

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проєкту (роботи)

бакалавра

(ступінь вищої освіти (освітній ступінь))

на тему «РОЗРОБКА ІОТ-СИСТЕМИ З ПІДВИЩЕНИМ РІВНЕМ
ЗАХИСТУ З ВИКОРИСТАННЯМ ТРМ МОДУЛЯ»

Виконав: студент 4 курсу, групи КНТ-511
спеціальності 123 Комп'ютерна інженерія

Освітня програма (спеціалізація)

Комп'ютерна інженерія

(код і назва спеціальності)

КОДАК І.В.

(прізвище та ініціали)

Керівник СКРУПСЬКИЙ С.Ю.

(прізвище та ініціали)

Рецензент ЄФИМЕНКО М.В.

(прізвище та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування вищого навчального закладу)

Факультет Комп'ютерних наук і технологій

Кафедра «Комп'ютерні системи та мережі»

Ступінь вищої освіти (освітній ступінь) бакалаврський

Спеціальність 123 Комп'ютерна інженерія
(код і назва)

Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва)

ЗАТВЕРДЖУЮ
Зав. кафедри _____ Кудерметов Р.К.
“14” квітня 2025 року

ЗАВДАННЯ НА ДИПЛОМНИЙ ПРОЄКТ СТУДЕНТУ

КОДАК Ірина Василівна

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) «Розробка IoT-системи з підвищеним рівнем захисту з використанням TPM модуля»

керівник проекту (роботи) СКРУПСЬКИЙ С.Ю., к. т. н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “08” квітня 2025 року № 151

2. Строк подання студентом проекту (роботи) 01.06. 2025 року

3. Вихідні дані до проекту (роботи) модуль ТРМ, протокол MQTT,

IBM Watson IoT Platform

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) _____

1) Опис предметної області

2) Розробка вимог до програмного забезпечення

3) Розробка IoT системи

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Слайди презентації

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	СКРУПСЬКИЙ С.Ю., к.т.н.. доцент		
Нормоконтроль	ПОЛЬСЬКА О.В., ст. викладач		

7. Дата видачі завдання 05.05. 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Опис предметної області	05.04.2025	
2	Принцип роботи Інтернету речей	10.05.2025	
3	Компоненти Інтернету речей	17.04.2025	
4	Вимоги безпеки в IoT	23.04.2025	
5	Особливості та ризики безпеки на рівнях архітектури	18.05.2025	
6	Розробка IoT системи	25.05.2025	
7	Оформлення отриманих результатів у ПЗ	26.05.2025	
8	Оформлення графічного матеріалу	29.05.2025	
9	Захист роботи	01.06.2025	

Студент Ірина КОДАК
(підпис) (ініціали та прізвище)

Керівник проекту (роботи) Степан СКРУПСЬКИЙ
(підпис) (ініціали та прізвище)

РЕФЕРАТ

ПЗ: 59 с., 19 табл., 14 рис., 14 джерел.

БЕЗПЕКА, ЗАХИЩЕНА МЕРЕЖА, КОНТРОЛЬ СТАНУ, КОНФІДЕНЦІЙНІСТЬ, МЕРЕЖЕВІ АТАКИ, РИЗИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Метою даної дипломної роботи є розробка системи для забезпечення захисту даних і пристроїв у середовищі Інтернету речей.

Для досягнення мети, поставлені такі задачі:

- визначити ключові компоненти Інтернету речей;
- розглянути еталонну архітектуру IoT;
- розглянути сервісно-орієнтовану архітектуру;
- провести порівняльний аналіз існуючих методів забезпечення безпеки в IoT-системах;
- спроектувати систему Інтернету речей із запропонованими методами забезпечення її безпеки.

У ході роботи проведено аналіз особливостей Інтернету речей, визначено потенційні загрози та розглянуто методи безпеки на різних рівнях системи. На основі цього було розроблено систему захисту даних і пристроїв IoT, у якій реалізовано запропоновані рекомендації та методи безпеки.

ABSTRACT

Explanatory note to the master's work: 59 p., 19 tables, 14 figures, 14 sources.

SECURITY, SECURE NETWORK, HEALTH MONITORING,
CONFIDENTIALITY, NETWORK ATTACKS, INFORMATION SECURITY RISK

The purpose of this thesis is to develop a system to ensure the protection of data and devices in the Internet of Things environment.

To achieve this goal, the following tasks have been set:

- identify the key components of the Internet of Things;
- to consider the IoT reference architecture;
- to consider the service-oriented architecture;
- conduct a comparative analysis of existing methods of ensuring security in IoT systems;
- to design an IoT system with the proposed methods of ensuring its security.

The study analyses the features of the Internet of Things, identifies potential threats, and considers security methods at different levels of the system. Based on this, a system for protecting IoT data and devices was developed, which implements the proposed security recommendations and methods.

ЗМІСТ

Вступ.....	9
1 Опис предметної області	11
1.1 Основні історичні дані про інтернет речей.....	11
1.2 Інтернет речей у сьогоденні.....	12
1.3 Принцип роботи інтернету речей	13
1.3.1 Компоненти SOA для IoT	15
1.3.2 Компоненти Інтернету речей (IoT).....	16
1.3.3 Еталонна модель Інтернету речей (IoT)	17
1.4 Висновки до розділу.....	18
2 Розробка вимог до програмного забезпечення	19
2.1 Проблеми інформаційної безпеки на сьогоднішній день.....	19
2.1.1 Вимоги до безпеки в IoT	20
2.1.2 Питання безпеки Інтернету речей	22
2.1.3 Забезпечення безпеки на сенсорному рівні	25
2.1.4 Безпека мережевого рівня	26
2.2 Пошук проблем безпеки на програмному та апаратному рівні Інтернету речей.....	27
2.3 Оцінка особливостей та ризиків безпеки на рівнях архітектури.....	33
2.3.1 Сенсорний рівень	33
2.3.2 Мережевий рівень	36
2.3.3 Рівень інтерфейсів	38
2.3.4 Особливості рівня служб	39
2.3.5 Міжрівневі загрози.....	41
2.4 Висновки до розділу.....	45
3 Розробка IoT системи.....	45
3.1 Діаграми варіантів використання	45
3.1.1 Функціональні блоки IoT	48
3.1.2 Моделі зв'язку IoT.....	49

3.1.3 API зв'язку IoT	49
3.2 Побудова системи	49
3.3 Реалізація методів безпеки.....	51
3.4 Висновки до розділу.....	56
Висновки.....	57
Перелік джерел посилання	58

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

CIoT	Consumer Internet of Things, Користувацький Інтернет речей
DDoS	Distributed Denial of Service, Розподілена відмова в обслуговуванні
IoT	Internet of Things, Інтернет речей
IoT-ARM	IoT Architectural Reference Model, Еталонна архітектурна модель IoT
IIoT	Industrial Internet of Things, Промисловий Інтернет речей
IEEE	Institute of Electrical and Electronics Engineers, Інститут інженерів електротехніки та електроніки
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission, Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія
RSA	Rivest-Shamir-Adleman, Криптографічний алгоритм
RFID	Radio Frequency Identification, Радіочастотна ідентифікація
SOA	Service-Oriented Architecture, Сервісно-орієнтована
QoS	Quality of Service, Якість обслуговування
WSN	Wireless Sensor Network, Бездротові сенсорні мережі

ВСТУП

Інтернет речей можна вважати наступним етапом розвитку Інтернету, що передбачає взаємодію фізичних пристроїв через мережу. Це дозволяє автоматизувати процеси, а також здійснювати дистанційне керування, значно спрощуючи повсякденне життя.

IoT швидко впроваджується у різні сфери, зокрема в розумні будинки, транспортні системи та розумні міста. Використання цієї технології сприяє підвищенню ефективності промислових процесів, медицини та інших галузей завдяки збору й аналізу даних за допомогою штучного інтелекту.

Водночас стрімке розширення IoT-технологій привертає увагу кіберзлочинців. Системи Інтернету речей стають дедалі розумнішими, інтегруючи новітні датчики, бездротові технології, хмарні сервіси та аналітичні інструменти. Згідно зі статистичними даними (statista.com), у 2021 році кількість IoT-пристроїв перевищила населення Землі та досягла 10,07 мільярдів підключень, а до 2030 року очікується їхнє зростання до 25,44 мільярда. Ці тенденції підтверджують, що IoT і надалі відіграватиме важливу роль у розбудові сучасної інфраструктури. Проте, поряд із перевагами, існують і значні виклики, зокрема питання безпеки.

Однією з головних загроз є кібератаки. Яскравим прикладом стала атака ботнету Mirai, що спрямовувалася на пристрої зі стандартними пароллями та завершилася масштабною DDoS-атакою на постачальника доменних імен Dyn, що вплинуло на роботу численних американських компаній [1].

Захист мереж, додатків та інфраструктури IoT має бути безперервним процесом, адже нехтування цим аспектом може спричинити значні збитки. Проте багато виробників не приділяють належної уваги безпеці через фінансові витрати на її впровадження, що включають як підвищені витрати на обчислення, так і зростання енергоспоживання автономних пристроїв.

Розвиток безпечного середовища IoT є критично важливим завданням. В іншому випадку подальший прогрес технологій може сповільнитися. Незважаючи

на те, що Інтернет речей суттєво покращує різні аспекти життя, недостатній рівень безпеки підриває довіру користувачів до цих рішень.

Розробка системи забезпечення безпеки даних та пристроїв у системі Інтернету речей.

Завдання для роботи:

- аналіз загроз та проблем, пов'язаних із Інтернетом речей;
- визначення особливостей та оцінка ризиків на різних рівнях IoT-систем;
- порівняння існуючих методів безпеки IoT;
- розробка рекомендацій та практичних заходів для підвищення безпеки даних і пристроїв;
- проєктування системи Інтернету речей із впровадженням механізмів безпеки.

Практична цінність: на основі аналізу загроз та методів захисту розроблено IoT-систему, що забезпечує мінімізацію кіберризиків та підвищує рівень безпеки Інтернету речей.

1 ОПИС ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Основні історичні дані про Інтернет речей

У 1990-х роках почали використовувати словосполучення "Інтернет речей". Одним із перших, хто ввів цей термін, був дослідник технологій RFID Кевін Ештон, який згодом заснував Auto-ID Labs. З часом з'явилися й інші назви для IoT, однак усі вони наголошували на необхідності підключення та сенсорних технологій для взаємодії фізичних об'єктів.

Протягом 1990-х років дослідження та обговорення IoT носили переважно теоретичний характер. Лише у 2000-х розпочався активний розвиток цієї технології. З'явилося багато проєктів та розробок, що сприяли поширенню IoT у споживчому та промисловому секторах [2].

У результаті сформувалися дві основні сфери застосування Інтернету речей (рис. 1.1):

- Consumer Internet of Things (CIoT) – орієнтований на кінцевого користувача;
- Industrial Internet of Things (IIoT) – спрямований на промислові галузі, корпоративний сектор та повсякденне життя людини.

