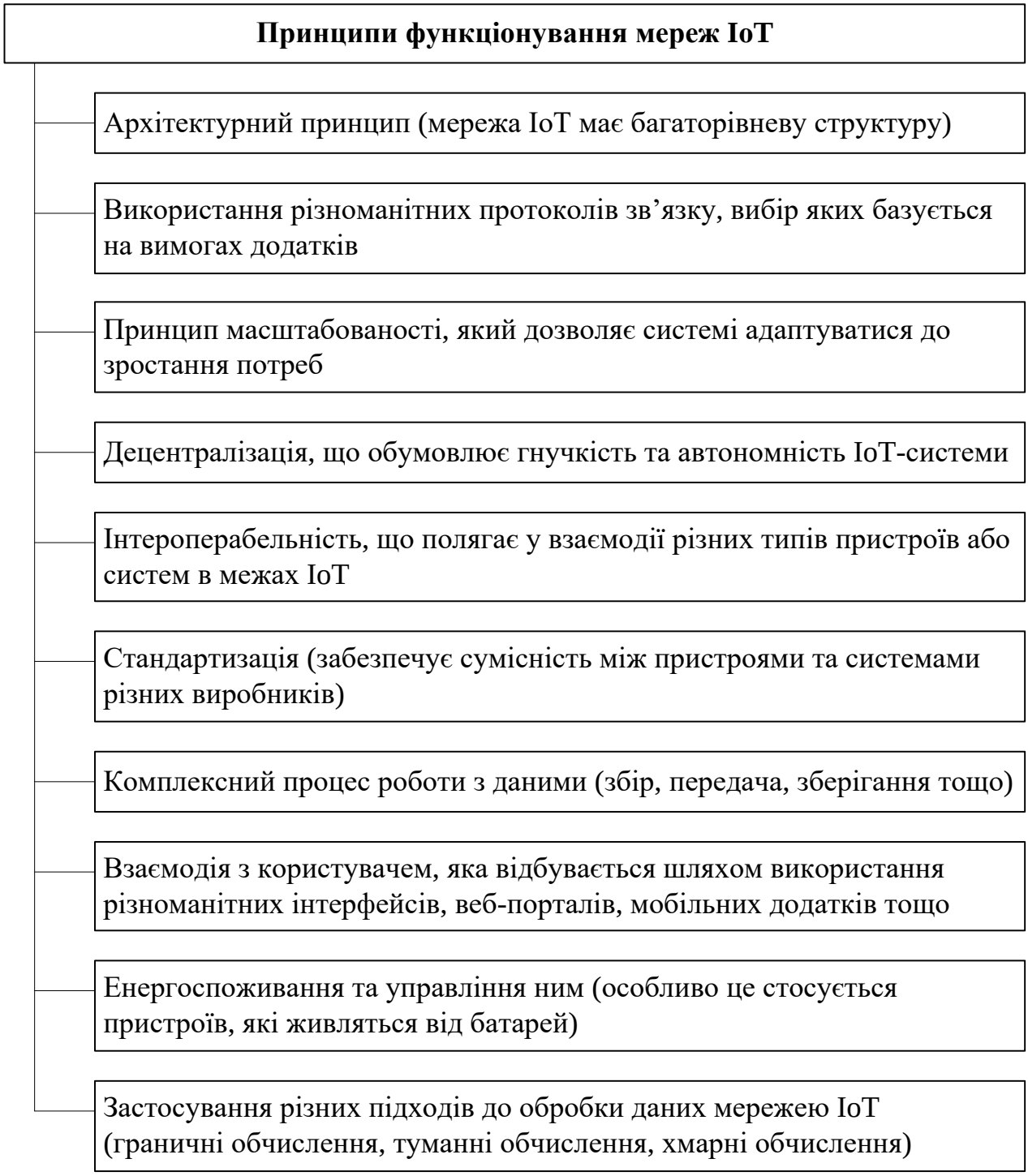

Рисунок 2.2 – Принципи функціонування мереж IoT

Децентралізація обумовлює гнучкість та автономність IoT-системи. Децентралізація забезпечує надійність системи шляхом роботи пристроїв незалежно один від одного, що автоматично знижує навантаження на систему та оптимізує використання обчислювальних ресурсів.

Інтероперабельність полягає у взаємодії різних типів пристроїв або систем в межах IoT. Це відбувається шляхом застосування різних стандартів та протоколів, що «знайомлять» різні елементи системи та дозволяє ефективно взаємодіяти один з одним. Цей процес забезпечує універсальність системи та допомагає їй інтегруватися у ширший спектр вже існуючих рішень.

Стандартизація є важливим компонентом роботи мереж Інтернету речей, забезпечуючи сумісність між пристроями та системами різних виробників. Основну увагу приділяють стандартизації протоколів зв'язку, форматів даних, що передаються IoT-мережею і вимог та протоколів безпеки. Процес стандартизації охоплює усі рівні функціонування IoT-мереж. Найпоширенішими стандартами функціонування мереж на рівні сприйняття є протоколи Bluetooth Low Energy (BLE), ZigBee, NB-IoT, LoRaWAN тощо. Стандартні протоколи на мережному рівні є IPv6, 6LoWPAN, Thread. На прикладному рівні, окрім вже зазначених вище MQTT, CoAP, AMQP, також застосовують стандарти типу HTTP/2 і WebSocket. Для ефективної роботи IoT-мереж необхідна інтеграція з вже існуючими системами. Для цього потрібна сумісність з legacy-системами, підтримка протоколів та форматів даних з можливістю їхньої міграції, тим самим забезпечуючи гнучкість мережі [15].

Дані в IoT мають свій життєвий цикл, що є комплексним процесом, який розпочинається зі збору даних через сенсори і датчики. Дані проходять етапи передачі, де ключову роль відіграють обрані протоколи комунікації. Обробка отриманих даних складається з їх фільтрації, синхронізації та аналізу, завдяки чому отримується корисна інформація з великого обсягу необроблених, сирих даних. Концепція в IoT припускає зберігання даних та обробленої інформації локально на пристроях, хмарних сховищах або в базах даних. Спосіб зберігання напряму залежить від доступності цих даних, стану їх обробки та аналізу та загального обсягу інформації. Фінальним етапом життєвого циклу даних у межах концепції є використання даних, яке полягає у візуалізації для користувачів, автономії прийнятті рішень системою або синхронізації з іншими системними процесами.

У концепції IoT передбачена взаємодія з користувачем, яка відбувається шляхом використання різноманітних інтерфейсів, веб-порталів, мобільних додатків тощо. Сучасний інтерфейс дозволяє користувачеві не лише переглядати дані, а й керувати пристроями, коригувати їх роботи та отримувати важливі сповіщення щодо стану системи і важливих подій для користувача. Остання функція концепції є одним із важливих елементів IoT, адже своєчасне інформування користувача щодо критичних ситуацій у середовищі або змін у роботі системи забезпечують безпековий аспект і надійність Інтернету речей.

Ключовим аспектом функціонування мереж IoT є безпека. Реалізація безпеки в системах IoT відбувається завдяки заходам, які спрямовані на збереження конфіденційності, цілісності та доступності даних. Основні механізми полягають у використанні шифрування даних при їх зберіганні та передачі і застосуванні автентифікації пристроїв та користувачів, а перевірки цілісності даних забезпечують їх незмінність. Балансування навантажень на систему та резервування відповідають за доступність даних для користувача.

Крім того, для забезпечення належного рівня безпеки виконується контроль доступу до ресурсів мережі та відбувається активний моніторинг для своєчасного виявлення аномалій функціонування IoT-мережі.

Окрім вже зазначених аспектів, важливим елементом IoT-мереж є енергоспоживання та управління ним, особливо це стосується пристроїв, які живляться від батарей. Ефективність енергоспоживання досягається завдяки процесам оптимізації протоколів зв’язку, використанню режимів сну пристроїв, впровадженню адаптивного управління потужністю передачі даних та синхронізації даних на edge-пристроях. Як вже було зазначено, ключовою особливістю функціонування мережі Інтернету речей є масштабованість. Вона забезпечуються шляхом підключення нових пристроїв без перебудування загальної мережі та балансування навантаження на неї. Автоматичне відновлення після збоїв та стійкість мережі до відмови її окремих компонентів характеризують надійність функціонування IoT.

Застосування різних підходів до обробки даних мережею IoT є ще одним принципом її роботи. Подібне рішення дозволяє зменшити затримки обробки даних, знизити навантаження на мережу, забезпечити автономність IoT навіть за умови втрати зв’язку та підвищити рівень локальної безпеки під час обробки конфіденційних даних. Для цього використовують різні види обробки даних:

– обробка даних безпосереднього на самих пристроях (edge computing – граничні обчислення),

– обробка даних на вузлах мережі (fog computing – туманні обчислення),

– обробка даних на хмарних платформах (cloud computing – хмарні обчислення).

Зазвичай, для функціонування мережі застосовують комбінації різних підходів. Вибір комбінації залежить від обсягів даних, безпекових вимог, вимог до швидкості обробки даних та їх обсягів, доступності до ресурсів мережі та економічних факторів. Наприклад, для досягнення ефективності мережі у режимі реального часу та для зберігання та аналізу великого обсягу даних використовують комбінацію Edge + Cloud, а для синхронізації даних за умови їхньої локальної обробки та глобальної аналітики впроваджують комбінацію Edge + Fog + Cloud.

2.2 Сучасні засоби IoT

Сучасні засоби IoT – це комплекс апаратних та програмних рішень для організації мереж IoT. Ці технології можна представити у вигляді декількох категорій, де кожна відіграє ключову роль у роботі системи Інтернету речей (рис.2.3).

Сучасні системи IoT активно застосовують технології зв’язку, зокрема бездротового. Найбільш перспективною технологією зв’язку, яка у подальшому суттєво вплине на розвиток IoT, справедливо можна вважати технологію 5G, що характеризується високою швидкістю передачі даних і низькою затримкою.

Бездротова технологія NB-IoT (Narrowband IoT) була розроблена спеціально для використання пристроями з низьким енергоспоживанням. Вона дозволяє забезпечити широке покриття. Технології LPWAN (Low-Power Wide-Area Network), які складаються з двох компонентів - LoRaWAN та Sigfox – створені для передачі невеликих обсягів даних, за умови великої відстані і мінімального енергоспоживання. Ці технології ефективно застосовуються для моніторингу та управління у секторі сільського господарства, «розумних» містах та виробничих процесах промисловості.