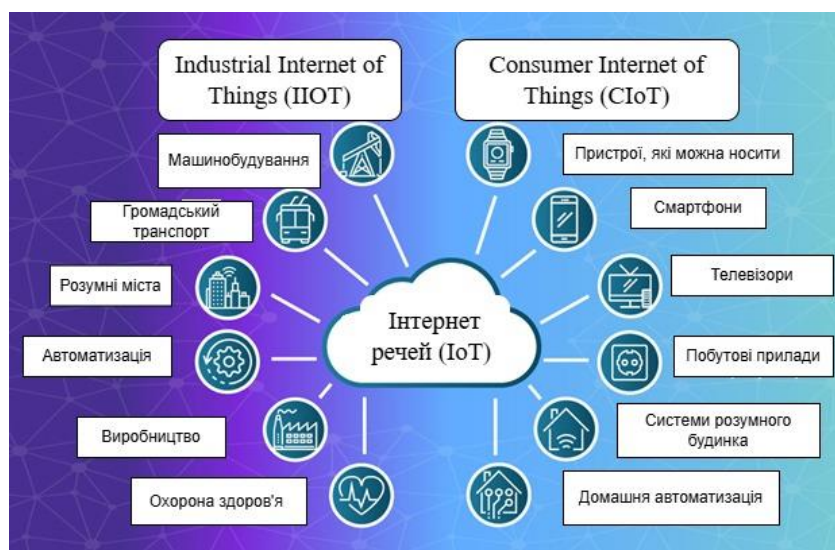


Рисунок 1.1 - Приклад IoT

Якщо дотримуватися загальноприйнятих визначень, то нові концепції, пов'язані з IoT, мають значну цінність для автономних та розподілених мереж. Важливу роль у цьому відіграють технології ідентифікації та обслуговування. Одним із таких розширень концепції IoT є "Інтернет усього" (Internet of Everything, IoE), який компанія Cisco використовує для позначення взаємодії IoT-пристроїв зі смартфонами, комп'ютерами та іншими підключеними пристроями.

1.2 Інтернет речей у сьогоденні

Фізичні об'єкти, що взаємодіють між собою або із зовнішнім середовищем через передачу даних по мережі, утворюють систему, відому як Інтернет речей (IoT). У сучасному світі ця технологія забезпечує машинну взаємодію (M2M), комунікацію між людиною та машинами, а також інтеграцію людини з навколишнім середовищем [3].

З розвитком нових протоколів зв'язку та збільшенням кількості розумних пристроїв IoT еволюціонує у напрямку об'єднання автономних і розумних мереж. Залучення людини до системи IoT відкриває нові можливості в охороні здоров'я та підвищенні готовності до надзвичайних ситуацій. Завдяки датчикам система IoT зможе оперативно реагувати на події та передавати важливу інформацію, що впливатиме на підприємства, медицину, якість життя та бізнес. Серед основних можливостей Інтернету речей:

- інтегроване середовище - для взаємодії фізичних об'єктів, яке розширює канали зв'язку та надає дані про пульс, місцезнаходження, серцебиття тощо;
- віддалений доступ - для адміністраторів, що спрощує автоматизацію та управління;
- передача важливих даних - через IoT-пристрої, що знижує витрати на впровадження, розгортання та обслуговування систем.

Деякі приклади застосування IoT.

Підключені дороги (Connected Roadways) - IoT активно впроваджується в транспортні системи, що видно на прикладі безпілотних автомобілів Google, Uber, Яндекс. Завдяки інтеграції розумних систем автомобілі можуть ефективніше взаємодіяти з транспортною інфраструктурою, покращуючи безпеку та координацію руху.

Розумні фабрики (Connected Factory) - традиційні заводи поступово трансформуються в підключені фабрики, де датчики IoT допомагають вирішити такі завдання, як:

- усунення простоїв у виробництві,
- контроль якості продукції,
- виявлення неефективних виробничих процесів.

Розумні будівлі (Smart Connected Buildings) - IoT активно застосовується для створення розумних будівель, де сенсорні системи збирають та обробляють дані для підвищення ефективності управління. Завдяки автоматизації будівлі стають енергоефективнішими та безпечнішими.

Таким чином, Інтернет речей сприяє розвитку ключових сфер життєдіяльності, роблячи їх більш ефективними, зручними та безпечними.

1.3 Принцип роботи інтернету речей

Основними елементами Інтернету речей, що існують уже багато років, можна вважати віддалений виклик служб, сенсорні пристрої, комунікаційні мережі та обробку подій із врахуванням контексту. IoT прагне створити єдину мережу розумних об'єктів і людей, що можуть взаємодіяти та обмінюватися інформацією. Ключовою умовою для розподіленого середовища є повний взаємозв'язок між об'єктами, і саме IoT є яскравим прикладом такої взаємодії.

Архітектура IoT як цілісної системи має забезпечувати безперебійну роботу своїх компонентів, а головним фактором її проектування виступає

надійність. Вона також повинна поєднувати фізичний і віртуальний світи, забезпечуючи можливість швидкого відновлення після збоїв і масштабованість.

З розвитком мобільних технологій і повсюдним використанням смартфонів, мобільність та динамічна зміна місця розташування стали одними з головних аспектів IoT. Це означає, що сучасна архітектура повинна бути достатньо гнучкою, щоб правильно обробляти змінні взаємодії в межах всієї екосистеми. Використання високорівневої абстракції, що приховує складність реалізації та технічні обмеження, є важливою перевагою еталонних архітектур і моделей.

Однією з таких моделей є IoT-ARM (IoT Architectural Reference Model), яка зосереджена на розробці та перевірці інтегрованої мережевої архітектури Інтернету речей.

IoT-ARM відображає різні рівні функціонування системи, зокрема:

- рівень обслуговування, що включає події обробки й аналітики, систему виявлення служб та управління ресурсами;
- механізми об'єднання повідомлень, а також сервісну шину підприємства, що забезпечують зв'язок між фізичним і комунікаційними рівнями.
- управління API, яке використовується для визначення та спільного використання системних служб, а також надає веб-інтерфейси для управління доступом.

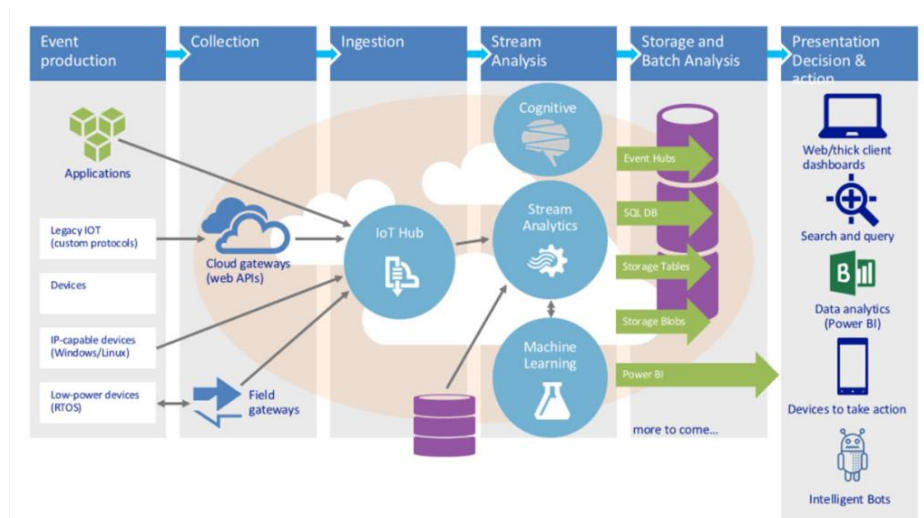


Рисунок 1.2 - Базова архітектура IoT

Таким чином, архітектура IoT повинна бути масштабованою, адаптивною до динамічних змін та забезпечувати ефективний обмін інформацією між усіма її компонентами.

Сервіс-орієнтована архітектура (SOA) відіграє ключову роль в інтеграції IoT, забезпечуючи ефективну взаємодію між різноманітними пристроями та користувачами.

1.3.1 Компоненти SOA для IoT

SOA-архітектура розділяє систему на чотири основні рівні, кожен з яких виконує важливу функцію:

- сенсорний рівень – відповідає за взаємодію з фізичними пристроями, зчитування даних та визначення стану речей;
- мережевий рівень – створює інфраструктуру для провідного та бездротового з'єднання між пристроями, сервісами та користувачами;
- службовий рівень – дозволяє створювати, керувати та використовувати сервіси, необхідні для функціонування IoT-системи;
- рівень інтерфейсів – забезпечує можливість взаємодії користувачів та додатків із сервісами системи через різні методи доступу.

Переваги використання SOA в IoT (рис.1.3):

- гнучкість та масштабованість – завдяки слабкому зв'язку між підсистемами, кожен сервіс можна легко замінювати, доповнювати або використовувати повторно;
- надійність – у разі збою одного з компонентів решта системи продовжує функціонувати, що є важливим для критичних IoT-додатків;
- абстракція та зручність взаємодії – користувачам і розробникам простіше працювати з протоколами та рівнями системи.

Бездротові сенсорні мережі (WSN) широко застосовують SOA через її високий рівень абстракції та підтримку розподілених систем. Впровадження SOA в IoT дозволяє значно підвищити ефективність взаємодії між пристроями та забезпечити їхню безперебійну роботу в автономних умовах [4].

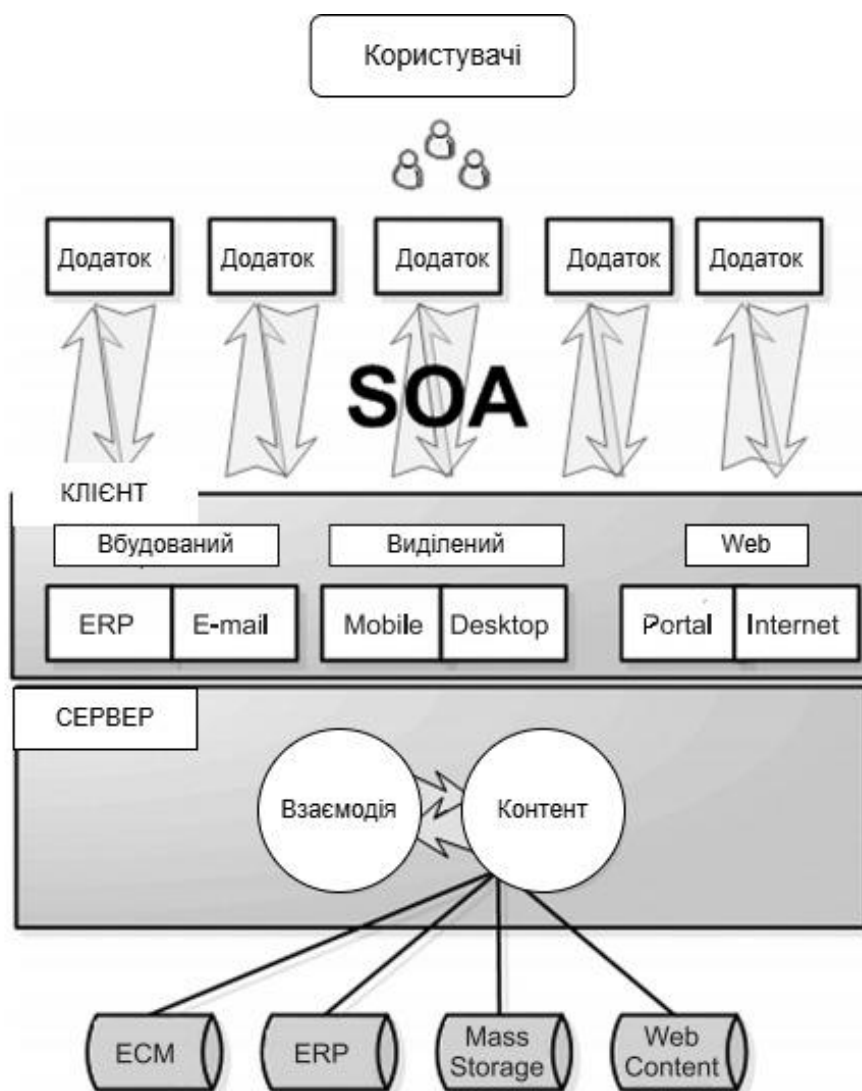


Рисунок 1.3 - Сервіс-орієнтована архітектура IoT

Таким чином, завдяки SOA, Інтернет речей отримує можливість створення складних, розподілених та гнучких сервісів, які адаптуються до змінних умов використання та потреб користувачів.

1.3.2 Компоненти Інтернету речей (IoT)

Інтернет речей складається з кількох ключових компонентів, кожен з яких виконує свою функцію в забезпеченні роботи системи [5]:

а) датчики та сенсори – збирають інформацію з навколишнього середовища:

- 1) вбудовані системи (Embedded Systems);
- 2) мікроелектромеханічні системи (MEMS);

- 3) ОС з мінімальним відгуком для критичних місць;
- б) сенсорні системи зв'язку – забезпечують передачу даних через:
 - 1) персональні мережі бездротового доступу (PAN);
 - 2) мережі зі слабкими каналами зв'язку;
- в) LAN-мережі – локальні мережі на основі IP (найпоширеніший стандарт – 802.11 WiFi);
- г) шлюзи та маршрутизатори – ключові пристрої для взаємодії IoT-систем;
- д) глобальні обчислювальні мережі:
 - 1) оператори стільникового зв'язку;
 - 2) LPWAN-провайдери (Low Power Wide Area Network);
 - 3) супутникові мережі;
- ж) хмара (Cloud) – забезпечує зберігання, обробку та аналіз даних;
- к) безпека IoT – охоплює захист даних, автентифікацію, цілісність системи та інформаційну безпеку.

1.3.3 Еталонна модель Інтернету речей

Компанія Cisco запропонувала семирівневу еталонну модель IoT, яка допомагає структурувати систему:

- фізичний рівень – містить датчики, пристрої та виконавчі механізми;
- мережевий рівень – забезпечує комунікацію між пристроями;
- обчислювальний рівень – обробляє та зберігає дані;
- інформаційний рівень – проводить аналітику та розпізнає патерни в даних;
- прикладний рівень – взаємодія з користувачем через додатки;
- управління рівнем – відповідає за безпеку, контроль доступу та оновлення систем;
- бізнес-рівень – застосовує IoT для вирішення бізнес-завдань та прийняття рішень.

Ця модель допомагає забезпечити масштабованість, надійність та ефективне управління IoT-системами.

В таблиці 1.1 представлено типову модель ієрархії IoT.

Таблиця 1.1 - Модель ієрархії IoT

Рівні	Характеристики
Фізичні пристрої та контролери	Пристрої кінцевої точки, експоненціальне зростання
Зв'язок	Надійність, своєчасна передача, комутація та маршрутизація
Туманні обчислення	Перетворення даних в інформацію, яка може бути ефективною
Накопичення даних	Зберігання даних, постійні та перехідні дані
Абстракція даних	Семантика даних, цілісність даних до програми, стандартизація даних
Додатки	Значущі інтерпретації та дії даних
Співробітництво і процеси	Люди, процеси, розширення можливостей та співпраця

Для проєктування Інтернету речей необхідно використовувати комунікаційні протоколи та відповідну інфраструктуру. Третій рівень, відомий як «туманні обчислення», виконує ключові функції – перетворення даних та аналітику на рівні обробки інформації. Саме ці дані стають основою для подальших дій.

Перші три рівні моделі відповідають за рух даних, тоді як вищі рівні зосереджені на отриманій інформації. У «туманних обчисленнях» обробка даних може здійснюватися в режимі реального часу, що підвищує їхню цінність та ефективність взаємодії процесів і людей із системою IoT.

1.4 Висновки до розділу

Сучасний Інтернет речей зазнав значної трансформації і тепер розглядається не лише як мережа взаємопов'язаних пристроїв, а як ціла парадигма, що потребує безперервної інтеграції, зв'язку та аналізу пристроїв. Важливими аспектами цієї концепції стали сумісність, інтеграція та підключення

численних гібридних мереж IoT.

У першому розділі основна увага була зосереджена на таких ключових завданнях:

- визначення основних компонентів Інтернету речей;
- аналіз еталонної архітектури IoT;
- розгляд SOA-архітектури;
- огляд еталонної моделі IoT-систем.

2 РОЗРОБКА ВИМОГ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Проблеми інформаційної безпеки на сьогоднішній день

Доступ до інфраструктури IoT та персональних даних можна отримати через майже будь-який підключений пристрій IoT. Ризики, пов'язані з Інтернетом речей, набувають нового рівня через сумісність пристроїв, програмне забезпечення та автономне прийняття рішень. Це створює потенційні вразливості та лазівки в системах безпеки, що робить захист даних та конфіденційність одним із ключових пріоритетів (рис. 2.1).

Об'єднання мобільних мереж, соціальних мереж, Інтернету та різних розумних об'єктів створює концепцію IoT, що надає користувачам різноманітні послуги та додатки (рис. 2.2).

Безпека на всіх рівнях безпосередньо впливає на успіх IoT систем, адже вона покращує взаємодію об'єктів, їх надійність та сумісність. Інтернет речей досяг такого рівня розвитку, коли здатен з'єднувати різні простори, зокрема цифровий та фізичний, де різноманітні датчики взаємодіють із фізичним середовищем. Ці датчики активно застосовуються у всьому - від іграшок до медичних систем, що підтверджує, як вразливості цифрового світу можуть впливати на наш реальний світ [6].

Six principles of IoT Cyber Security across the stack

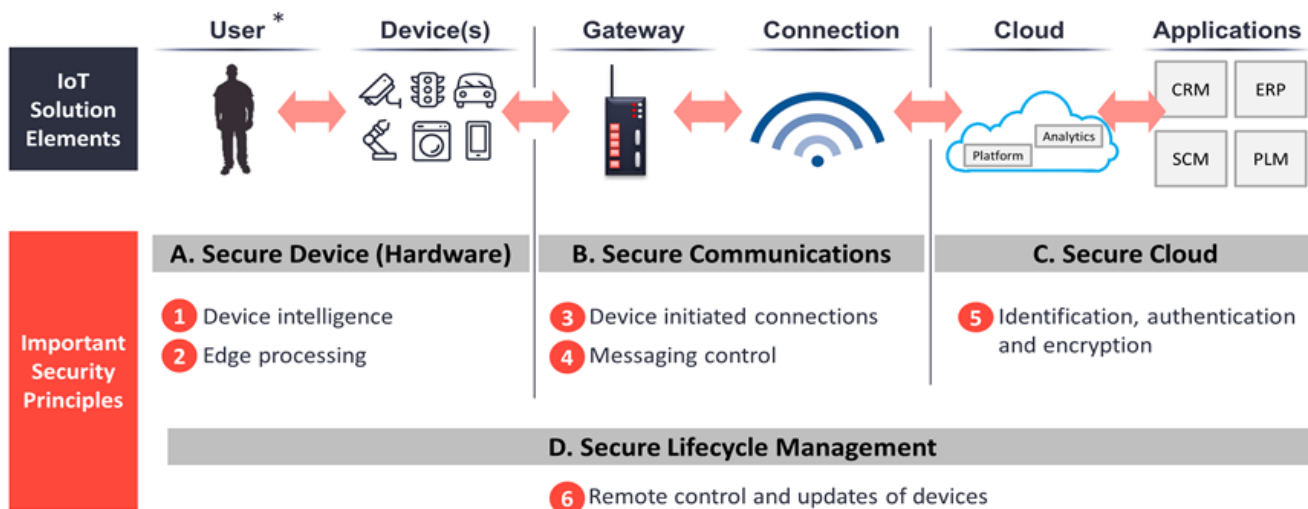


Рисунок 2.1 - Типові проблеми безпеки IoT

Система може бути визнана успішною лише тоді, коли вона забезпечує гарантії безпеки від потенційних вразливостей. Успіх додатків та інфраструктури IoT значною мірою залежить від здатності гарантувати безпеку та мінімізувати вразливості.

2.1.1 Вимоги до безпеки в IoT

Інтернет - це величезна кількість нових інструментів, які вбудовуються в організаційну інфраструктуру або в систему IoT. Кожен підключений пристрій може стати потенційним входом до інфраструктури Інтернету або особистих даних. Дані з цих пристроїв можуть бути проаналізовані й використані для створення невидимих посилань, які загрожують конфіденційності осіб або організацій.

Проблеми безпеки та конфіденційності в IoT є дуже важливими, але ризики, що з ними пов'язані, переходять на новий рівень. Сумісність, гібридні програми та автономне прийняття рішень створюють складності, прогалини в безпеці та нові вразливості.

Ризики захисту даних виникають у IT, коли складність систем може спричинити високу вразливість у зв'язку з наданими послугами. В Інтернеті речей

значна частина інформації пов'язана з особистими даними, такими як дата народження, місце розташування, бюджет тощо. Ризики, пов'язані з використанням таких даних, становлять один із аспектів проблем великих даних. Інтернет речей має бути реалізований законним, етичним, соціально та політично прийнятним способом з урахуванням юридичних, технічних і бізнесових аспектів.

Безпека була важливою проблемою з самого початку, але важливі питання безпеки даних та конфіденційності ще не мають чітких відповідей. Проблеми безпеки даних та конфіденційності не є новими для Інтернету речей, оскільки подібні питання вже вирішувалися на етапі впровадження RFID.

Незважаючи на те, що нове покоління RFID-міток є більш безпечним, ризики, пов'язані з Інтернетом речей, зростуть на новий рівень через сумісність гібридних додатків та вразливості автономної безпеки, що змушує до комплексного підходу в прийнятті рішень.