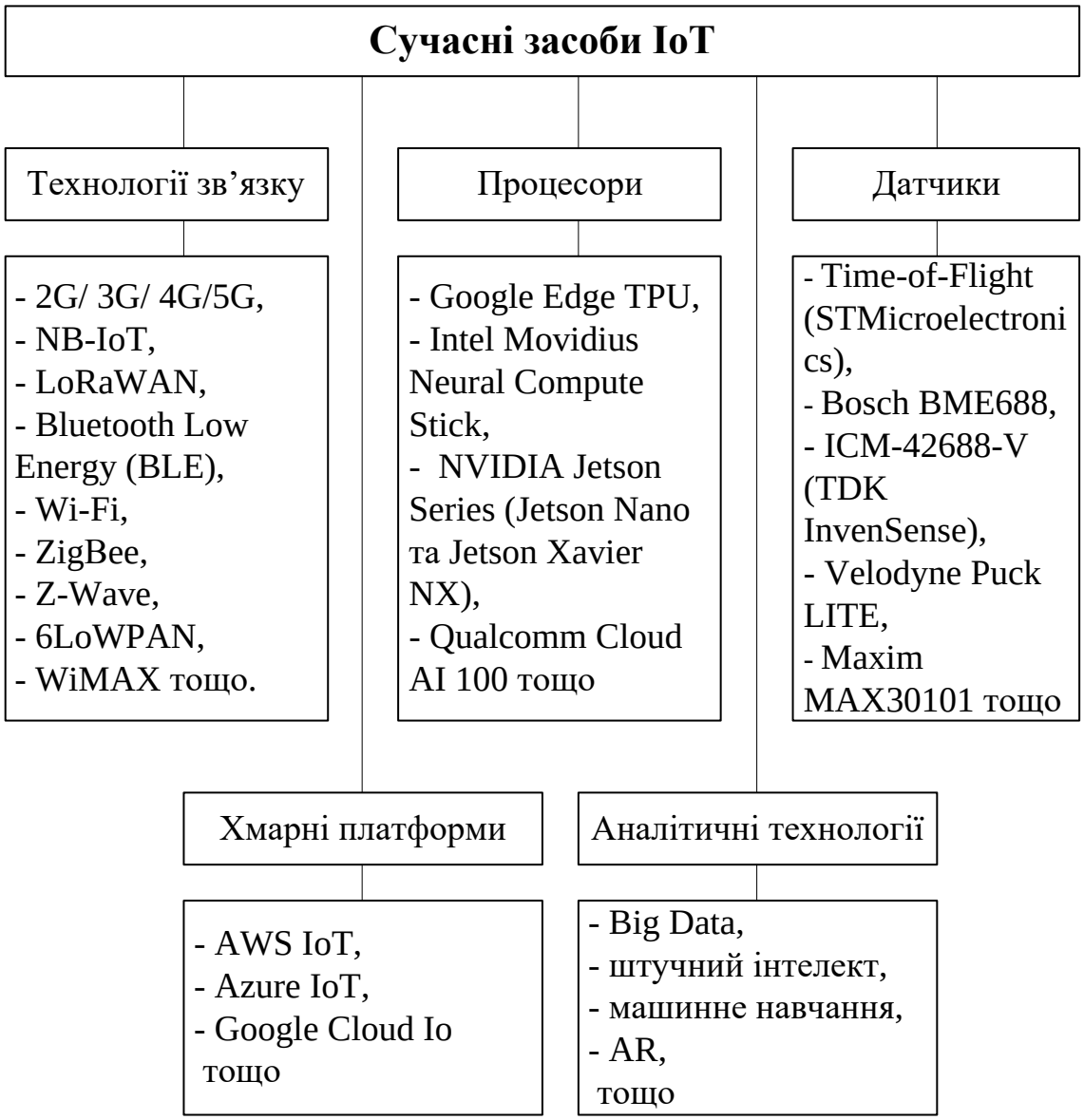

Рисунок 2.3 – Сучасні засоби для організації мереж IoT

Нове покоління IoT-пристроїв з'явилося завдяки розвитку мікроелектроніки. Сучасні апаратні технології, що застосовуються у системах Інтернету речей, представляють собою різноманітні мікроконтролери та SoC-системи, які характеризуються високою продуктивністю та низьким рівнем енергоспоживання. Для роботи штучного інтелекту та машинного навчання у межах IoT-систем використовуються спеціалізовані процесори, які можуть виконувати складні обчислення безпосередньо на пристроях системи Інтернету речей. Наприклад, найпоширеніші процесори Google Edge TPU, Intel Movidius Neural Compute Stick, процесори NVIDIA Jetson Series (Jetson Nano та Jetson Xavier NX) і Qualcomm Cloud AI 100.

Процесори Google Edge TPU може обробляти до 4 трильйонів операцій в секунду, Intel Movidius Neural Compute Stick використовується для прискорення ШІ на edge-пристроях. Процесор Jetson Nano вважається найбільш енергоефективним, а Jetson Xavier NX має оптимальний рівень балансу продуктивності, що позитивно впливає на роботу усієї IoT-системи з інтегрованим у неї штучним інтелектом. Qualcomm Cloud AI 100 був спеціально розроблений для edge computing, має змогу підтримувати різні формати даних та оптимізований для 5G-мереж.

Сучасні датчики, завдяки стрімкому розвитку сенсорних технологій, стали більш точним, компактними та енергоефективними. Постійно з'являються нові види сенсорів, які здатні вимірювати велику кількість параметрів, від біометричних даних людини до показників навколишнього середовища. З відомих інноваційних розробок варто зазначити оптичні сенсорні датчики Time-of-Flight компанії STMicroelectronics. Їхня продукція може проводити вимірювання відстані до об'єктів дистанцією до 4 метрів, використовуючи 8x8 матрицю чутливих елементів, при цьому маючи низьке енергоспоживання [16]. Датчик екологічного моніторингу Bosch BME688 поєднує у собі функції вимірювання одразу чотирьох важливих параметрів: температури, вологості, тиску та якості повітря. Датчик вміє виявляти органічні сполуки у повітрі та використовує алгоритми ШІ для розпізнавання запахів у навколишньому середовищі, що є корисним для промислової сфери та побуту людей [17]. Сенсор руху ICM-42688-V, який розробила компанія TDK InvenSense, представляє собою об'єднані акселерометр та гіроскоп, має вбудований процесор обробки руху, що дозволяє датчику мати широкий спектр застосування від «розумних» годинниках до навігаційних систем [18]. Незамінним для автономних транспортних засобів є сенсори просторового сканування, зокрема LiDAR-сенсори, серед яких найпоширенішими вважається сенсор Velodyne Puck LITE. Він здатний вести круговий огляд з високою точністю вимірювань [19]. Біометричний датчик Maxim MAX30101 використовується медичних виробах для проведення пульсоксиметрії та моніторингу серцевого ритму, маючи високу точність даних та мінімальне енергоспоживання [20].

Постійний розвиток програмних технологій створює умови для розробки ефективних платформ управлення пристроями та даними, які активно

застосовуються в IoT-системах. Зокрема, хмарні платформи AWS IoT, Azure IoT і Google Cloud IoT, забезпечують збір, обробку та аналіз даних. Крім того, платформи надають інструменти управління пристроями, моніторингу їхньої роботи та стану і керування оновленнями програмного забезпечення.

Аналітичні технології відіграють важливу роль у функціонуванні сучасних систем Інтернету речей, зокрема, забезпечуючи ефективну обробку даних. Для цього використовують технології обробки великих обсягів даних (Big Data), штучного інтелекту та машинного навчання. Інтеграція технологій візуалізації в IoT-системи відповідають за створення інтуїтивно зрозумілих інтерфейсів моніторингу і керування системою. Для промислових додатків та технічного обслуговування IoT-систем активно використовують технології доповненої реальності (AR) задля візуалізації даних з пристроїв системи у режимі реального часу і простору.

Наразі системи Інтернету речей, використовуючи сучасні технології, повинні інтегруватися з вже існуючими IT-системами. Окрім вже перелічених технологій, цьому процесу сприяють використання API (інтерфейс програмування застосунків) і технологій мікросервісної архітектури. Вони роблять процес інтеграції гнучким, а для спрощення масштабування додатків Інтернету речей використовують Docker та Kubernetes - технологій контейнеризації, суть яких полягає у створенні, розгортанні та керуванні програмним забезпеченням, шляхом його упакування у так званий контейнер, де є все необхідне для запуску програми.

2.3 Порівняльний аналіз сучасних технологій зв’язку для мереж IoT

Структура мережі Інтернету речей спирається на телекомунікаційні технології, які забезпечують зв’язок між пристроями IoT-мережі, обумовлюючи їх вихід до глобальної мережі та взаємодію між собою і навколишнім середовищем.

Сучасні мережі Інтернету речей, здебільшого, використовують технології бездротової комунікації. Основні технології бездротового зв’язку поділяють за радіусом дії на 3 категорії. Особливості цих категорій наведено в табл. 2.1.

Порівняльний аналіз сучасних технологій зв’язку для мереж IoT за їхніми основними технічними характеристиками наведено в табл. 2.2.

Таблиця 2.1 – Категорії технологій бездротового зв’язку для IoT

№	Категорія	Технології	Особливості
1	Технології малого радіусу дії (десятки метрів)	Bluetooth Low Energy (BLE)	- BLE побудований на основі Bluetooth і є його більш енергоекономною версією, - застосовують для побутовой автоматизації, у системах «розумного» будинку, - працює на швидкості до 2 Мбіт/с під час передачі даних з економією енергії, - пристрої працюють довгий час від батареї.
		Wi-Fi	- має високу пропускну здатність і гарну сумісність із вже існуючими системами і інфраструктурою, що дозволяє активно застосовувати технологію для офісних IoT-пристроїв та для домашнього користування, за умови безперебійного живлення
2	Технології середнього радіусу дії (до кількох сотень метрів)	Zigbee	- стандарт бездротового зв’язку відкритого типу, який працює на частоті 2,4 ГГц, - характеризується низьким енергоспожи-ванням та здатністю створювати mesh-мережі, у якому кожен з пристроїв може бути ретранслятором для інших пристроїв, що дає можливість розширити зону покриття без необхідності додаткових точок доступу
		Thread	- перспективний протокол IoT-мережі є, який створює mesh-мережі, забезпечуючи надійний зв’язок між пристроями, - здебільшого слугує протоколом зв’язку для домашньої автоматизації
3	Технології великого радіусу дії (до десятків кілометрів)	LoRaWAN (Long Range Wide Area Network)	- низьке енергоспоживання, - велика зона покриття, - ідеально підходить до впровадження сенсорних IoT-мереж у СГ діяльності, для розумних міст і для екологічного моніторингу

Таблиця 2.2 – Порівняння телекомунікаційних технологій для IoT

№	Техно-логія	Стан-дарт	Енерго-спожи-вання	Тип мережі	Швид-кість	Діапа-зон дії	Діапа-зон частот	Mesh
1	Bluetooth (BLE)	IEEE 802.15.1	10мВт	PAN	1 Мбіт/с	50 м	2,4 ГГц	немає
2	ZigBee	IEEE 802.15.4	Дуже низьке	PAN	250 Кбіт/с	100 м	2,4 ГГц	є
3	Z-Wave	Z-Wave Alliance	Дуже низьке	PAN	100 Кбіт/с	30 м	908,42 МГц	є
4	6LoWPAN	IEEE 802.15.4	Дуже низьке	PAN	250 Кбіт/с	10 – 100 м	2,4 ГГц	є
5	Wi-Fi	IEEE 802.11	Високе	LAN	100 – 250 Мбіт/с	100 м +	2,4 ГГц / 5 ГГц	немає
6	LoRa/ LoRaWAN	IEEE 802.15.g	Високе	LPWAN	27 Кбіт/с	10 км +	865 – 925 МГц	немає
7	WiMAX	IEEE 802.16	Високе	MAN	70 Мбіт/с	50 км	2 – 11 ГГц	немає
8	GSM / GPRS	ETSI	Дуже високе	WAN	Помір-на	35 км +	850 МГц/ 1,9 ГГц	немає
9	LTE	3GPP	Дуже високе	WAN	0,1 – 1 Гбіт/с	28 км / 10 км	700 – 2600 МГц	немає
10	LTE-M	3GPP	Помір-не	LPWAN	1 Мбіт/с	великий	різні	немає
11	NB-IoT	3GPP	Помір-не	LPWAN	250 Кбіт/с	20 км +	різні	немає

Окреме місце в організованій структурі IoT відведено стільниковим технологіям зв’язку, зокрема NB-IoT (Narrowband IoT) та LTE-M, які працюють, використовуючи інфраструктуру мобільних мереж. Ця особливість застосування забезпечує широке покриття, безпеку та надійність зв’язку. Технологія NB-IoT має надзвичайно низьке енергоспоживання та створений для передачі невеликого обсягу даних, зібраних з великої кількості пристроїв. LTE-M має більшу пропускну здатність та придатний до вимогливіших IoT-систем [21].

Активне впровадження 5G відкриває перед технологіями Інтернету речей нові можливості. Надзвичайно низька затримка з надвисокою пропускною здатністю у сумі з підключенням до мільйону пристроїв на квадратний кілометр дозволяє вирішити критично важливі питання для IoT-системи. Зокрема, прогнозується, що розповсюдження 5G дозволить ширше використовувати Інтернет речей у логістиці, промисловому секторі та телемедицині.

Задля забезпечення безпеки та надійності зв’язку, переважна більшість сучасних технологій використовує потужні протоколи шифрування та автентифікації. Так, LoRaWAN підтримує двошарову систему автентифікації та 128-битне шифрування, що дозволяє забезпечити високий рівень захисту даних. Стільникові технології, що застосовуються в IoT-мережах, користуються стандартними протоколами безпеки мобільного зв’язку [22].

Вибір конкретної технології зв’язку, перш за все, залежить від відстані між пристроями для передачі даних, пропускної здатності мережі, енергоспоживання, особливостей застосування мережі IoT у подальшому. Крім того, масштабованість мережі та її вартість теж мають суттєвий вплив на вибір технології. Наприклад, технології зв’язку, які можуть створювати mesh-топологію, є більш економічними для покриття великої території. Стільникові технології при тому ж широкому покритті та використанні інфраструктури мобільного зв’язку мають вищу вартість експлуатації.

Наразі розвиток у сфері технологій, які будуть використовуватися для мереж Інтернету речей, активно продовжується. Зокрема, приділяють особливу увагу питанням енергоефективності, безпеки та надійності комунікації. Крім цих питань, проводжуються роботи над забезпечення стандартизації IoT та сумісності між мережами.

2.4 Переваги та недоліки Інтернету речей

Інтернет речей (IoT) є найбільш впливовою технологічною концепцією сьогодення, яка докорінно змінює звичні процеси взаємодії між людьми і навколишнім середовищем. Як і будь-яка технологія, IoT має ряд переваг (рис. 2.4) та недоліків (рис. 2.5), які суттєво впливають на подальші рішення користувачів щодо впровадження Інтернету речей.

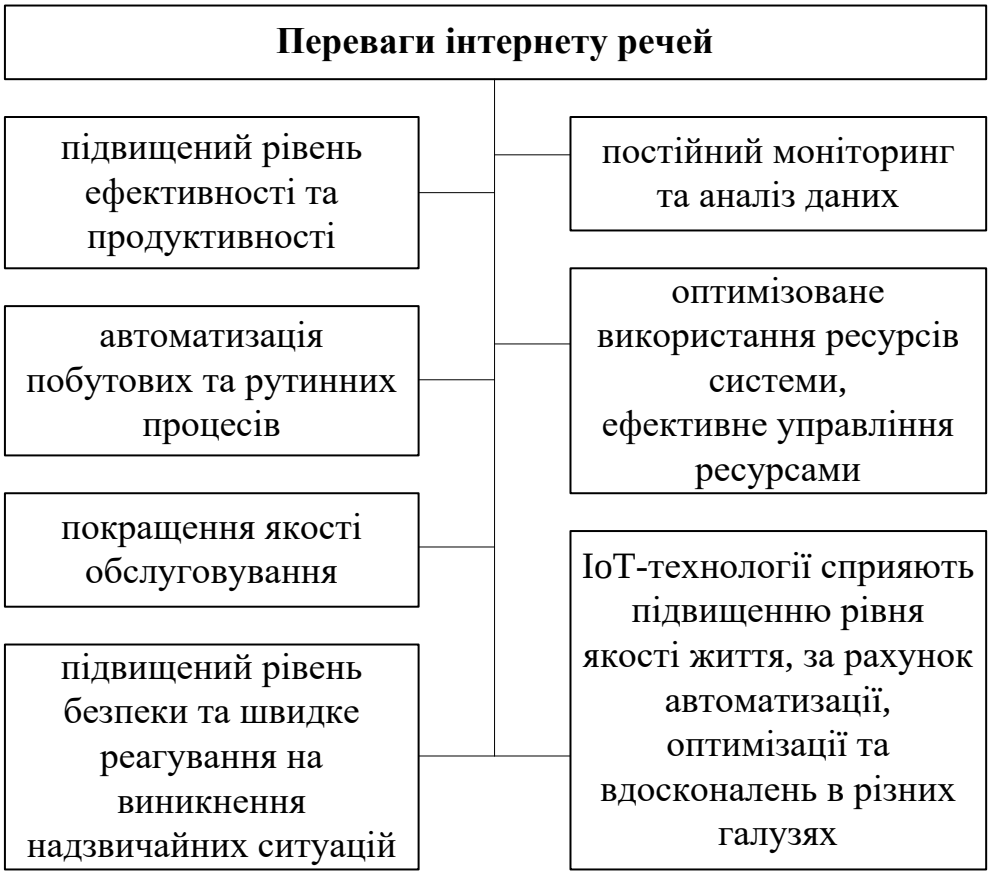

Рисунок 2.4 – Переваги інтернету речей

Завдяки підвищеному рівню ефективності та продуктивності, IoT-система може автоматизувати побутові та рутинні процес, при цьому оптимізуючи використання ресурсів. Так, у промисловій сфери подібні рішення значно підвищують продуктивність та знижують витрати на виробництво. Зокрема, впровадження IoT-рішень у процеси виробництва знижують енергоспоживання та час простою обладнання [23].

Вплив IoT-систем на покращення якості обслуговування відбувається завдяки постійному моніторингу та аналізу даних. Це дозволяє системі ефективно передбачити виникнення проблем у роботі обладнання, застосувавши превентивні заходи. Найбільш корисною ця перевага IoT буде у сфері охороні здоров'я, адже медичні IoT-пристрої виконують постійний моніторинг стану здоров'я пацієнта та сприяють ранньому виявленню ускладнень та станів, що загрожують життю.

Оптимізоване використання ресурсів системи Інтернету речей сприяє більш ефективному управлінню ресурсами шляхом точного і постійного моніторингу. Наприклад, системи з використанням теплиць, є одним із основних застосувань IoT у сільському господарстві. Параметри середовища, такі як температура, інформація про вологість грунту вимірюється в режимі реального часу і надсилається на сервер для аналізу. Ця система не тільки покращує якість та кількість врожаю, а й зменшує споживання води [15].

Системи IoT характеризуються підвищеним рівнем безпеки та швидко реагують на виникнення надзвичайних ситуацій. Ця перевага має ключовий сенс для використання у концепції «розумних» міст, яка включає в себе системи відеоспостереження, моніторингу стану інфраструктури та раннього виявлення природних катаклізмів.

IoT-технології сприяють підвищенню рівня якості життя, адже завдяки автоматизації, оптимізації міського середовища та вдосконалення медичного обслуговування повсякденне життя користувачів стає більш комфортним.

Проте, як і будь-яка технологія, окрім значущих переваг, IoT має і ряд проблем, що потребують уваги та розв'язання (рис. 2.5).

На сьогоднішній день основою проблемою та, як наслідок, питанням, яке постає перед розробниками і потребує вирішення, залишається проблема безпеки та конфіденційності даних. Кожен з підключених до системи або мережі IoT стає мішенню для потенційних кібератак. Статистика невтішна – в період 2018-2022р. кількість кібератак на пристрої IoT зросла більш ніж на 200% [24].

Технічна складність складових систем Інтернету речей вимагає значних знань та ресурсів, включаючи інтеграцію різноманітних технологій сумісності та управління об'ємними даними, що робить системи IoT непростими у встановленні та подальшій експлуатації.

Крім того, впровадження та експлуатація системи є дороговартісним процесом, особливо для масштабних проектів. Значні витрати стосуються спеціалізованого обладнання, програмного забезпечення, навчання персоналу та подальшої модернізації інфраструктури.

Рисунок 2.5 – Проблеми інтернету речей

Ще однією проблемою є залежність системи від якості зв'язку. Надійність функціонування IoT напряму залежить від якості сигналу, адже перебої в мережі призводять до виникнення помилок у роботі системи. Особливо від подібних проблем страждають критично важлива інфраструктура, у яку інтегрована IoT-система.

Недостатня кількість єдиних стандартів продукує проблеми сумісності між пристроями різних компаній і розробників, тим самим ускладнюючи інтеграцію систем.

Наразі більшість пристроїв IoT працює на автономних елементах живлення, і це скорочую терміни їхньої автономної роботи. Від цієї проблеми найбільше потерпають пристрої, які надто віддалені або знаходяться у важкодоступних місцях.

Масове виробництво IoT-пристроїв також шкодить екології, адже через короткий життєвий цикл компонентів Інтернету речей збільшується електронні відходи, які важко піддають переробці.

Наразі ведуться дослідження і роботи, направлені на подолання цих проблем. Розробляються та впроваджуються більш надійні протоколи безпеки, з посиленим використанням шифрування, регулярним оновлення програмного забезпечення, що суттєво підвищує захищеність IoT. Відбувається активна робота над створенням єдиної стандартизації для пристроїв Інтернету речей, постійно вдосконалюються технології, які створюють більш ефективні рішення, проводяться навчальні заходи, направлені на підвищення кваліфікації спеціалістів, які працюють з IoT-системами, що допомагає полегшити технічний процес впровадження та подальшої експлуатації системи.

Тим не менш, технічний характер більшості проблем дає можливості до їх подолання шляхом розвитку технологій та впровадження єдиної системи стандартів. Крім того, ретельне планування та врахування потенційних ризиків і проблем ще на етапі проекту, впливає на успіх впровадження IoT.

3 АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ В IoT

3.1 Проблеми безпеки в мережах Інтернету речей

Внаслідок активного зростання кількості підключених пристроїв та їх поширення у дедалі більше сфер суспільного, економічного та побутового життя людства, актуальність питань безпеки у мережах IoT не вщухає.

Аналіз сучасних проблем систем Інтернету речей показав три основні проблемні області (рис. 3.1).