Діаграма оцінки кількості підключених IoT пристроїв (рис. 2.2) демонструє тенденції по всьому світу з 2019 до 2030 року за даними сайта [statista.com](https://www.statista.com) [7].

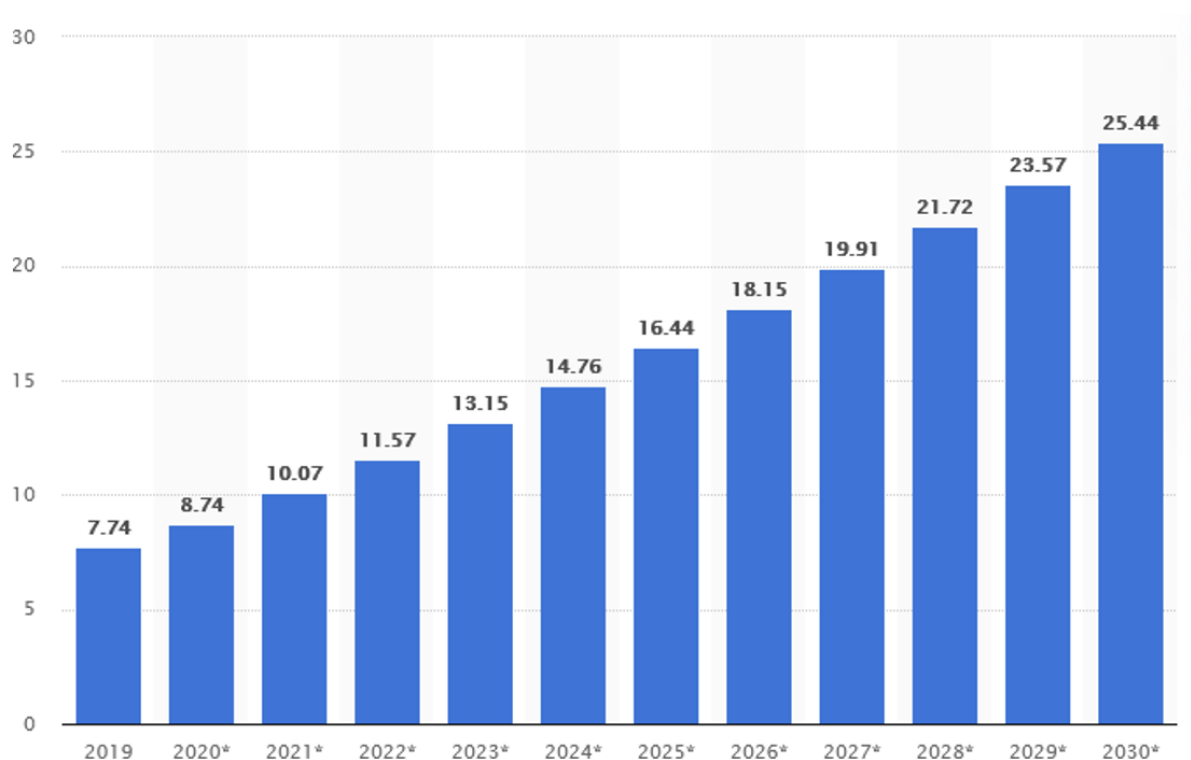


Рисунок 2.2 - Діаграма оцінки кількості підключених IoT пристроїв

2.1.2 Питання безпеки Інтернету речей

На рисунку 2.3 відображені основні вимоги до безпеки системи, які включають шість основних критеріїв:

- критерій конфіденційності - дані повинні бути захищені та доступні тільки уповноваженим особам або системам;
- критерій цілісності - забезпечення того, щоб дані залишалися надійними, без змін або пошкоджень, несанкціонованих змістом;
- критерій доступності - дані повинні бути доступні у будь-який час і в будь-якому місці, де це необхідно;
- критерій безвідмовності - система повинна забезпечувати надійний аудиторський шлях, що дозволяє відслідковувати всі операції для запобігання відмов і виявлення порушень;
- критерій достовірності - компоненти системи повинні бути здатні підтвердити свою ідентичність, щоб уникнути підробок або несанкціонованого доступу;
- критерій безпека - служба або система не повинна автоматично бачити дані клієнтів, гарантуючи захист приватності користувача.

Ризики захисту даних виникають, коли об'єкти в інтернеті речей збирають і узагальнюють фрагменти даних, що містять особисту інформацію. Ці дані можуть бути перетворені на корисну інформацію через зіставлення точок, таких як місце, час і періодичність, які формують контекст для аналізу подій. Це є одним з викликів обробки великих даних, і фахівці з безпеки повинні враховувати потенційні ризики для конфіденційності, які можуть виникати через збір та аналіз таких даних. Основні проблеми безпеки в контексті IoT стосуються конфіденційності даних, секретності та довіри.

Конфіденційність даних включає:

- недостатня аутентифікація/достовірність;
- небезпечні інтерфейси (Інтернет, мобільні пристрої тощо);
- відсутність транспортного шифрування;
- проблеми із збереженням конфіденційності;

- управління доступом.



Рисунок 2.3 - Вимоги до безпеки системи IoT

Секретність включає:

- захист даних та управління ризиками інформаційного забезпечення;
- секретність за замовчуванням;
- політика конфіденційності;
- відстеження/профілювання/незаконна обробка даних.

Довіра, це:

- система управління особистими даними;
- небезпечне програмне забезпечення/прошивки;

- забезпечення безперервності та доступності послуг;
- шкідливі атаки на пристрої та системи IoT;
- втрата перевірки користувача/складність у прийнятті рішень.

Для демонстрації вимог до безпеки в Інтернеті речей, можна змоделювати архітектуру IoT, яка складається з чотирьох рівнів: сенсорного, мережевого, рівня служб та рівня інтерфейсів. Кожен з цих рівнів має забезпечити належне управління безпекою, таке як контроль доступу, інструменти автентифікації, збереження цілісності даних та конфіденційності, захист від вірусів та атак.

У таблиці 2.1 наведено узагальнені та найважливіші проблеми безпеки в IoT.

Сучасні виробничі об'єкти та смарт-міста, які з'єднані в єдину платформу, вимагають створення оптимальної архітектури безпеки пристроїв IoT.

Ця архітектура повинна дозволяти відстежувати кожен підключений пристрій, попереджати про можливий зловмисний доступ, а також захищати або відключати пристрої в разі загрози. Тому надзвичайно важливим є розробка та використання стандартів у сфері IoT.

В області стандартизації на всіх рівнях IoT активно працюють деякі великі організації, зокрема IEEE та ISO/IEC.

Таблиця 2.1 - Розповсюджені вразливості в Інтернеті речей

Проблеми безпеки	Рівень інтерфейсів	Рівень служб	Мережевий рівень	Сенсорний рівень
Небезпечний веб-інтерфейс	+	+	+	
Недостатня автентифікація/авторизація	+	+	+	+
Небезпечні мережеві послуги		+	+	
Відсутність транспортного шифрування		+	+	
Проблема конфіденційності		+	+	+
Небезпечний хмарний інтерфейс	+			

Продовження таблиці 2.1

Проблеми безпеки	Рівень інтерфейсів	Рівень служб	Мережевий рівень	Сенсорний рівень
Небезпечний мобільний інтерфейс	+		+	+
Небезпечність конфігурації	+	+	+	
Небезпечне ПЗ/прошивка	+		+	
Погана фізична безпека			+	+

2.1.3 Забезпечення безпеки на сенсорному рівні

Цей рівень можна описати як точку перехрестя між людьми, місцями та речами. Він включає як прості інструменти, такі як термометри і лампочки, так і більш складні пристрої, наприклад, медичне обладнання чи виробничі пристрої.

Для забезпечення повної реалізації безпеки необхідно, щоб вона була впроваджена безпосередньо у пристроях. Це означає, що інструменти IoT повинні мати можливість підтвердження своєї ідентичності для підтримки довіри, а також використовувати підписання та шифрування для забезпечення цілісності даних і обмеження збереження даних локально з метою захисту особистої інформації [8].

Модель безпеки пристроїв повинна бути достатньо суворою, щоб запобігти несанкціонованому доступу, але водночас достатньо гнучкою, щоб дозволяти тимчасову, безпечну та спеціалізовану взаємодію між людьми та іншими пристроями.

Пристрої Інтернету речей будуть присутні у всіх аспектах нашого оточення, що підвищує важливість розробки системи захисту від несанкціонованого доступу до цих пристроїв. Це дозволить знизити ймовірність витоку конфіденційної інформації, такої як особисті дані, криптографічні ключі та облікові дані. Оскільки пристрої IoT мають тривалий термін служби, важливо передбачити регулярні оновлення програмного забезпечення, щоб уникнути використання вразливостей і експлойтів, які можуть виникнути після випуску певних пристроїв на ринок.

2.1.4 Безпека мережевого рівня

Цей рівень відповідає за з'єднання та обмін даними між пристроями Інтернету речей і хмарними службами. У цьому контексті зв'язок в Інтернеті зазвичай включає комбінацію приватних і публічних мереж, тому питання безпеки стають особливо актуальними. Цей рівень забезпечує найкраще розуміння безпеки в системах IoT, оскільки технології шифрування, такі як TLS/SSL, є ефективними рішеннями для захисту даних.

Основною проблемою є реалізація криптографічних методів на пристроях з обмеженими ресурсами, наприклад, 8-бітових мікроконтролерах з обмеженою оперативною пам'яттю. Наприклад, для Arduino Uno шифрування даних за допомогою 1024-бітових ключів RSA займає близько 3 хвилин, тоді як використання алгоритму цифрового підпису на основі еліптичних кривих з такою ж довжиною ключа дає змогу зашифрувати те саме корисне навантаження за 0,3 секунди. Це підкреслює, що обмежені ресурси пристроїв не повинні використовуватися як виправдання для ігнорування аспектів безпеки в продуктах IoT.

Цей рівень відповідає за систему управління IoT і бере на себе відповідальність за інтеграцію пристроїв, користувачів, політик і правил, а також організацію автоматизації на різних пристроях. На цьому рівні критично важливим є забезпечення високого рівня контролю доступу, управління ідентифікацією пристроїв і користувачів, а також визначення дій, які мають дозвіл на виконання.

Для досягнення безпеки необхідно вести чіткий аудиторський слід змін для всіх користувачів і пристроїв, щоб уникнути спростування дій, здійснених в системі. Ці дані також можуть бути використані для виявлення скомпрометованих пристроїв шляхом аналізу аномальної поведінки. Аналіз великих даних, зібраних з пристроїв IoT, є однією з найцінніших складових у системі.

Підтримка конфіденційності є пріоритетом для державних установ, таких як Федеральна торгова комісія в США і Агентство Європейського Союзу ENISA. Вони випускають інструкції для захисту IoT, які включають вимоги до безпеки,

зокрема щодо чіткого сповіщення про використання даних, контролю за ними, а також зберігання даних клієнтів у хмарних службах із захистом через шифрування за допомогою ключів, наданих замовником. При аналізі сукупних даних між клієнтами дані повинні бути анонімізовані для забезпечення конфіденційності.

На рівні інтерфейсів виникає значна кількість проблем, оскільки забезпечення безпеки IoT повинно враховувати унікальні особливості кожного рівня. Першочерговим завданням є впровадження надійних заходів безпеки для пристроїв IoT. Навіть малогабаритні пристрої з обмеженими ресурсами повинні бути розроблені таким чином, щоб підтримувати конфіденційність, цілісність і довіру під час обміну даними в мережі. Останнім важливим аспектом є необхідність досягнення балансу між конфіденційністю користувачів і захистом бізнесових даних, щоб не порушувати приватність жодної зі сторін.

2.2 Пошук проблем безпеки на програмному та апаратному рівні Інтернету речей

Безсумнівно, переваги та можливості нових технологій швидко стануть частиною нашого повсякденного життя. Концепція Інтернету речей також розповсюджується на такі інновації, зокрема, в контексті розвитку інтелектуальних міст. Однак із цим виникають проблеми поширення нових технологій, що супроводжуються очевидними перевагами. Одна з головних проблем полягає в тому, що виробники інтернет-компонентів часто не надають достатньої уваги питанням інформаційної безпеки, які виникають при використанні окремих компонентів системи та програмного забезпечення.

Випуск великої кількості виробників з комунікаційним і контрольним обладнанням підвищує питання сумісності компонентів складних систем і можливість їх роботи без ризику несанкціонованого доступу, витоку або доставки

конфіденційної інформації. Речі, що входять до Інтернету речей, є не лише гаджетами, а й численними пристроями, кількість яких значно перевищує кількість ПК, ноутбуків та смартфонів, виходячи за межі захищеного корпоративного середовища.

Питання безпеки залишалося актуальним багато років, однак за останні роки спостерігається зростаючий інтерес до цієї теми в сфері IoT. Наприклад, згідно з дослідженням Microsoft 2019 року, 19% експертів визнали, що безпека є однією з найважливіших проблем, які потрібно вирішувати [9].

Основними питаннями залишаються пошук правильних IP-рішень, виділення коштів на спеціалізованих працівників, недостатня кількість знань по цій темі, а також складнощі у виборі правильних рішень для забезпечення безпеки/

Дослідження показали, що більшість експертів зосереджуються на проблемах безпеки на мережевому рівні, зокрема, 43% респондентів зазначають, що саме цей рівень найбільше турбує їх у контексті IoT-безпеки (рис. 2.4).

<i>Перехід до контролю на рівні ідентифікації</i>	<i>23%</i>
<i>Зміна паролів/облікових даних</i>	<i>24%</i>
<i>Безпечне надання пристроїв в Інтернет</i>	<i>30%</i>
<i>Оновлення прошивок пристроїв</i>	<i>31%</i>
<i>Своєчасне оновлення ПЗ</i>	<i>32%</i>
<i>Проведення тестування пристроїв</i>	<i>32%</i>
<i>Проведення комплексних програм навчання</i>	<i>33%</i>
<i>Оновлення протоколів шифрування</i>	<i>34%</i>
<i>Забезпечення безпеки для кожного пристрою</i>	<i>36%</i>
<i>Управління кожним пристроєм</i>	<i>38%</i>
<i>Забезпечення безпеки на рівні мережі</i>	<i>43%</i>

Рисунок 2.4 - Актуальність проблем безпеки

Багато недооцінено захищених пристроїв полегшують проведення DDoS-атак, де різні пристрої можуть бути використані для нападу на корпоративні системи. Часто ці пристрої працюють з пароллями "за замовчуванням", що є серйозною вразливістю, що сприяє утворенню ботнетів, таких як Mirai.

Сила організованої атаки Mirai на вебсайт журналіста В. Krebs, який створив його для розслідування продажу ботнет-услуг, досягла піка в 665 Гбіт/с, при цьому використовувалися лише інтелектуальні камери спостереження. Це показує важливість вивчення загроз безпеки в IoT, щоб створити перелік рекомендацій для захисту таких систем.

Сьогодні кількість пристроїв, підключених до Інтернету речей, значно перевищує кількість людей на планеті. Ці пристрої можуть бути як інтелектуальні годинники, так і RFID-зчитувачі. Обмін даними через різноманітні мережеві та хмарні платформи є важливою частиною IoT-систем. Отримання інформації в реальному часі є передумовою для трансформації всіх сфер IoT. Інтернет речей сприяє позитивним змінам у багатьох галузях, таких як охорона праці, здоров'я, бізнес, а також у вирішенні глобальних екологічних і гуманітарних проблем.

Ця технологія орієнтована на використання невеликої кількості енергії для обчислень і енергозберігаючих інструментів при виконанні простих завдань, наприклад, у розумному будинку чи місті. Інші застосування можуть включати геоінформаційні та інші розподілені системи. У таких системах управління пристроями відрізняється, оскільки при використанні M2M (Machine-to-Machine) взаємодія людина може не бути необхідною, на відміну від використання комп'ютерів або інших розумних пристроїв.

За прогнозами, до кінця 2021 року кількість пристроїв IoT, інтегрованих у систему, перевищить 16 мільярдів, що удвічі більше за населення Землі. Безпека цих систем стає критично важливою не лише для кінцевих користувачів, а й для величезних потоків даних, що виникають при M2M взаємодії.

Виробники компонентів IoT часто ігнорують питання безпеки. Причиною є високі витрати на енергію і необхідність знижувати ці витрати для забезпечення автономності пристроїв, таких як батареї. Більш того, додавання безпеки підвищує вартість рішень на ринку. Після детального розгляду проблем можна виділити основні загрози в IoT-системах. Проблеми безпеки є результатом порушення наскрізного принципу інформаційної безпеки, що є основною проблемою, яку помітили експерти.

Принцип наскрізної безпеки повинен бути врахований на всіх етапах створення IoT-продукту, а після завершення розробки пристрою важливо забезпечити підтримку інформаційної безпеки до кінця його терміну служби. Дослідження показали кілька ключових проблем, з якими стикаються розробники та користувачі IoT [10]:

- ігнорування вимог безпеки з боку власників пристроїв: багато користувачів не змінюють паролі за замовчуванням, що дозволяє зловмисникам отримати доступ до пристроїв;
- проблеми з шифруванням трафіку - 70% пристроїв не забезпечують шифрування бездротового трафіку;
- вразливості веб-додатків: близько 60% веб-додатків IoT пристроїв мають уразливості, пов'язані з міжсайтовим скриптингом;
- слабкі паролі: більшість пристроїв мають недостатньо надійні паролі;
- збір даних без відома користувача: 90% пристроїв IoT збирають дані без дозволу власника;
- велика кількість вразливостей: дослідження показали, що IoT пристрої можуть мати понад 20 різних уразливостей.

Висновок: відсутність належної безпеки у всіх компонентах IoT-системи. Зокрема, існують проблеми з живленням пристроїв, сертифікацією та стандартизацією архітектур, аутентифікацією, відсутністю оновлень ПЗ та ОС, захистом від атак і використанням незахищених хмарних інфраструктур.

На початку 2019 року, група дослідників за допомогою "пасток" для зловмисників (honeypots) зафіксувала 276 тисяч унікальних атак і 105 мільйонів неунікальних атак. Згідно з результатами дослідження, кількість атак збільшилася в 7 разів порівняно з 2018 роком. Зловмисники створюють нові ботнети, оскільки поки не існує ефективних рішень для боротьби з цими загрозами.

Технічні зловмисники активно використовують різні типи атак, збираючи заражені пристрої з різних мереж для проведення DDoS-атак або створення власних проксі-серверів для інших шкідливих дій (табл.. 2.2).

Таблиця 2.2 - Ширина DDoS – атаки

Викорис- тання пристроїв	Доступні пристрої					
	1 %	10 %	25 %	50 %	75 %	100 %
1	2	3	4	5	6	7
1 %	34,28	342,83	908,96	1815,56	2721,83	3629,21
10 %	364,78	3647,86	9089,63	18155,68	27218,37	36292,19
15 %	908,96	9089,63	22678,69	46457,41	68020,82	91794,43
50 %	1815,56	18155,68	46457,41	91794,43	147151,74	182989,22
75 %	2721,83	27218,37	68020,82	147151,74	214172,57	283194,39
100 %	3629,21	36292,19	91794,43	182989,22	283194,39	373676,83

Більшість атак на пристрої IoT мають потайливий характер, що значно знижує ймовірність їх виявлення користувачем. Це особливо вірно для атак, які не є складними чи комплексними системами, що ускладнює їх виявлення. Однією з найбільших загроз є ботнет Mirai, який складається з різноманітних шкідливих програм. Ці програми намагаються знайти вразливості в додатках та, у разі успіху, інфікують пристрій. Після цього ботнет використовує знайдені експлойти для подальшого контролю над інфікованими пристроями. Ще однією значною загрозою є троян Nyadrop, який складає 38% від усіх атак. Цей троян використовує метод брутфорсу для здійснення атак. Інший ботнет, Gafgyt, привернув увагу фахівців, проте його частка серед атак становить лише 2%.

Завдяки дослідженням експертів у сфері інформаційної безпеки, був складений порівняльний аналіз атак по різних країнах за 2022 та 2023 роки (таблиця 2.3).

У 2022 році найбільша кількість атак була зафіксована в Бразилії, Китаї та Японії, де частка атак склала 28%, 14% та 11% відповідно. У 2023 році ситуація змінилася, і лідерами стали Китай, Бразилія та Єгипет, з частками атак у 30%, 19% та 12%.

Таблиця 2.3 - Країни та відсоток ураження кібератаками

І-ша половина 2022		І-ша половина 2023	
Бразилія	28%	Китай	30%
Китай	14%	Бразилія	19%
Японія	11%	Єгипет	12%
США	5%	США	8%
Греція	5%	В'єтнам	4%
Туреччина	4%	Індія	4%
Мексика	4%	Греція	4%
Південна Корея	3%	Південна Корея	4%
Італія	2%	Японія	4%

Нижче наведено список основних типів атак, на основі яких розроблено рекомендації щодо посилення безпеки:

- технологія "Amplification" використовує LDAP і TCP протоколи для атаки, шляхом надсилання на сервер великої кількості повідомлень, що призводить до перевантаження веб-сайту;
- атака зміни маршруту в розподілених мережах включає зміну маршруту вузлів мережі, зокрема маршрутизаторів, що збільшує час доставки пакетів;
- вибіркова розсилка - атака, спрямована на часткове видалення пакетів. Вона залишає слід на вузлі і призводить до подальших негативних наслідків, таких як зменшення цілісності і доступності даних у мережі;
- технологія "Sinkhole Attack" використовується для збору трафіку через доступ до певного вузла, що дозволяє зловмиснику маніпулювати ним;
- атака Sybil створює збої в роботі маршрутизації та агрегації даних, намагаючись отримати контроль над вузлом за допомогою псевдоідентифікаторів, що імітують кілька вузлів одночасно;
- атака червоточини націлена на захоплення кількох вузлів мережі, що дозволяє зловмиснику створити шлях для перехоплення пакетів;
- флуд атака використовує пакети HELLO, щоб перевантажити мережу величезною кількістю повідомлень, що створює навантаження на обчислювальні

ресурси та інші критичні компоненти.