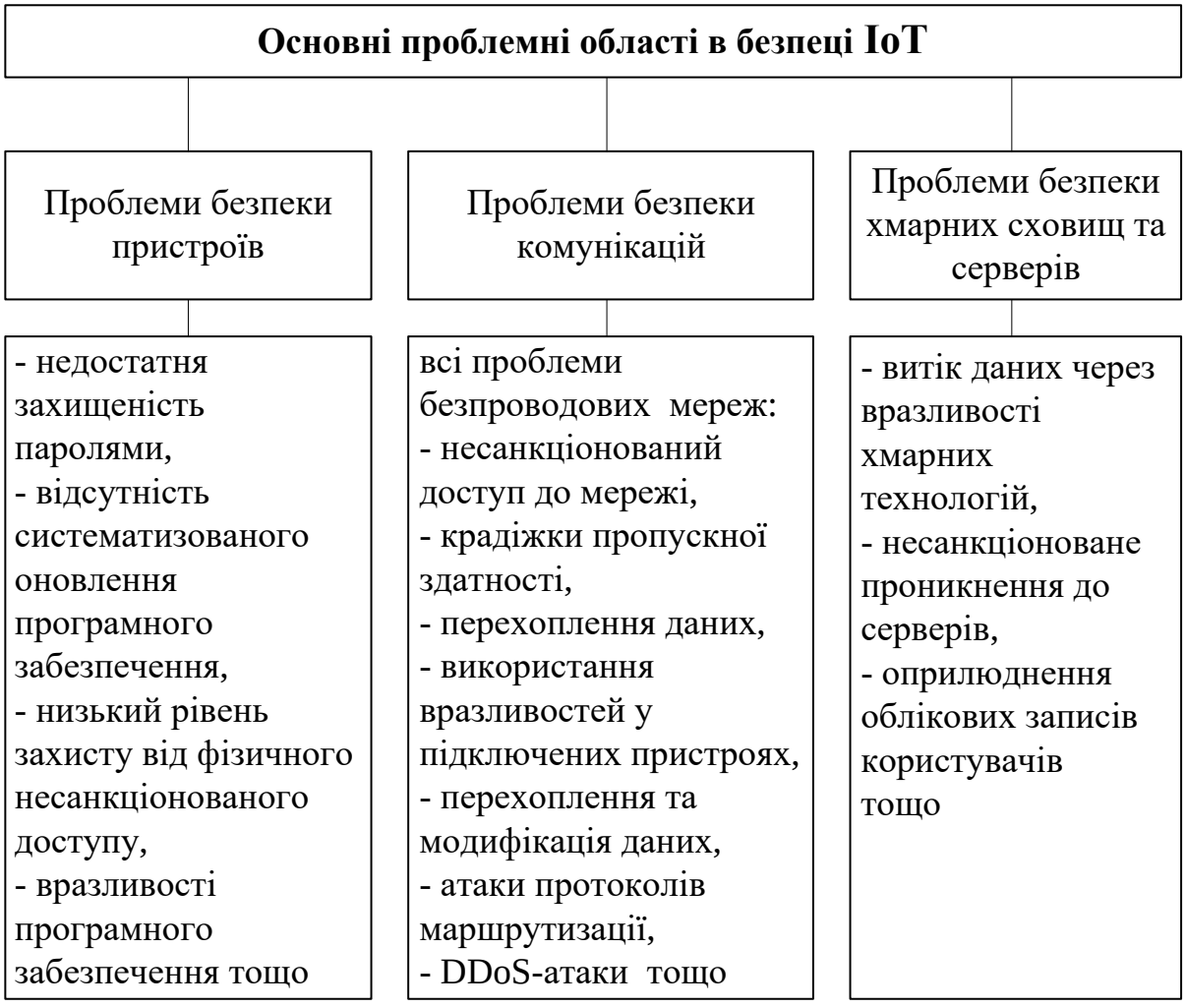

Рисунок 3.1 – Основні проблемні області в безпеці IoT

Вразливості пристроїв обумовлені недостатньою захищеністю паролями, відсутністю систематизованого оновлення програмного забезпечення та

низьким рівенем захисту від фізичного несанкціонованого доступу [25]. Питання безпеки комунікації та зв’язків обумовлені тим, що переважна більшість пристроїв Інтернету речей користуються бездротовими технологіями для передачі даних між собою та навколишнім середовищем, що автоматично наражає їх на небезпеку перехоплення та зміни інформації. Такі атаки частіше проходять за сценарієм підміні рідної точки доступу чужою.

Важливими є також проблеми захисту хмарних сховищ та серверів, якими IoT-системи користуються задля обробки та зберігання даних. Висновки аналізу цього питання не надто втішні – не менш 74% організацій мають відкриті хмарні сховища, в тому числі ті, у яких збегається конфіденційна інформація. При цьому, не менше 84% організацій мають не надійні ключи доступу до хмарних сховищ [26], що є суттєвою проґалиною в системі безпеки та представляє серйозні ризики витоку інформації для кінцевих користувачів.

Останнім часом почастішали випадки комбінованих атак, які несуть особливу загрозу та поєднують у собі декілька напрямків «удару». Наприклад, аби потрапити до мережі IoT, атакуючий може спочатку використати вразливість пристроїв, а потім проникнути до критично важливих елементів системи.

Проблеми безпеки, здебільшого, пов’язані із вразливостями існуючих протоколів через їх незахищеність, слабку автентифікацію, вразливості на етапах маршрутизації, а також вразливостями перед мережними атаками - DDoS-атаками та перехопленням даних.

На сьогоднішній день, спостерігаються тенденції застосування для вирішення проблем безпеки технології штучного інтелекту та машинного навчання для виявлення потенційних загроз та використання превентивних заходів. Проте, інтеграція цих технологій викриває питання підвищеної потреби обробки великих обсягів інформації та створення умов для точності виявлення небезпеки.

3.2 Вразливості мереж IoT

Вразливості мереж Інтернету речей (рис. 3.2) створюють небезпеку, яка потенційно може вплинути на будь-який етап функціонування IoT, завдавши значної шкоди кінцевому користувачу.

Рисунок 3.2 – Основні вразливості мереж IoT

Найбільш критичною вразливістю IoT-мережі є низький рівень автентифікації та вразлива система управління обліковими даними користувача. Причиною цьому явищу є постачання пристроїв із стандартними паролями, які не змінюються користувачами після приєднання до мережі. Подібне нехтування продукує серйозну небезпеку для мережі IoT, адже зловмисники легко проникають усередину системи, «обійшовши» протоколи безпеки шляхом використання примітивних облікових даних.

Незахищеність мережних служб також становить значну небезпеку. Через використання більшістю пристроїв IoT незашифрованих протоколів передачі даних або відкритих портів, створюється потенційна загрози атаки типу «людина посередині» та інших форм мережного перехоплення. Неналежний

рівень та якість шифрування при передачі даних призводить до витоку конфіденційної інформації, які можуть включати в себе особисті і облікові дані користувача та критично важливу інформацію щодо функціонування мережі, що у подальшому може призвести до виробничих та фінансових втрат користувачів. Крім того, вразливість під час реалізації протоколів зв’язку включає використання застарілих видів протоколів, відсутність належної сертифікації та використання слабкого шифрування.

Локальне зберігання даних, тобто безпосередньо на пристроях IoT, теж несе значну загрозу безпеці мережі. Так, якщо зловмисники отримають фізичний доступ до пристрою, то й автоматично отримає доступ до конфіденційних даних. Особливо небезпечно подібним чином зберігати інформацію щодо паролів, ключів шифрування та персональних даних.

Окремим видом вразливостей є відсутність єдиного механізму вчасного та безпечного оновлення програмного забезпечення [27]. Це дозволяє встановлювати стороннє шкідливе програмне забезпечення, що провокує потенційні загрози від саботажу окремого пристрою до його включення до ботнет-мереж та проведення DDoS-атак.

Ще однією вразливістю мереж IoT є недостатня якість моніторингу та аналізу подій безпеки, які могли бути зафіксованими самою мережею. Зокрема, відсутність необхідної якості моніторингу та журналу подій у IoT-мережі знижує можливості для виявлення спроб несанкціонованого доступу та подальшого розслідування випадків проникнення шкідливого програмного забезпечення або зловмисників. До того, багато пристроїв не мають вбудованої системи оповіщення загрозливої активності, що не дозволяє вчасно реагувати на потенційні загрози.

Критичним елементом також незахищені веб-інтерфейси, які часто стають «вхідними воротами» для кібератаки. Значними вразливостями є міжсайтовий скриптинг (XSS), SQL-ін'єкції та знижена валідація вхідних даних. Наявність подібних вразливих елементів у мережі дозволяють отримати несанкціонований доступ до пристрою, схованих у ньому конфіденційних даних і програмного забезпечення, яке за бажанням можна модифікувати шкідливим оновленням.

При проектуванні мереж IoT фізична безпека пристроїв часто буває не надто продуманою, і це особливо критично відображається на пристроях, які

розташовані у публічних місцях або у легкому фізичному доступі сторонніх людей і тварин. Відсутність належного захисту від фізичного доступу до структур налаштувань створює потенційну загрозу злому пристрою.

Для корпоративної безпеки особливу небезпеку ставить недостатня сегментація мережі. Корпорації зрідка впроваджують сегментацію задля безпеки усієї мережі, і це означає, що навіть проникнення в один пристрій IoT може саботувати роботи усієї мережі, отримавши доступ до критично важливих даних та систем корпорації.

Конфіденційність користувачів у мережа IoT часто не забезпечена належним чином. Статистика показує, що переважна більшість пристроїв Інтернету речей збирає більшу кількість даних, аніж цього потребують для ефективного функціонування [28]. Користувачі, зазвичай, не мають повноцінної змоги контролювати цей процес, і це створює загрозу порушення нормативно-правових норм про захист персональних даних та продукує подальші можливі серйозні інциденти, пов’язані з приватністю користувачів.

3.3 Загрози та атаки мереж Інтернету речей

Стрімкий розвиток технологій IoT створив умови для появи нових видів загроз та атак, метою яких є завдання серйозної шкоди користувачам і корпораціям. Загрози і атаки на мережі Інтернету речей поділяють на декілька основних типів (рис. 3.3).

Атака типу DoS/DDoS, тобто «відмова в обслуговуванні», є найпоширенішою кібератакою на мережі IoT, для виконання якої використовують ботнет-мережі із компрометованих пристроїв Інтернету речей для створення масивного штучного трафіку і спрямовують його на вузли комунікації мережі, пристрої або платформи зберігання даних. Особливої шкоди, зокрема у фінансовому плані, подібні атаки наносять промисловим IoT-мережам.

Протоколи маршрутизації також часто піддаються кібератакам. Так, зловмисники використовують проґалини у протоколах, щоб перехопити або змінити трафік мережі. Найчастіше використовують атаки підміни маршруту, створення петель маршрутизації, атаки за типом «чорної діри».

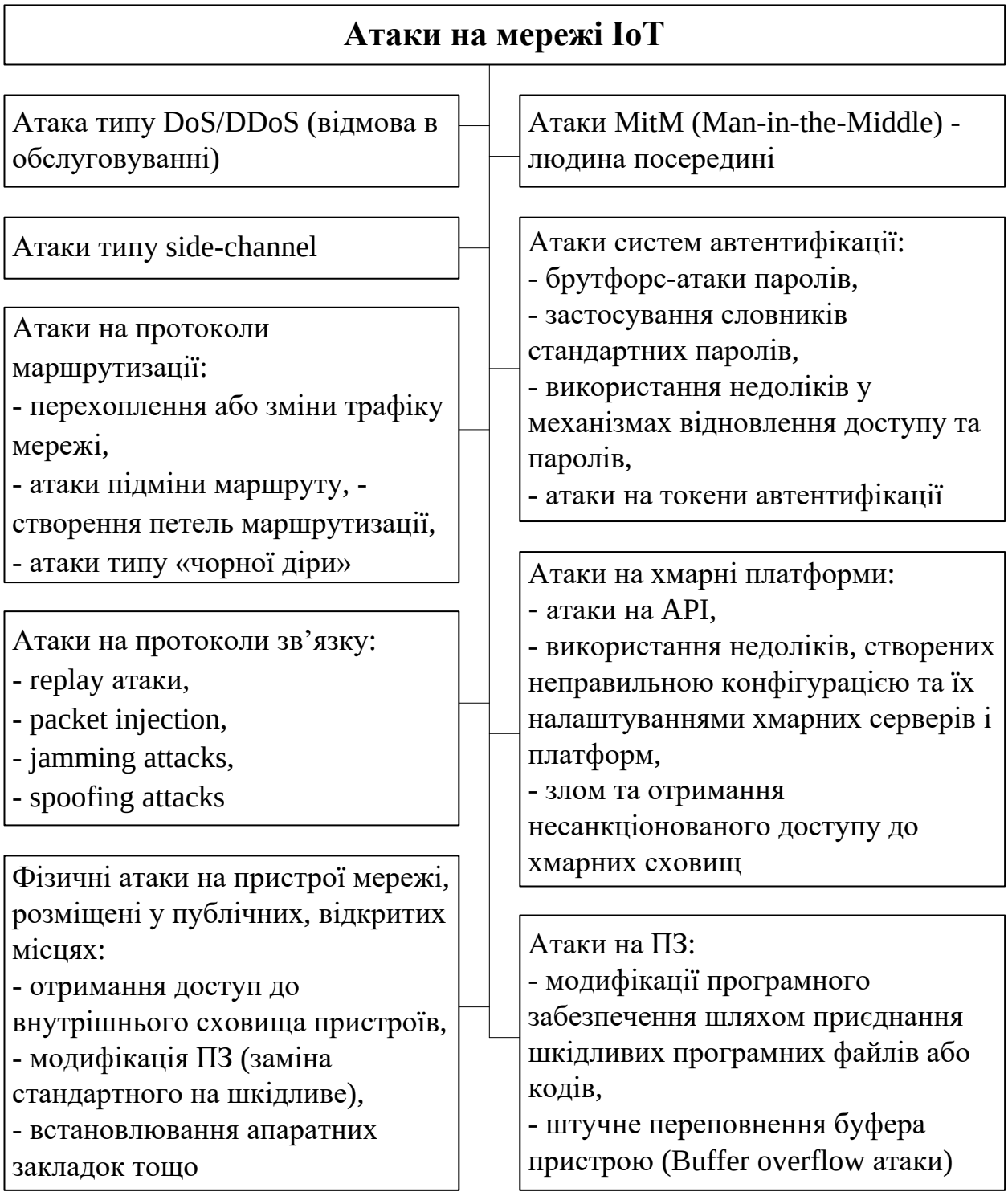

Рисунок 3.3 – Атаки на мережі IoT

Загрозу для мереж IoT також становлять атаки безпосередньо на протоколи зв'язку. Атаками на протоколи зв'язку є: replay атаки, packet injection, jamming attacks, spoofing attacks.

Сутність replay атаки полягає у записі та подальшому відтворенні надісланих коректних повідомлень або їх частин, і така атака дозволяє отримати сторонній несанкціонований доступ до даних мережі, зокрема, й для подальшої імітації проходження автентифікації. Packet injection – процес втручання у мережу шляхом створення пакету даних, який маскується під стандартний трафік інформації, і це дозволяє зловмиснику перехоплювати реальні пакети даних. Цей метод часто використовують для атаки «людина посередині» або «відмова в обслуговуванні».

Jamming attacks – тип злому, який полягає у втручанні у бездротові системи зв'язку, зокрема, Wi-Fi, Bluetooth, стільниковий зв'язок та GPS. Такого типу атаки досягається шляхом глушіння зв'язку між пристроями з метою саботажу роботи мережі IoT.

Spoofing attacks - атака, направлена на мережі Інтернету речей, відбувається шляхом маскування особи або шкідливої програми за допомогою фальсифікації даних

Особливо небезпечними для мереж Інтернету речей є атаки MitM (Man-in-the-Middle), які використовують вразливості незахищених протоколів зв'язку. Кібератака цього типу полягає у перехопленні та модифікуванні даних під час їх передачі між пристроями.

Ще одним типом загроз є атаки систем автентифікації, які включають у себе брутфорс-атаки паролів, застосування словників стандартних паролів, використання недоліків у механізмах відновлення доступу та паролів, атаки на токени автентифікації.

Хмарні платформи, на яких зберігається великий обсяг інформації, також часто стають ціллю для кібератак. Зазвичай, виток конфіденційної інформації відбувається внаслідок атак на інтерфейси прикладного програмування (API), використання недоліків, створених неправильною конфігурацією та їх налаштуваннями хмарних серверів і платформ, злому та отримання несанкціонованого доступу до хмарних сховищ. Крім того, витік конфіденційних даних відбувається через ряд вразливостей хмарних інтерфейсів та використання недостатньо надійних механізмів захисту.

Ще однією категорію загрози, що становлять небезпеку IoT-мережам, є фізичні атаки, які, зазвичай, направлені на пристрої мережі, розміщених у публічних, відкритих місцях. Зокрема, такі атаки дозволяють зловмисникам

отримати доступ до внутрішнього сховища пристроїв, модифікувати програмне забезпечення, змінивши стандартне на шкідливе, встановлювати апаратні закладки тощо.

Атаки на програмне забезпечення становлять чи не найбільшу загрозу для мереж IoT. Більше половини кібератак відбувається саме шляхом злому програмного забезпечення, тому що зловмисники використовують вразливості цього елементу мережі, яка має проґалині у захисті внаслідок недостатньо продуманих механізмів вчасного оновлення ПО пристроїв. Цей тип атак полягає у використанні вже відомих вразливостей, модифікації програмного забезпечення шляхом приєднання шкідливих програмних файлів або кодів, штучне переповнення буфера пристрою (Buffer overflow атаки).

Атаки типу side-channel використовують непрямі канали витоку інформації та становлять значну та особливу загрозу для функціонування мережі IoT. Під час атаки зловмисники використовують акустичні сигнали, часові характеристики виконання операцій, аналіз енергоспоживання та навіть електромагнітні випромінювання. Часто цей тип загроз спрямовують на криптографічні механізми пристроїв.

Не можна виключати соціальний фактор із ієрархії загроз систем IoT. Окрема категорія атак пов’язана із соціальним фактором, адже зловмисники можуть обманим шляхом маніпулювати користувачами з метою отримання їхніх облікових даних. Вони також можуть видавати себе за технічних спеціалістів обслуговування мережі, розсилати фішингові повідомлення або розробляти підроблені інтерфейси управління пристроями мережі.

4 РІШЕННЯ ДЛЯ ЗАХИСТУ МЕРЕЖ IoT

4.1 Аналіз засобів захисту мереж Інтернету речей

Для захисту мереж IoT використовуються різні технічні та організаційні механізми. В роботі проведено аналіз засобів захисту мереж IoT (рис. 4.1).

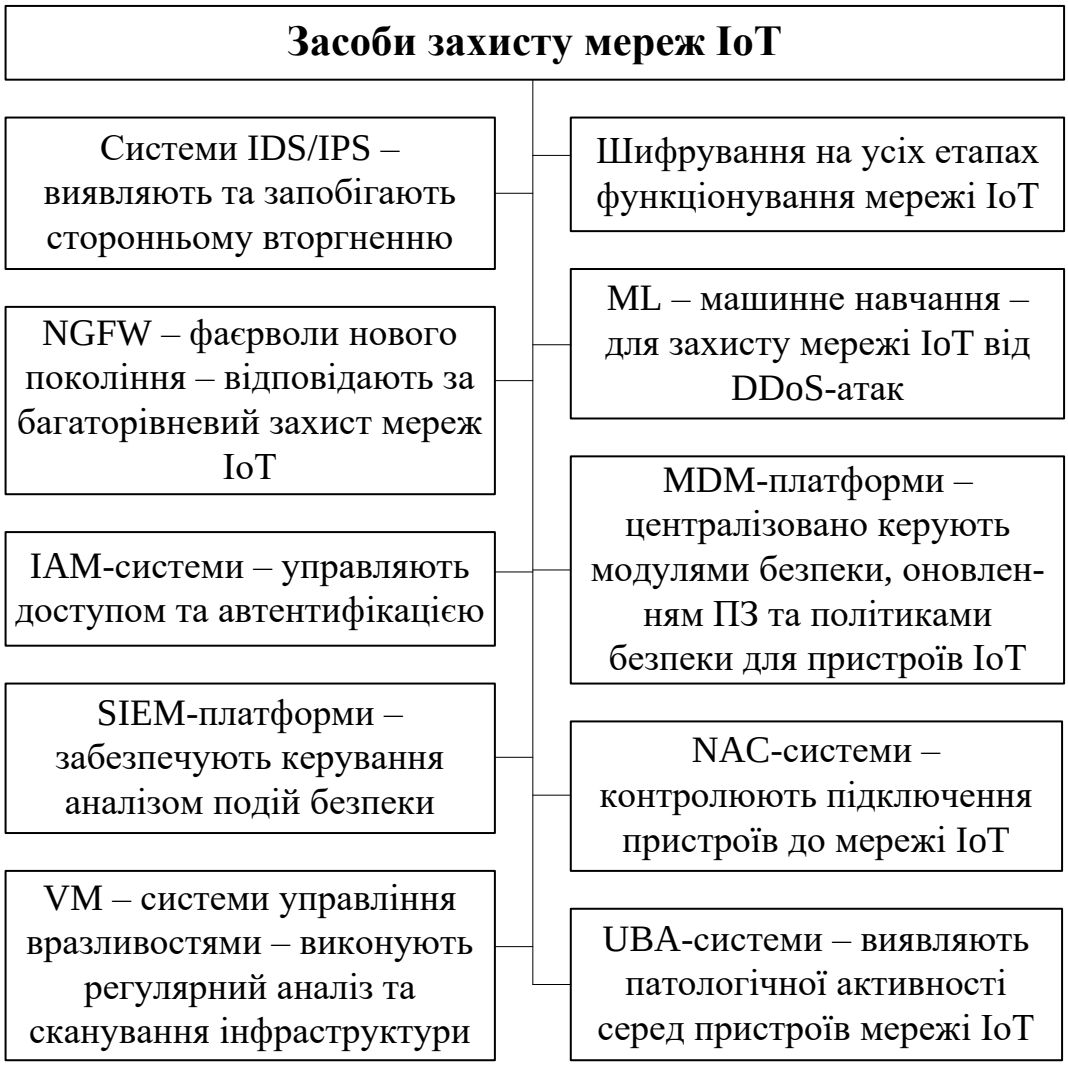

Рисунок 4.1 – Засоби захисту мереж IoT

Одним із ключових елементів захисту мережі є системи IDS/IPS. Сучасні системи IDS/IPS представляють собою комбінацію сигнатурного аналізу (механізм антивірусного захисту, який полягає у виявленні характерних властивостей кожного вірусу і пошуку вірусу у файлах, у яких проявилися

подібні властивості) та виявлення аномалій для попередження потенційних загроз. Особливістю цього елементу захисту є функціонування з урахуванням специфічних ознак, зокрема протоколів та комбінації трафіку, що характерні для пристроїв IoT.

NGFW – міжмережні екрани нового покоління проводять перевірку пакетів шляхом аналізу прикладних протоколів. Також вони контролюють доступ на рівні додатків мережі.