Рекомендації щодо забезпечення безпеки для користувачів IoT:

- надійне збереження паролів - користувач повинен замінювати стандартні паролі, адже багато IoT пристроїв за замовчуванням мають однакові паролі. Якщо заміна пароля неможлива, пристрій не слід підключати до IoT-мережі;
- надання привілеїв - для безпеки пристроїв необхідно забезпечити мінімальний рівень привілеїв, щоб обмежити можливості для злоумисників;
- тестування пристроїв - перед підключенням пристроїв до мережі важливо провести повну перевірку на справність, а також перевірити локальні та хмарні сервіси;
- ізоляція IoT - для захисту важливих ресурсів від IoT пристроїв слід створити окрему мережу для їх взаємодії та використовувати міжмережевий екран;
- керування трафіком IoT - важливо заблокувати небажаний вхідний трафік або провести сканування пристроїв на наявність відкритих портів, щоб запобігти можливості компрометації;
- використання шифрування - якщо пристрій підтримує шифрування трафіку, його обов'язково слід використовувати для забезпечення конфіденційності даних;
- придбання продуктів з підтримкою оновлень - купувати лише ті IoT пристрої, для яких ще доступні оновлення безпеки.

2.3 Оцінка особливостей та ризиків безпеки на рівнях архітектури

2.3.1 Сенсорний рівень

Пристрої, що входять до складу багаторівневої мережі, де відбувається постійний збір та обмін даними, забезпечують взаємодію між інтелектуальними мітками та сенсорними мережами [12]. Основні особливості цього рівня можна визначити через кілька ключових можливостей:

- зменшення витрат і ресурсів при проектуванні IoT-системи, де основними проблемами є обмеження ресурсів, розміри, вартість і енергоспоживання, оскільки використовуються різноманітні пристрої, наприклад, RFID-мітки, RFID-зчитувачі та інші сенсорні пристрої;

- ключовою можливістю є розгортання, оскільки кінцеві вузли Інтернету речей вимагають установки різних сенсорних пристроїв, що може відбуватися як поетапно, так і одночасно;

- інтернет речей переповнений різними пристроями, гібридними мережами, що робить таку систему повністю неоднорідною;

- використання бездротових сенсорних мереж, SCADA, бездротових ніздрюватих мереж та інших гібридних мереж.

Головною проблемою на сенсорному рівні є безпека. Річке зростання ПоТ, метою якого є підключення до промислових мереж для отримання інтелектуальних послуг, створює нові виклики в управлінні взаємодією пристроїв. Наприклад, визначення довіреної особи для аутентифікації та встановлення рівня довіри до додатків.

Прийняття рішень і визначення команд у відповідні моменти часу є важливим пріоритетом для моделі безпеки IoT. Всі пристрої на сенсорному рівні характеризуються обмеженими можливостями підключення та низьким енергоспоживанням. Величезна кількість IoT-додатків призводить до виникнення нових проблем безпеки.

Проблеми безпеки на цьому рівні можна поділити на дві основні категорії:

- для кінцевого вузла системи IoT важливими вимогами є аутентифікація, конфіденційність, цілісність, доступність, фізичний захист і управління доступом;

- для сенсорного рівня вимагаються аутентифікація джерела та пристроїв, забезпечення конфіденційності, автономності, доступності та цілісності.

В таблицях 2.4 та 2.5 зображені найбільш поширені потенційні загрози та вразливості безпеки для кінцевих вузлів IoT.

Таблиця 2.4 – Поширені вразливості на кінцевому вузлі IoT пристрою

Загрози безпеки	Характеристика
Несанкціонований доступ	Захоплюється зловмисником через фізичне захоплення або логічні атаки, конфіденційна інформація на кінцевих вузлах
Доступність	Кінцевий вузол перестає працювати, оскільки фізично захоплений або логічно атакований
Шкідливий код	Віруси і небажані повідомлення, які можуть викликати збій програмного забезпечення
Загрози передачі	Такі як переривання, блокування, маніпулювання даними, підробка і т.і.
Маршрутна атака	Атака на шлях маршрутизації
DoS атака	Спроба зробити ресурс кінцевого вузла Інтернету речей недоступним для користувача
Spoofing атака	За допомогою шкідливого ПО зловмисник успішно маскується під кінцевий пристрій IoT, кінцевий вузол або кінцевий шлюз шляхом фальсифікації даних
Selfish загроза	Деякі кінцеві вузли Інтернету речей перестають працювати, щоб заощадити ресурси або пропускну здатність, щоб викликати збій мережі

Таблиця 2.5 – Порівняльна таблиця загроз безпеки та вразливостей у IoT

Загрози та вразливості кінцевих вузлів IoT	Кінцеві пристрої IoT	Кінцевий вузол IoT	Кінцевий шлюз IoT
Несанкціонований доступ	+	+	+
Шкідливий код	+	+	+
Загрози передачі		+	+
Маршрутна атака	+	+	+
DoS	+	+	+
Spoofing атака		+	+
Selfish загроза		+	+

2.3.2 Мережевий рівень

Мережевий рівень є важливою частиною архітектури, оскільки забезпечує взаємодію всіх об'єктів IoT, дозволяючи їм розпізнавати своє оточення через мережу. Цей рівень відповідає за передачу агрегованих даних між сенсорним і службовим рівнями. Оскільки Інтернет речей складається з численних гібридних мереж, виникає низка складнощів, пов'язаних з мережевими проблемами, питаннями безпеки та зв'язку[10].

Для досягнення спільної мети необхідно враховувати, що мережевий рівень вимагає ефективного управління, планування та розгортання мереж. Для виконання всіх функцій цей рівень потребує вирішення таких проблем:

- технології для повного контролю та управління бездротовими, мобільними та фіксованими мережами;
- підвищення ефективності мережі;
- пошук рішення для вирішення проблем з вимогами до якості обслуговування QoS.

Особливу увагу необхідно приділити питанням конфіденційності та безпеки даних та користувачів. Рішення цих проблем має першочергове значення, оскільки сучасні технології в сфері безпеки забезпечують лише базовий рівень захисту для IoT, і існує багато невирішених завдань у цій сфері.

Основні вимоги безпеки на мережевому рівні включають:

- набір базових вимог до безпеки: конфіденційність даних, захист людини, цілісність, аутентифікація, доступність та захист ключів;
- витік конфіденційної інформації є важливим аспектом безпеки. Різні об'єкти IoT, розміщені в ненадійних або легкодоступних місцях, можуть стати вразливими для розкриття інформації в разі фізичного контакту злоумисника з об'єктом IoT. Наприклад, це стосується ідентифікації користувачів;
- цілісність і конфіденційність при передачі сигналів між різними мережами Інтернету речей створюють додаткові вимоги безпеки зв'язку;
- надмірність підключень може спричиняти проблеми безпеки, пов'язані з DoS-атаками (від перевантажень мережі) та проблеми безпеки ключів (від

високого споживання мережевих ресурсів). Такі проблеми виникають у разі втрати контролю над користувачами;

- атака типу Man-In-The-Middle є ще однією загрозою, коли зловмисник перехоплює і передає повідомлення між жертвою та зловмисником через незалежні з'єднання. Зловмисник змушує жертв вірити, що між ними існує приватне з'єднання, але насправді жертви перебувають під контролем зловмисника.

Також важливо запобігти створенню підроблених сигналів, які можуть призвести до неправильного використання пристроїв, що є важливим аспектом безпеки для запобігання підроблених мережевих повідомлень.

В таблиця 2.6 та 2.7 описані основні загрози безпеки та вразливості мережевого рівня.

Слід так само додати, що є проблеми, пов'язані з безпекою протоколів і мережевою інфраструктурою в системі IoT. Проблеми, які на даний момент не мають рішення, представлені нижче:

- уразливості пароля і контролю доступом, які надають доступ до аутентифікації і авторизації;
- створення зашифрованої передачі даних на мережевому рівні.

Таблиця 2.6 – Потенційна загроза на мережевому рівні

Загрози безпеки	Характеристика
Порушення даних	Передача захищеної інформації в ненадійну середу
Відкритий і закритий ключ	Складається з ключів в мережах
Шкідливий код	Віруси і небажані повідомлення, які можуть викликати збій ПЗ
DoS	Спроба зробити ресурс кінцевого вузла IoT недоступним для користувача
Загрози передачі	Такі як переривання, блокування, маніпулювання даними, підробка і т.і.
Маршрутна атака	Атаки на шляхах маршрутизації

Таблиця 2.7 – Потенційна загроза на мережевому рівні

	Витік конфіден- ційності	Конфіден- ційність	Ціліс- ність	DoS	PKI	MITM	CSRF
Фізичний захист	+	+					+
Безпека передачі		+	+	+	+	+	+
Переповнення підключень			+	+	+		
Міжрівневе з'єднання	+	+				+	+

2.3.3 Рівень інтерфейсів

Концепції розумного будинку, RFID-мітки, що реалізуються за допомогою стандартних протоколів Інтернету речей та службово-складових технологій, розглядаються на рівні інтерфейсів. Цей рівень має залежність виключно від програмного забезпечення, тому для забезпечення безпеки повинні бути виконані наступні вимоги:

- завантаження і оновлення програмного забезпечення, включаючи патчі, необхідні для підтримки безпеки та аутентифікація адміністратора;
- забезпечення цілісності, конфіденційності, аутентифікації та авторизації.

При розробці системи на рівні інтерфейсів необхідно дотримуватися таких вимог безпеки:

- впроваджувати безпеку в системи IoT, де кінцеві вузли працюють без нагляду;
- увагу надавати збірці енергоефективних методів для забезпечення безпеки при виборі рішень;
- приділяти належну увагу прийняттю рішень для різних частин системи, враховуючи, що схема захисту на різних кінцевих вузлах може бути різною.

У таблицях 2.8 і 2.9 узагальнено основні загрози безпеки та вразливості на рівні інтерфейсів.

Отже, інтерфейсний рівень виконує роль посередника між IoT-системою та різними додатками. Він забезпечує легітимність взаємодії між додатками та системою, гарантуючи безпечний і коректний обмін даними.