IAM-системи суттєво вливають на процеси забезпечення безпеки і захищеності IoT. Сучасна конфігурація цих систем підтримує більшість технологічних рішень (токени, біометричні дані, сертифікати X.509). Цей засіб захисту також приділяє увагу життєвим циклами облікових даних та управлінню ними і автоматизації надання або відкликання доступів.

SIEM-платформи виконують централізований збір та порівняння подій безпеки з різноманітних джерел. Це дозволяє системі виявити атаку або аномалію у функціонуванні пристрою.

Системи управління вразливостями (VM) оцінюють ризики виникнення позаштатної ситуації та виявляють потенційні недоліки у функціонуванні мережі. Ключовою особливістю сучасних VM-систем є підтримка специфічних протоколів і безпечне сканування вразливих елементів мережі.

Для захисту мережі IoT від DDoS-атак використовують машинне навчання, що дозволяє виявляти та блокувати штучний і шкідливий трафік, залишаючи при цьому доступ до коректних серверів.

Шифрування даних в IoT-мережаж є важливим елементом їх захисту. Шифрування має відбуватися на усіх етапах функціонування мережі, від передачі даних до їх зберігання. У впровадженні методу захисту особливу увагу приділяють використанню апаратних модулів безпеки (HSM) для захисту важливої криптографічної інформації та управлінню ключами доступу.

MDM-платформи централізовано керують модулями безпеки, оновленням ПЗ та політиками безпеки для пристроїв IoT. Використання цих платформ автоматизує процеси інтеграції великої кількості пристроїв з урахуванням безпекових вимог.

NAC-системи – це системи контролю доступу до мережі, що інспектують відповідність між пристроями та політикою безпеки, забезпечують сегментацію мережі та ізолюють потенційно загрозливих пристроїв.

Засоби UBA (User Behavior Analytics) аналізують поведінку пристроїв, застосовуючи механізми машинного навчання з метою виявлення патологічної активності серед пристроїв мережі IoT. UBA-системи створюють профілі з нормальною поведінкою пристроїв та проводять кореляцію усередині мережі для виявлення потенційно небезпечних відхилень у функціонуванні пристрою.

Мережі IoT потребують комплексного захисту, якого можна досягти шляхом розробки та впровадження багаторівневої безпекової системи, яка могла б охоплювати різноманітні елементи функціонування мереж Інтернету речей. В даній роботі пропонується створювати та впроваджувати комплексну багаторівневу систему захисту мереж IoT (рис. 4.2).

Рисунок 4.2 – Комплексна багаторівнева система захисту мереж IoT

Запропонована багаторівнева система захисту (рис. 4.2) допоможе врахувати всі проблеми безпеки мереж IoT та забезпечити надійний захист на всіх рівнях функціонування мереж IoT.

Для забезпечення комплексного захисту мереж IoT також доцільно використовувати не тільки засоби кібербезпеки, але і фізичні засоби безпеки (системи відеоспостереження, датчики відкриття корпусів, системи контролю доступу до приміщень тощо).

4.2 Рекомендації щодо захисту мереж IoT

На основі проведеного детального аналізу структури, принципів функціонування, вразливостей та загроз, які виникають внаслідок розглянутих проблем, можна виділити ряд рекомендацій щодо забезпечення захисту IoT-мереж (рис.4.3).

Впровадження суворих принципів управління обліковими даними та паролями має стати основою захисного механізму мережі IoT.

Строго регламентований механізм регулярного оновлення програмного забезпечення обумовить безпечне функціонування мереж Інтернету речей. Пропонується впровадження систем автоматизованого оновлення з інспекцією цифрових підписів та аналізом файлів на цілісність. Попередньою, перед завантаженням оновлень, рекомендується проведення детального тестування за принципом обмеженої групи пристроїв для виявляння недоліків в оновленні.

Рекомендується здійснення моніторингу безпеки мережі IoT у режимі реального часу, у тому числі із застосуванням спеціалізованих систем для виявлення та запобігання можливим вторгненням. Надважливо організувати збір та аналіз інформації про стан з усіх елементів мережі IoT, включаючи пристрої, системи управління та мережного обладнання для гарантування вчасного виявлення аномальної активності та попередження потенційних загроз.

Рекомендується також розробка плану аварійного відновлення IoT-мережі у разі виникнення позаштатної ситуації у її функціонуванні, що допоможе забезпечити безперервність роботи критично важливих систем мережі. План аварійного відновлення може включати у себе тестування процесів

відновлення, резервне копіювання даних, резервне обладнання з детальною інструкцією його запуск у разі виникнення позаштатної ситуації.

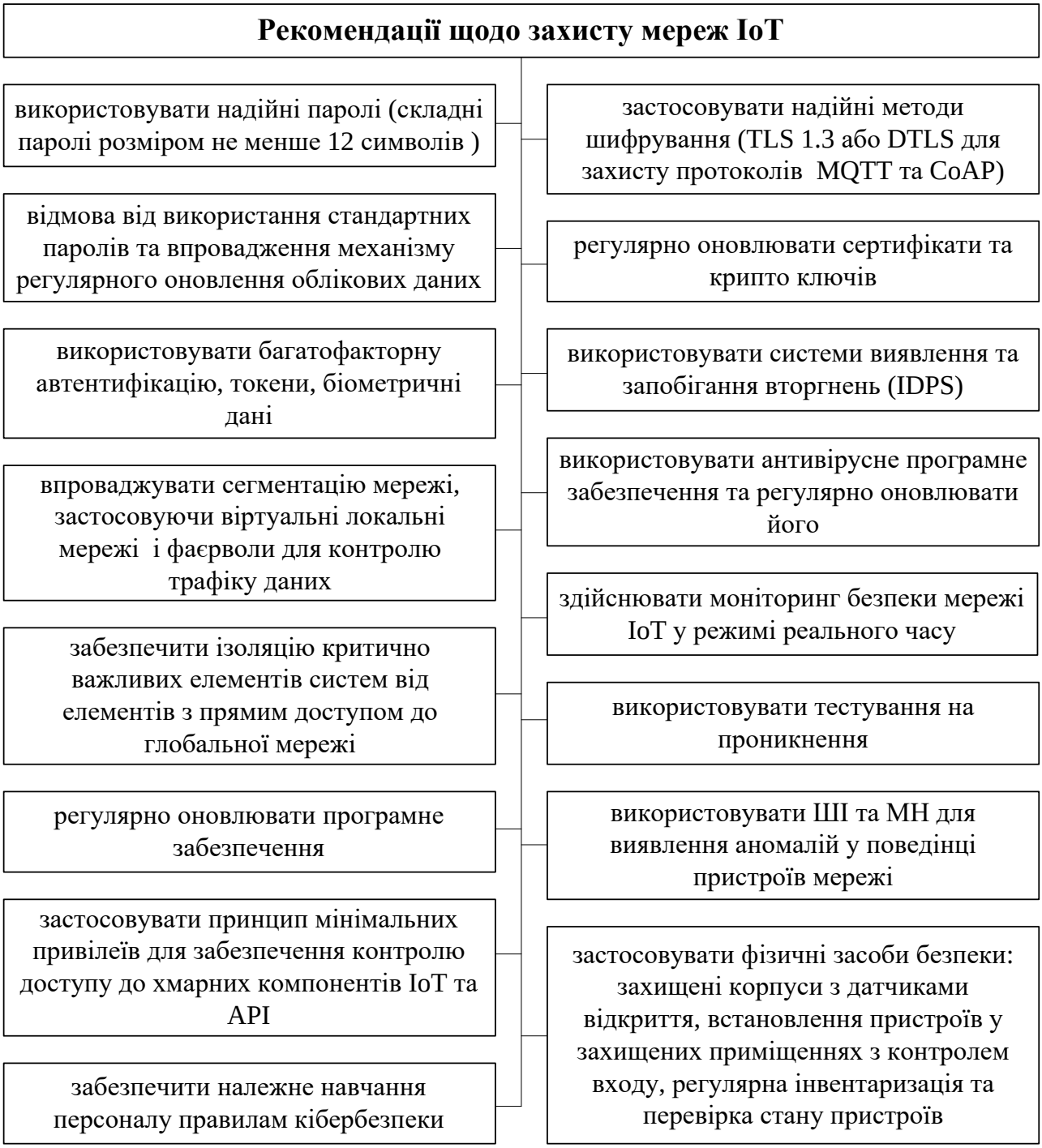

Рисунок 4.3 - Рекомендації щодо захисту мереж IoT

Впровадження цих рекомендацій (рис. 4.3) та регулярне оновлення конфігурацій мережі підвищить рівень захищеності від нових та потенційних загроз, мінімізувавши ризики проведення успішної кібератаки. Проте, варто

пам’ятати, що безпека мереж IoT потребує постійної адаптації до нової небезпеки, а тому має бути забезпечений безперервний процес вдосконалення безпекових механізмів.

4.3 Порівняльний аналіз платформ безпеки IoT

Сьогодні на ринку існують різноманітні платформи безпеки для IoT. Платформа безпеки IoT – це набір інструментів, спеціально розроблених для захисту взаємопов’язаних пристроїв і мереж IoT [29]. Ці платформи використовуються компаніями, галузями та окремими фахівцями, які використовують пристрої IoT для різноманітних функцій, починаючи від домашньої автоматизації та закінчуючи керуванням промисловими процесами.

Використовуючи платформу безпеки IoT, користувачі забезпечують цілісність, конфіденційність і доступність даних під час їх переміщення між пристроями. Це запобігає несанкціонованому доступу та потенційним кіберзагрозам, а також підтримує ефективну роботу всієї системи IoT.

В роботі виконано порівняльний аналіз найкращих (згідно [29]) платформ безпеки IoT: Sectigo IoT, KeyScaler, BugProve, Palo Alto Networks, Entrust, Microsoft Azure Sphere, Mbed OS, Nozomi Networks, Microsoft Defender, Google IoT Core. Результати аналізу представлено в табл. 4.1.

Платформа безпеки Sectigo IoT розроблена для захисту взаємопов’язаних пристроїв шляхом впровадження надійного керування ідентифікацією. Зосереджуючись на ідентифікації, перевірці та захисті пристроїв, він створює надійний захист від несанкціонованого доступу.

Платформа KeyScaler від Device Authority ставить особливий акцент на автентифікації пристрою. Спрямованість на протоколи автентифікації пристрою робить KeyScaler ідеальним рішенням для мереж, які вимагають суворої перевірки пристроїв.

Платформа BugProve розроблена для відстеження та моніторингу програмних помилок протягом життєвого циклу розробки. Акцент на сповіщеннях у реальному часі, візуальному відстеженні та можливостях інтеграції робить BugProve ідеальною для розробників і команд контролю якості для ефективного керування помилками.

Таблиця 4.1 – Порівняльний аналіз сучасних платформ безпеки для IoT

№	Рішення безпеки для IoT	Переваги	Недоліки	Вартість (корист./ місяць)	Висновок
1	Sectigo IoT Security Platform	- Розширені функції шифрування та сертифікатів - Інтеграція з існуючими системами - Комплексне рішення для керування ідентифікацією	- Вартість може бути високою для невеликих реалізацій - Для оптимізації можуть знадобитися технічні знання - Складність у налаштуванні певних інтеграцій	Від 9$	Найкраще для надійного керування ідентифі-кацією
2	KeyScaler	- Кероване політикою керування ключами шифрування - Інтегрується з різними платформами та стандартами IoT - Надійні протоколи автентифікації пристрою	- Можуть знадобитися спеціальні знання для отримання максимальної вигоди - Обмежуючись автентифікацією пристрою, інші потреби безпеки можуть потребувати додаткових інструментів - Ціни можуть не підходити для невеликих реалізацій	Від 15$	Найкраще підходить для протоколів автентифі-кації пристрою
3	BugProve	- Візуальне відстеження помилок для кращої видимості - Інтеграція з популярними засобами розробки - Сповіщення та оновлення в реальному часі	- Річна виставка рахунків може підійти не всім організаціям - Новим користувачам може знадобитися крива навчання - Не вистачає деяких розширених функцій звітування	Від 9$	Найкраще підходить для відстежен-ня та моні-торингу помилок
4	Palo Alto Networks	- Інтеграція з існуючими системами безпеки та платформами SIEM - Комплексний моніторинг розумних пристроїв - Надійний аналіз загроз на основі ШІ	- Для оптимального використання можуть знадобитися додаткові ресурси - Інформація про ціни може бути менш прозорою - Може бути складним для налаштування	Від 30$	Найкраще для захисту розумних пристроїв

Продовження табл. 4.1

№	Рішення безпеки для IoT	Переваги	Недоліки	Вартість (корист./ місяць)	Висновок
5	Entrust	- Сильна інтеграція з корпоративними системами - Масштабований PKI, адаптований для IoT - Спеціалізується на безпеці на основі сертифікатів	- Потенційні проблеми сумісності з нестандартними сертифікатами - Зосереджені головним чином на безпеці сертифікатів, інші сфери можуть бути менш надійними - Може бути складним для невеликих реалізацій	Ціна за запитом	Найкраще для захисту на основі сертифікатів
6	Microsoft Azure Sphere	- Гнучкість у підключенні та управлінні різними пристроями IoT - Широкі можливості інтеграції з іншими службами Azure - Комплексне рішення безпеки, яке об’єднує апаратне забезпечення, ОС і хмару	- Складність налаштування та налаштування може потребувати професійної допомоги - Може вимагати певної апаратної сумісності - Інформація про ціни не є прозорою	Ціна за запитом	Найкраще для безпечного підклю-чення пристроїв
7	Mbed OS	- Сильна інтеграція з популярними інструментами розробки - Комплексна підтримка різних MCU - Спеціально для безпеки вбудованої системи	- Деякі методи навчання для нових розробників - Потрібна технічна експертиза у вбудованих системах - Може бути надмірним для невбудованих випадків використання	Від 5$	Найкраще підходить для безпеки вбудованої системи
8	Nozomi Networks	- Постійний моніторинг і виявлення загроз у реальному часі - Інтеграція з існуючими промисловими системами та протоколами - Спеціалізується на промислових мережних середовищах	- Обмежене застосування поза промисловими контекстами - Може знадобитися широке налаштування для конкретних промислових установок - Інформація про ціни не розголошується	Ціна за запитом	Найкраще підходить для захисту промислових мереж

Продовження табл. 4.1

№	Рішення безпеки для IoT	Переваги	Недоліки	Вартість (корист./ місяць)	Висновок
9	Microsoft Defender for IoT	- Розширені можливості виявлення загроз - Добре інтегрується з іншими продуктами безпеки Microsoft - Спеціалізується на захисті кінцевих точок для IoT	- Потенційні проблеми сумісності з середовищами, що не належать Microsoft - Ціни можуть бути вищими порівняно з деякими конкурентами - Для повного використання може знадобитися технічний досвід	Від 10$	Найкраще для захисту кінцевих точок
10	Google IoT Core	- Надійні функції безпеки для підключення та керування пристроєм - Проста інтеграція з іншими службами Google Cloud - Спрощує складність керування, обробки та зберігання даних IoT	- Обмежена гнучкість при використанні сервісів чи інструментів, що не належать Google Cloud - При наявності великої кількості пристроїв ціна зростає - Може бути складно реалізувати для тих, хто не знайомий із Google Cloud Platform	Від $0,0045 за 1 пристрій на місяць	Найкраще підходить для керування, обробки та зберігання даних

Платформа Palo Alto Networks пропонує повний набір продуктів, спрямованих на захист розумних пристроїв. Їхня зосередженість на безпеці IoT, запобіганні загрозам і адаптивних заходах безпеки робить її найкращою для захисту розумних пристроїв.

Рішення безпеки IoT від Entrust розроблено, щоб забезпечити надійну безпеку на основі сертифікатів, забезпечуючи необхідну цифрову гарантію для пристроїв в IoT. Із зростанням кількості пристроїв IoT у різних галузях, наявність платформи, яка спеціалізується на управлінні сертифікатами, стає надзвичайно важливою, що робить Entrust найкращим рішенням для цієї конкретної проблеми безпеки.

Комплексне рішення Microsoft Azure Sphere пропонує безпечне та масштабоване підключення пристроїв IoT. Воно об’єднує апаратне забезпечення, програмне забезпечення та хмарні служби для створення надійної

системи безпеки для пристроїв IoT, завдяки чому є найкращим для безпечного підключення пристроїв.

Платформа Mbed OS – це популярна операційна система з відкритим кодом, спеціально розроблена для підвищення безпеки вбудованих систем. Зосередженість на вбудованій безпеці робить Mbed OS кращою для безпеки вбудованої системи.

Платформа Nozomi Networks спеціалізується на захисті промислових мереж та пропонує набір функцій для виявлення та протидії загрозам у середовищах критичної інфраструктури, що робить її найкращим рішенням для захисту промислових мереж.

Microsoft Defender для IoT – це комплексне рішення безпеки, спеціально розроблене для захисту кінцевих точок у середовищах IoT. Воно забезпечує надійний захист від різноманітних загроз, націлених на пристрої IoT, і є найкращим для захисту кінцевих точок завдяки розширеним можливостям визначення та зменшення ризиків на рівні пристрою.

Google IoT Core – це керована служба, яка дозволяє користувачам підключатися, керувати та завантажувати дані з пристроїв, розташованих у всьому світі. Здатність цього інструменту пропонувати повністю інтегровану послугу для всіх аспектів управління даними IoT узгоджується з його позицією як найкращого для керування, обробки та зберігання даних, подолання розриву між різними пристроями IoT та інтелектуальними даними, потрібними сучасному бізнесу.

4.4 Рішення для забезпечення безпеки IoT методом життєвого циклу

Розширення сфер застосування Інтернету речей, приріст підключених пристроїв та впровадження технології у повсякденність людей і великих компаній дозволяють кінцевим користувачам отримати значну перевагу у функціонуванні процесів та систем, особливо, виробничих. Проте, активне застосування IoT викликає ряд нових проблем, які не завжди вдається вирішити традиційними методами захисту та стандартними готовими рішеннями.

В роботі пропонується використовувати перспективний підхід, а саме забезпечення безпеки методом життєвого циклу IoT (рис.4.4). Перевагою цього методу є інтеграція методу на всіх етапах впровадження безпеки IoT – від

виявлення пристроїв IoT та ризиків, що їх охоплюють, до безпекових заходів, які забезпечують належний захист від відомих та невідомих загроз [30].

Рисунок 4.4 –Життєвий цикл безпеки IoT

Метод життєвого циклу представляє собою п’ятикомпонентну структуру, процеси кожної компоненти наведено в табл. 4.2.

Таблиця 4.2 – Компоненти методу життєвого циклу

№	Компонента	Основні процеси
1	Визначення та проявлення усіх пристроїв IoT, що підключені до конкретної мережі	- виявлення датчиків, що під’єднанні до інфраструктури мережі IoT, - зчитування основних характеристик пристрою (марка, операційна система, програмне забезпечення, наявність портів, додатків, антивірусного устаткування тощо), - моніторинг нових, раніше не підключених пристроїв (виключаючи з цього процесу необхідність участі людини), - виявлення пристроїв з підозрілою активністю та реєстрація кількості вже визначених некорованих пристроїв.

Продовження табл. 4.2

№	Компонента	Основні процеси
2	Активний моніторинг пристроїв у режимі реального часу	- безперервний аналіз активності усіх підключених пристроїв для подальшої сегментації мережі, - детальний контроль за трафіками даних, а також для забезпечення адекватного навантаження на мережу, - інтеграція з декількома каналами даних виявленних загроз для проведення їхньої кореляції, - виявлення та повідомлення кінцевому користувачу про випадки аномальної поведінки пристроїв мережі Інтернету речей, - відстеження дінаміки ризиків, пов’язаних з пристроями IoT та оцінювання їх.
3	Рекомендації безпекових політик та автоматизо-ваний процес їхнього впровадження	- принцип нульової довіри під час впровадження безпекових політик, - застосування багаторівневої політики для групи пристроїв, - підтримка заборонених та дозволених індентифікаційних адрес, - відслідковування дотриманності політик безпеки пристроями та додатками незалежно від їх активності у мережі, - забезпечення автоматичного оновлення безпекових політик.
4	Належний рівень реагування та запобігання відомим загрозам	- адекватне виявлення шкідливого програмного забезпечення, - запобігання відомим загрозам, - блокування атак на пристрої IoT, - попередження атак, що використовують DNS для управляння і керування інформацією, - запобігання крадіжки даних.
5	Виявлення та запобігання невідомим загрозам	- моніторинг аномальної поведінки пристроїв на різних рівнях, - використання машинного навчання та краудсорсингової аналітики з моделюванням потенційних загроз.

Метод життєвих циклів підходить для впровадження у великі IoT-мережі, адже застосування рішення ґрунтується на принципах маштабованності та адаптивності, завдяки розрахунку можливого розширення мережі ще на етапі проектування, а також впливає на адаптацію мережі до змін навколишнього середовища та нових вимог.

Метод забезпечує високий рівень безпеки мережі IoT завдяки механізмам автономного та регулярного оновлення програмного забезпечення підключених пристроїв, виключаючи з цього етапу необхідність стороннього втручання, а також дотримання належних стандартатів та протоколів функціонування і експлуатації (наприклад, слідкує за відповідністю пристроїв один одному та вимогам, на яких базується IoT-мережа).

ВИСНОВКИ

Постійне зростання кількості підключених пристроїв до мереж IoT, активне впровадження новітніх технологій та розширення сфер їх застосування продукують велику кількість нових вразливостей систем Інтернету речей, якими можуть скористатися зловмисники, саме тому питання безпеки IoT-мереж не втрачають своєї актуальності.

В даній кваліфікаційній роботі було проведено дослідження засобів безпеки в мережах IoT.

В першому розділі проаналізовані еволюція IoT, актуальний стан та тенденції розвитку IoT у світі. Сучасні мережі IoT представляють собою цільну систему, до якої входить програмне забезпечення, розподільні пристрої, модулі комунікації, процесори та сенсори. Системи все частіше впроваджуються у різні сфери, зокрема, у промисловість, сільськогосподарське виробництво, логістику тощо, з метою оптимізації виробничих процесів та ресурсів.

В роботі було проведене дослідження актуального стану IoT в Україні. Однією із особливостей технології в Україні є її застосування у великій кількості стартапів та інноваційних проектах. Завдяки цьому країна входить у трійку найбільших стартап-індустрій Центральної та Східної Європи. В Україні активно впроваджують технології IoT у промисловий, аграрний та енергетичний сектори. Великі міста України також використовують IoT-системи, розвиваючи концепцію «розумних» міст, зокрема, впроваджуючи «розумні» транспортні та логістичні мережі, освітлення, екологічний моніторинг. Динаміка розвитку IoT в Україні має позитивні тенденції, проте економічне зниження та повномасштабна війна в країні значно знижують темпи розвитку та впровадження технології IoT.