Таблиця 2.8 - Потенційна загроза на рівні інтерфейсів

Загрози безпеки	Характеристика
Віддалена конфігурація	Не вдалося провести налаштування на інтерфейсах
Неправильна конфігурація	Неправильна конфігурація на віддаленому кінцевому вузлі IoT, кінцевому пристрої або кінцевому шлюзі
Управління безпекою	Витік логів та ключів
Система управління	Збій системи управління

Таблиця 2.9 - Потенційна загроза на рівні інтерфейсів

	Несанкціонований доступ	Помилка вузла	Masquerade атака	Selfish загроза	Вірус, Троян, спам	Витік конфіденційності
Фізичний захист безпеки	+		+			
Управління доступом	+	+	+			+
Конфіденційний рівень		+	+			+
Цілісність даних		+	+	+	+	
Антивірус				+		
Не відмова	+	+	+			+
Аутентифікація	+	+	+			+

2.3.4 Особливості рівня служб

Технологія міжрівневого програмного забезпечення є одним із ключових інструментів, що забезпечують підтримку програм та сервісів. Службовий рівень

створює ефективну та економічно вигідну платформу, яка дозволяє повторно використовувати апаратні та програмні ресурси. Інтернет речей залежить від середнього рівня технічних характеристик та функціонує завдяки стандартам, розробленим постачальниками послуг та організаціями.

Під час створення службового рівня були враховані загальні вимоги до API, додатків та службових протоколів. Основні його компоненти, такі як сервіси інтеграції та аналітики, обробки подій та безпеки, забезпечують обмін даними між службами та їхню обробку відповідно до функцій цього рівня.

Основні служби, що виконуються на цьому рівні:

- служба виявлення – дозволяє знаходити необхідну інформацію та послуги через пошук ефективної інфраструктури;
- служба складання – забезпечує повноцінну взаємодію між підключеними об'єктами, створюючи сервіси з вищим рівнем надійності відповідно до встановлених вимог;
- механізм обробки команд пристроїв – забезпечує розуміння доручень, що надходять від різних служб, а також контроль за довіреною інформацією;
- система управління надійністю – реалізує контроль стабільності сервісів;
- службові API – забезпечують виконання вимог користувача для інтеграції між сервісами.

На сьогодні ведуться активні дослідження щодо вдосконалення службового рівня:

- для покращення ефективності взаємодії між додатками та сервісами застосовується архітектура SOCRADES;
- об'єкти IoT представлені на нижчому рівні, включаючи служби виявлення мережі та обміну даними;
- сервіси, які забезпечують взаємодію між додатками та іншими компонентами, також реалізовані на рівні служб.

Для розробки ефективної стратегії безпеки необхідно враховувати такі аспекти:

- реалізація авторизації та аутентифікації сервісів;

- захист цілісності, конфіденційності даних та ключів, а також забезпечення стійкості до збоїв;
- усунення ризику витоку конфіденційної інформації;
- запобігання зловживанню службами, наприклад, використанню непідписаних сервісів;
- захист кінцевих вузлів IoT від атак типу masquerade;
- протидія DoS-атакам;
- механізми захисту від повторних атак;
- контроль аналізу трафіку та маніпулювання інформацією.

Для забезпечення належного рівня захисту службовий рівень повинен ефективно протидіяти загрозам. В нижченаведеній таблиці 2.10 представлено узагальнений перелік таких загроз.

Захист даних на цьому рівні має вирішальне значення. Сьогодні існує багато стандартів, протоколів і пропрієтарних рішень, що конкурують між собою. Архітектура SOA забезпечує підвищений рівень безпеки, однак залишаються проблеми, пов'язані з передачею даних між рівнями та службами. Крім того, безпека, контроль доступу та управління службами також потребують подальшого вдосконалення.

2.3.5 Міжрівневі загрози

Архітектура SOA дозволяє забезпечити обмін інформацією на всіх чотирьох рівнях, що значно покращує сумісність між різними сервісами та пристроями. Така гнучкість і можливість інтеграції створює додаткові виклики, пов'язані з безпекою: зокрема, виникають ризики для конфіденційності даних користувачів, складнощі із забезпеченням безпечного міжрівневого обміну інформацією та питання довіри до джерела даних [11].

Через особливості архітектури IoT передача інформації між різними рівнями може стати джерелом потенційних загроз безпеки. Основні з них описані у таблицях 2.10 та 2.11.

Таблиця 2.10 - Потенційна загроза на рівні служб

Загрози безпеки	Характеристика
Загрози конфіденційності	Витік конфіденційності або зловмисне відстеження місцезнаходження
Маскування особистості	Кінцевий пристрій IoT, вузол або шлюз маскуються зловмисником
Зловживання службами	Послуги несанкціонованого доступу користувачів або уповноважені користувачі отримують доступ до послуг, на які не має підписки
Маніпулювання службовою інформацією	Зловмисник маніпулює інформацією в службах
Маршрутна атака	Атака на шлях маршрутизації
Повтор атаки	Атака повторно надсилає інформацію для підробки одержувача
DoS	Спроба зробити ресурс кінцевого вузла IoT недоступним для своїх користувачів
Відмова	Відмова від операції

Таблиця 2.11 - Потенційна загроза між рівнями у IoT

Загрози безпеки	Характеристика
Витік конфіденційної інформації	Конфіденційна інформація може бути не захищена на межі різних рівнів
Конфіденційна інформація поширюється між рівнями	Конфіденційна інформація поширюється на різних шарах і спричиняє витік інформації
Підміна особистості	Особистість на різних рівнях має різні пріоритети

Методи забезпечення безпеки в Інтернеті речей відрізняються залежно від рівня, на якому вони застосовуються, та мають специфічні вимоги. Умовно їх можна поділити на три основні рівні.

Сенсорний рівень є першим типом, який охоплює фізичні пристрої, зокрема сенсори та датчики. Вони переважно використовують бездротові сенсорні мережі, Bluetooth, RFID та інші технології зв'язку.

Згідно з вимогами безпеки IoT, основними критеріями на цьому рівні є конфіденційність, захист даних, доступність, достовірність і цілісність інформації.

У таблиці 2.12 представлено порівняльний аналіз можливих методів забезпечення безпеки на сенсорному рівні, а також їхні переваги та недоліки.

Таблиця 2.12 - Засоби безпеки інформації на рівні сенсорів

Методи	Використання	Переваги	Недоліки
Управління ключами	Використовується для забезпечення генерації ключів і поновлення алгоритмів безпеки з використанням розподілу ключів (PK1 ті ін..)	Легкий механізм захисту	Займає багато часу при конфігуруванні
Протокол безпечної маршрутизації	Алгоритми безпечної маршрутизації: об'єднання даних, маршрутизація з декількома переходами і ключові механізми	До тих пір, поки вторгнення не виявлено, безпечна передача даних не потрібна	Більшість таких алгоритмів потребує багато енергії та часу
Захищені алгоритми ключів (SKA)	Для IoT використовуються симетричні та асиметричні алгоритми ключів (RC5, AES та ін..)	Менше споживання енергії, вартості та часу роботи вузлів завдяки симетричним алгоритмам ключів	Асиметричні алгоритми ключів споживають більше енергії і часу
IDE/IPS	Використовують ви для виявлення і запобігання більшості підозрілих користувачів і атак	Використовують ся для виявлення і запобігання більшості підозрілих користувачів і атак	Вимагає визначення політики безпеки, загрози та атаки обробляються відповідно до керівних принципів корпоративної політики безпеки

Продовження таблиці 2.12

Методи	Використання	Переваги	Недоліки
IPSec	Метод надає два рівня безпеки: аутентифікація (для визначених користувачів) і механізм шифрування (для даних RFID)	Підвищує рівень безпеки для RFID даних та сигналів	Споживає потужність і час

Мережевий рівень, який включає мобільні мережі та інтернет-з'єднання, також має власні методи захисту. Основні підходи до безпеки на цьому рівні описані у таблиці 2.13.

Таблиця 2.13 - Засоби безпеки інформації на мережевому рівні

Методи	Використання	Переваги	Недоліки
Наскрізна автентифікація та управління ключами	Пристрої IoT мають бути автентифіковані за допомогою механізму автентифікації, PKI та наскрізного шифрування	Забезпечує наскрізну автентифікацію та шифрування	Важкий механізм безпеки
Криптографічна система	Для перевірки передачі даних через інші вузли та виявлення будь-якої помилки в мережі	Може виявляти помилку мережі та перевіряти дані; споживає мало енергії та часу	Асиметрична криптографія витрачає ресурси і час
Секретність даних, цілісність	Для виявлення та контролю будь-якої помилки в мережі; цілісність даних використовує алгоритми шифрування перевірки вихідних даних, які надсилаються	Використовується для перевірки вихідних даних	Витрачає багато часу

2.4 Висновки до розділу

У другому розділі було детально розглянуто такі ключові аспекти:

- актуальні проблеми інформаційної безпеки;
- моніторинг загроз безпеки даних та пристроїв Інтернету речей;
- аналіз загроз безпеки на кожному рівні архітектури IoT.

Під час дослідження питань інформаційної безпеки було визначено спектр загроз для IoT, сформульовано вимоги до безпеки та здійснено аналіз потенційних ризиків на різних рівнях архітектури.

Друга частина розділу присвячена оцінці актуальних загроз, вивченню існуючих атак, їхнього механізму дії та формуванню рекомендацій щодо підвищення рівня безпеки з урахуванням сучасних тенденцій атак.

Завершальна частина розділу має дослідницький характер. Вона містить аналіз загроз і вразливостей на кожному рівні IoT, а також розгляд можливих шляхів покращення безпеки на різних рівнях архітектури.

3 РОЗРОБКА ІОТ СИСТЕМИ

3.1 Діаграми варіантів використання

При розробці мережі Інтернету речей необхідно враховувати дві основні складові:

- фізичне проектування мережі;
- логічне проектування мережі.

Фізичне проектування охоплює вибір та розміщення IoT-пристроїв, а також використання відповідних протоколів зв'язку [13].

Для ефективної взаємодії між IoT-пристроями та сервером існує широкий спектр протоколів, які забезпечують керування пристроями та отримання від них

команд через Інтернет (рис. 3.1, таблиці 3.1-3.5).

Логічне проектування мережі Інтернету речей відображає абстрактне розуміння сутностей і процесів, що відбуваються в системі [14].

Основні складові логічного проектування:

- функціональні блоки IoT;
- модель зв'язку IoT;
- API зв'язку IoT.