В другому розділі роботи проведено аналіз концепції IoT та принципів, на базі яких мережі IoT функціонують. Детальний аналіз концепції продемонстрував, що фундаментом надійного та ефективного функціонування мережі IoT слугують архітектурні принципи, використання різноманітних протоколів зв’язку, принципи масштабованості, децентралізації та інтероперабельності, а також застосування принципів стандартизації. Комплексний підхід до роботи з даними, використання різноманітних

інтерфейсів та веб-порталів, управління енергоспоживанням і застосування різних підходів до обробки інформації мережею також забезпечують ефективну роботу IoT-системи. Зазвичай відбувається використання комбінацій різних підходів, вибір яких залежіть від вимог до мережі: обсягів даних, вимог до швидкості обробки інформації, вимог безпеки, доступності ресурсів мережі.

В роботі було проведено аналіз сучасних засобів, які використовуються у IoT-мережах. Сучасні засоби IoT представляють собою апаратні та програмні рішення, які комплексно використовуються для організації мереж IoT. Завдяки постійному розвитку мікроелектроніки, технологій зв'язку, зокрема, бездротових, сенсорних і програмних технологій створюються сприятливі умови для активного застосування мереж IoT у різних галузях.

Проведення порівняльного аналізу сучасних технологій зв'язку, які використовуються мережами IoT продемонструвало, що вибір комунікаційної технології для рішення Інтернету речей залежить від відстані між пристроями, пропускної здатності мережі, енергоспоживання та особливостей використання IoT-мережі.

У роботі розглянуті переваги технології IoT, а також визначені проблеми IoT, які суттєво впливають на рішення користувачів щодо доцільності впровадження та експлуатації IoT.

В третьому розділі роботи проведено аналіз проблем безпеки IoT. Визначені три основні проблемні області технології: безпекові проблеми пристроїв, комунікації, хмарних сховищ та платформ. В роботі наведені основні вразливості мереж Інтернету речей та проаналізовані найчастіші атаки на мережі IoT.

В четвертому розділі роботи на основі детального вивчення структури, принципів функціонування та найпоширеніших атак на мережі IoT, було проведено аналіз засобів захисту мереж IoT. В роботі проаналізовані різні елементи захисту мереж Інтернету речей, такі як: IDS/IPS системи , NGFW (міжмережні екрани нового покоління), IAM-системи, SIEM-платформи, системи управління вразливостями (VM), машинне навчання, шифрування даних, MDM-платформи, NFC-системи, засоби UBA. Кожен з цих засобів виконує свою ключову роль у забезпечені безпеки мереж IoT, що потребують комплексного захисту. Тому в роботі запропоновано використання комплексної багаторівневої системи захисту IoT. Кожен із 10 рівнів цієї системи враховує

всі наявні та потенційні проблеми безпеки мереж IoT та забезпечує належний рівень захисту на усіх етапах функціонування мереж Інтернету речей.

В роботі запропоновані рекомендації щодо захисту мереж Інтернету речей. Основою захисту мереж IoT може стати суворе дотримання принципів управління обліковими даними та паролями, а строго регламентований механізм регулярних оновлень програмного забезпечення обумовить безпечне функціонування мереж. Для виявлення та запобігання можливими вторгненням рекомендовано впровадити моніторинг безпеки мереж IoT у режимі реального часу. При цьому, розробка плану аварійного відновлення допоможе зберегти безперервність роботи критично важливих елементів мережі. Зазначені у роботі рекомендації в поєднанні з регулярним оновленням конфігурації мережі допоможуть максимально підвищити безпеку.

Виконано порівняльний аналіз десяти платформ захисту IoT. Розглянуті латформи забезпечують цілісність, доступність та конфіденційність даних під час їх переміщення між пристроями мережі Інтернету речей. Впровадження подібного технологічного рішення дозволяє запобігти несанкціонованому доступу та потенційним кіберзагрозам, підтримуючи роботу усієї мережі IoT.

В роботі також запропоновано використання перспективного підходу для забезпечення безпеки мереж IoT, який полягає у використанні методу життєвого циклу. Метод базується на принципах масштабованості та адаптивності мережі, і тому підходить до використання у великих мережах IoT. Цей метод враховує потенційне розширення мережі ще на етапі планування, впливає на адаптивний рівень мережі, а завдяки механізмам регулярного та автономного оновлення програмного забезпечення пристроїв підтримує високий рівень безпеки мереж IoT.

Результати цієї роботи можуть бути використані при проектуванні нових мереж IoT з підвищеним рівнем безпеки, модернізації та вдосконаленні вже наявних мереж IoT, а також розробці засобів забезпечення захищеності компонентів мереж IoT.

Часткові результати роботи було опубліковано [31] в збірнику тез одинадцятої міжнародної науково-технічної конференції «Проблеми інформатизації».

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Back End News. IDC: IoT investments to exceed $1 trillion in 2026. Backendnews.net. 23.06.2023. URL: https://backendnews.net/idc-iot-investments-to-exceed-1-trillion-in-2026/.

2. Євген П. Кіберзагрози для інтернету речей (IoT): захист смарт-пристроїв. Wezom.com.ua. 20.09.2024. URL: https://wezom.com.ua/ua/blog/kiberzagrozi-dlya-internetu-rechey-iot-zahist-smart-pristroyiv.

3. Ashton K. That ‘Internet of Things’ Thing. RFID Journal. 2009.

4. Internet of Things—An Introduction. 6G Enabled Healthcare Systems / V. Sai, H. Kim, B. Fong. Springer, 2024. С. 59–75.

5. Graziani R. IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6. Indianapolis : Cisco Press, 2017.

6. IoT devices have outstripped non-IoT connections – what’s next for IoT connectivity?. Iot-now.com. 03.08.2022. URL: https://www.iot-now.com/2022/08/03/122754-iot-devices-have-outstripped-non-iot-connections-whats-next-for-iot-connectivity/?cn-reloaded=1.

7. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges / A. Shah Syed та ін. Smart Cities. 2021. Т. 4, вип. 2 : AI Perspectives in Smart Cities and Communities to Enable Road Vehicle Automation and Smart Traffic Control. С. 429–475.

8. The Internet Of Things: Mapping The Value Beyond The Hype / J. Manyika та ін. McKinsey & Company, 2015. 144 с.

9. Балашова Л. «Vodafone Україна» домовляється з «Нафтогазом» про використання IoT сім-карт у розумних лічильниках. Forbes.ua. 12.12.2024. URL: https://forbes.ua/news/vodafone-ukraina-domovlyaetsya-z-naftogazom-pro-vikoristannya-iot-sim-kart-u-rozumnikh-lichilnikakh-12122024-25536.

10. Digital AgriBusiness. Latifundist.com. URL: https://latifundist.com/kompanii/1882-digital-agribusiness.

11. Central and Eastern European startups 2024 / A. Nemeth та ін. Dealroom.co. 03.2024. URL: https://dealroom.co/uploaded/2024/03/Dealroom-cogito-uniqa-vestbee-CEE-report-2024.pdf?x67760.

12. Погорілко М. 10 маловідомих, але перспективних українських стартапів. Mezha.medi. 03.06.2024. URL: https://mezha.media/articles/perspektyvni-ukrainski-startapy-10-rozrobok/.

13. Generect.com. URL: https://generect.com/.

14. Сиваківський Я. "Розумні" міста вже з'являються в Україні: які інновації впроваджуються. 24tv.ua. 10.06.2023. URL: https://24tv.ua/business/rozumni-mista-vzhe-zyavlyayutsya-ukrayini-yaki-innovatsiyi-vprovadzhuyutsya_n2329904.

15. Pallavi Sethi, Smruti R. Sarangi. Internet of Things: Architectures, Protocols, and Applications. Electrical and Computer Engineering. 2017.

16. Time-of-Flight 8x8 multizone ranging sensor with wide field of view. St.com. URL: https://www.st.com/resource/en/datasheet/vl53l5cx.pdf.

17. EVALUATION KIT BOARD BME688 Bosch Sensortec. Rcscomponents. URL: https://www.rcscomponents.kiev.ua/product/evaluation%20kit%20board%20bme688.html.

18. ICM-42688-V. TDK. URL: https://invensense.tdk.com/products/motion-tracking/6-axis/icm-42688-v/.

19. «Деметра-5»: у кінці 2016 року відбулися випробування вимірювального літального комплексу NEXUS 800 для виконання топозйомки. Geoguide. 09.02.2017. URL: http://www.geoguide.com.ua/news?page=7&id=1202.

20. MAX30101 Datasheet. Alldatasheet. URL: https://www.alldatasheet.com/datasheet-pdf/view/1338716/MAXIM/MAX30101.html.

21. Розуміння технології NB-IoT проти LTE-M. Dusuniot. 14.09.2022. URL: https://www.dusuniot.com/uk/blog/nb-iot-vs-lte-m-technology/.

22. Технологія LoRaWAN. Deps. URL: https://deps.ua/ua/knowegable-base/reference-information/66634.html.

23. Mohsen Soori, Behrooz Arezoo, Roza Dastres. Internet of things for smart factories in industry 4.0, a review. Internet of Things and Cyber-Physical Systems. 2023. T. 3. C. 192–204.

24. Petrosyan A. Annual number of Internet of Things (IoT) malware attacks worldwide from 2018 to 2022. Statista. 10.12.2024. URL: https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/.

25. Vallabhaneni R., Maroju A., Dontu S. Analysis on Security Vulnerabilities of the Modern Internet of Things (IOT) Systems. International Journal on Recent and Innovation Trends in Computing and Communication. 2024. С. 801–808.

26. Tenable Holdings. Tenable Cloud Risk Report Sounds the Alarm on Toxic Cloud Exposures Threatening Global Organizations. Globenewswire. 08.10.2024. URL: https://www.globenewswire.com/news-release/2024/10/08/2959763/0/en/Tenable-Cloud-Risk-Report-Sounds-the-Alarm-on-Toxic-Cloud-Exposures-Threatening-Global-Organizations.html.

27. Parnashree Saha. How You Can Effectively Manage IoT Security Challenges and Vulnerabilities?. Encryption Consulting. 07.11.2024. URL: https://www.encryptionconsulting.com/managing-iot-security-challenges-and-vulnerabilities/.

28. The IoT sweet spot – how much data is too much data?. ERP Today. 13.02.2022. URL: https://erp.today/the-iot-sweet-spot-how-much-data-is-too-much-data/.

29. Paulo Gardini Miguel. 25 Best IoT Security Platforms Ranked. The CTO Club. 21.12.2024. URL: https://thectoclub.com/tools/best-iot-security-platform/.

30. Lim A. The Solution to Secure Across the 5 Stages of the IoT Security Lifecycle. Pupuweb. 19.10.2020. URL: https://pupuweb.com/solution-secure-stages-iot-security-lifecycle/.

31. Поддельський В., Чеботарьова Д. Аналіз загроз на мережі розумного будинку. Тези доповідей одинадцятої міжнародної науково-технічної конференції «Проблеми інформатизації», 16 – 17 листопада 2023 р., Баку – Харків – Бельсько-Бяла. 2023. 2. С. 64.