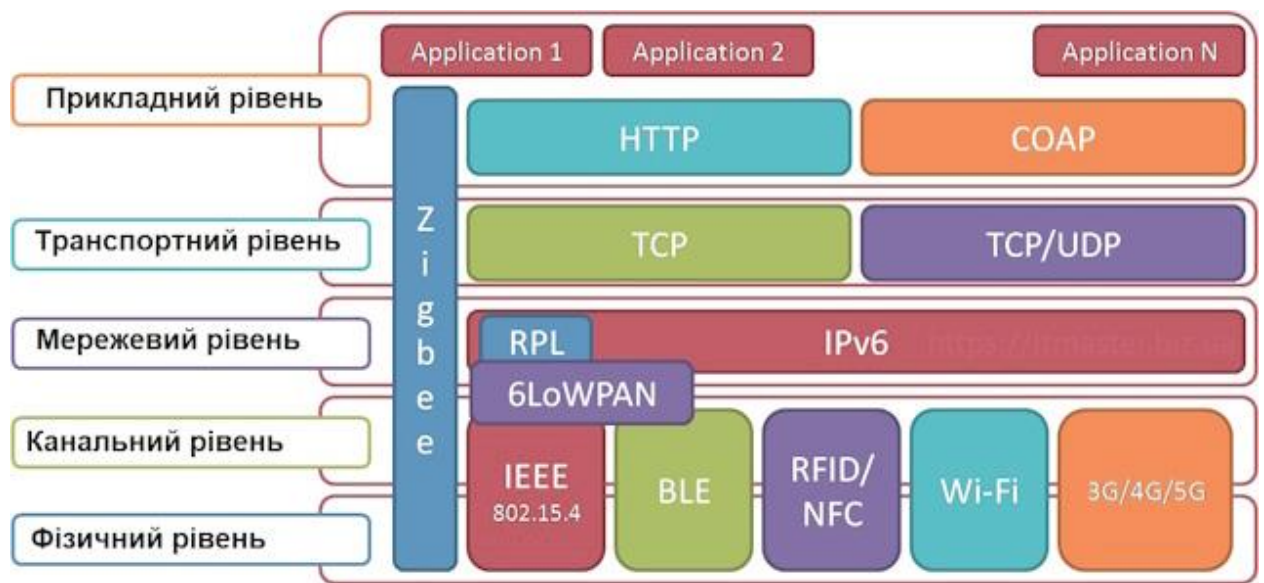


Рисунок 3.1 - Протоколи IoT

Таблиця 3.1 - Протоколи каналного рівня

Назва	Характеристика
Ethernet	Сукупність технологій та протоколів, які використовуються переважно в локальних мережах
Wi-max	Стандарт для бездротових мереж метрополітену (WMAN), спеціалізується на бездротовому широкосмуговому доступі від точки до багатоточок
2G/3G/4G	Різні типи телекомунікаційних поколінь, на основі цих стандартів IoT пристрої можуть обмінюватися даними через стільникові мережі
WiFi	Частина набору протоколів локальної мережі IEEE 802, визначає набір протоколів управління фізичного рівня (PHY) для реалізації локальної мережі (WLAN) WiFi комп'ютерного зв'язку на різних частотах

Продовження таблиця 3.1

Назва	Характеристика
LR-WPAN	Стандарти для низько швидкісної бездротової персональної мережі: - стандарт IEEE 802.15.4 визначає рівень MAC і PHY, який використовується, але не обмежується специфікаціями, такими як протоколи Zigbee, 6LoWPAN, Thread, WiSUN та MiWi; - недорогий та низько швидкісний зв'язок для пристроїв з обмеженою потужністю.

Таблиця 3.2 - Опис протоколів мережевого рівня

Назва	Характеристика
IPv4	Інтернет протокол версії 4, визначає IP- адресу. Виконує функції: - ідентифікація хоста або мережевого інтерфейсу; - адресація місцезнаходження.
IPv6	Інтернет протокол версії 6, забезпечує системи ідентифікації та розташування комп'ютерів у мережах та маршрутизує трафік через Інтернет
6LoWPAN	Назва робочої групи, поєднує останню версію Інтернет-протоколу (IPv6) та малопотужні бездротові персональні мережі (LoWPAN)

Таблиця 3.3 - Опис протоколів транспортного рівня

Назва	Характеристика
TCP	Стандарт, який визначає, як встановлювати та підтримувати мережеву розмову за допомогою якої прикладні програми можуть обмінюватися даними
UDP	Протокол транспортного рівня, не надійний і безпроводний протокол

Таблиця 3.4 - Опис протоколів прикладного рівня

Назва	Характеристика
HTTP	Протокол передачі гіпертексту – для передачі гіпермедійних документів, таких як HTML
CoAP	Протокол обмежених додатків – спеціалізований протокол для обмежених пристроїв, дозволяє здійснювати зв'язок через Інтернет
WebSocket	Протокол забезпечує двосторонній зв'язок між клієнтом, що запускає ненадійний код у контрольованому середовищі, із віддаленим хостом, який увійшов у зв'язок із цим кодом
MQTT	Протокол підключення «машина до машини» (M2M)/ «Інтернет речей»
XMPP	Розширюваний протокол обміну повідомленнями та присутності – комунікаційний протокол для орієнтованого на повідомлення проміжного програмного забезпечення на основі XML
DDS	Протокол проміжного програмного забезпечення та стандарт API для підключення, орієнтованого на дані від Object Management Group
AMQP	Протокол IoT складається з жорстких компонентів, які маршрутизують і зберігають повідомлення в операторі брокера з набором політик для з'єднання компонентів разом

3.1.1 Функціональні блоки IoT

Функціональна архітектура IoT включає такі основні компоненти [15]:

- блок пристроїв – відповідає за зондування, моніторинг та керування пристроями;
- блок зв'язку – забезпечує передачу даних та організацію зв'язку між компонентами IoT-системи;
- блок управління – реалізує механізми керування інфраструктурою Інтернету речей;
- блок безпеки – відповідає за захист інформації та безпечний доступ до системи;
- блок додатків – контролює функціонування різних сервісів та взаємодію з користувачами.

3.1.2 Моделі зв'язку IoT

Для обміну даними між пристроями та серверами використовуються такі моделі зв'язку:

- запит-відповідь – традиційна клієнт-серверна модель взаємодії;
- Push-Pull – механізм, у якому сервер надсилає дані клієнтам або клієнти отримують дані при запиті;
- парна модель – передбачає безпосередній зв'язок між пристроями без участі центрального сервера.

3.1.3 API зв'язку IoT

Основними інтерфейсами для взаємодії пристроїв є:

- API на основі REST – використовується для запитів через HTTP-протокол;
- API на основі WebSocket – забезпечує двосторонній зв'язок у режимі реального часу.

3.2 Побудова системи

Описана IoT система складається з таких пристроїв:

- розумний дверний замок – 3 шт.;
- датчик відкриття вікна – 3 шт.;
- розумна лампа – 2 шт.;
- датчик включення світла – 3 шт.;
- базова станція, шлюз – 1 шт.

Використані протоколи:

- каналний рівень – усі сенсори працюють через Wi-Fi;
- мережевий рівень – використовується протокол IPv4;
- транспортний рівень – підтримуються TCP та UDP;

- рівень додатків – для передачі даних застосовуються MQTT та WebSocket.

Топологія IoT системи.

На рисунку 3.6 представлена топологія, створена у Packet Tracer.

Основні особливості:

- шлюз забезпечує з'єднання між усіма сенсорами, маршрутизацію даних і їхню передачу;
- IoT система ізольована та працює в підмережі 192.168.25.0/24;
- взаємодія пристроїв організована за моделлю запит-відповідь;
- для комунікації застосовуються API на основі REST та WebSocket.

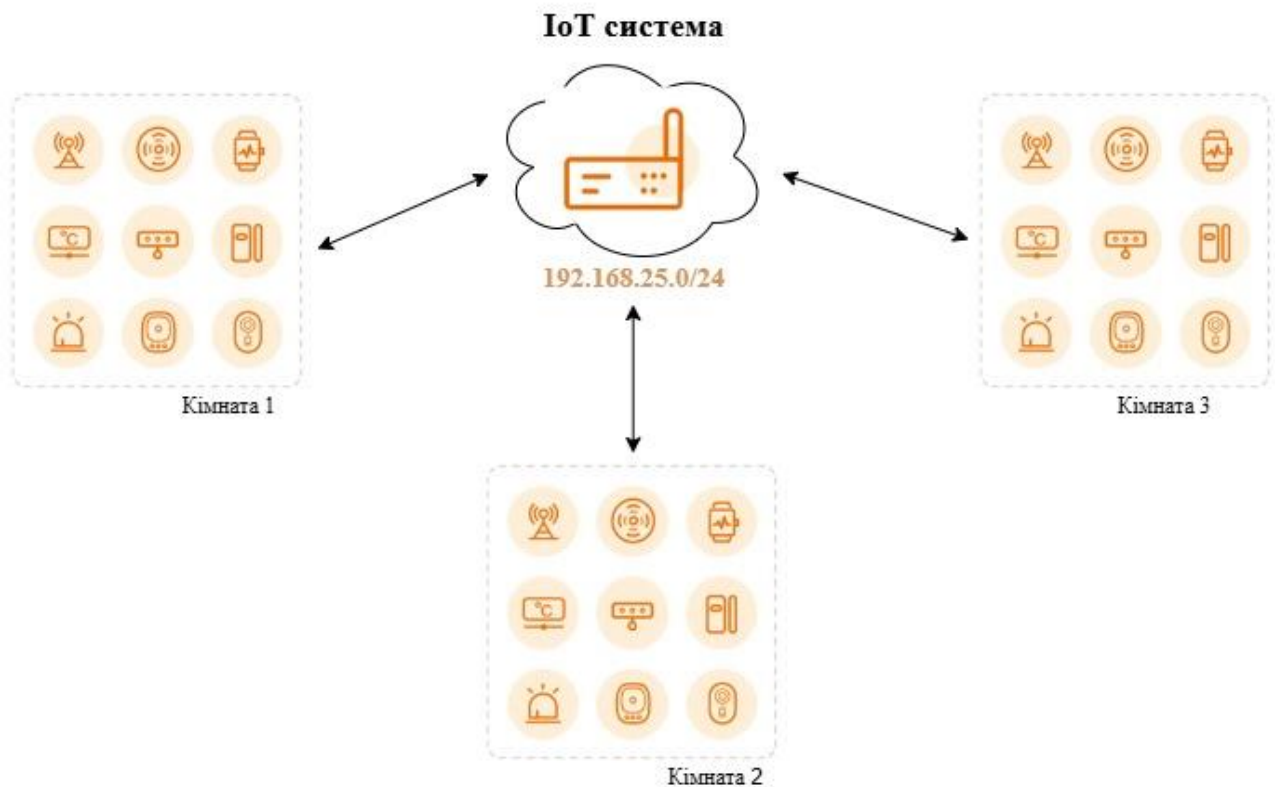


Рисунок 3.2 - Топологія проекту

3.3 Реалізація методів безпеки

Для підвищення безпеки IoT-системи додаємо TLS/SSL аутентифікацію поверх MQTT.

Метод аутентифікації. На рівні додатків, де використовується MQTT, додається SSL/TLS захист, реалізований через IBM Watson IoT Platform.

IBM Watson IoT Platform. Ця IoT-платформа (рис.3.3) забезпечує зв'язок між сенсорами та хмарою. Вона працює між сенсорним рівнем і рівнем додатків.

Основні особливості:

- аутентифікація здійснюється через TLS/SSL;
- ініціатором підключення до хмари стає смартфон, а не датчик;
- підключення: після створення пристрою завантажуюмо додаток на смартфон і проходимо аутентифікацію для доступу до IoT-платформи.

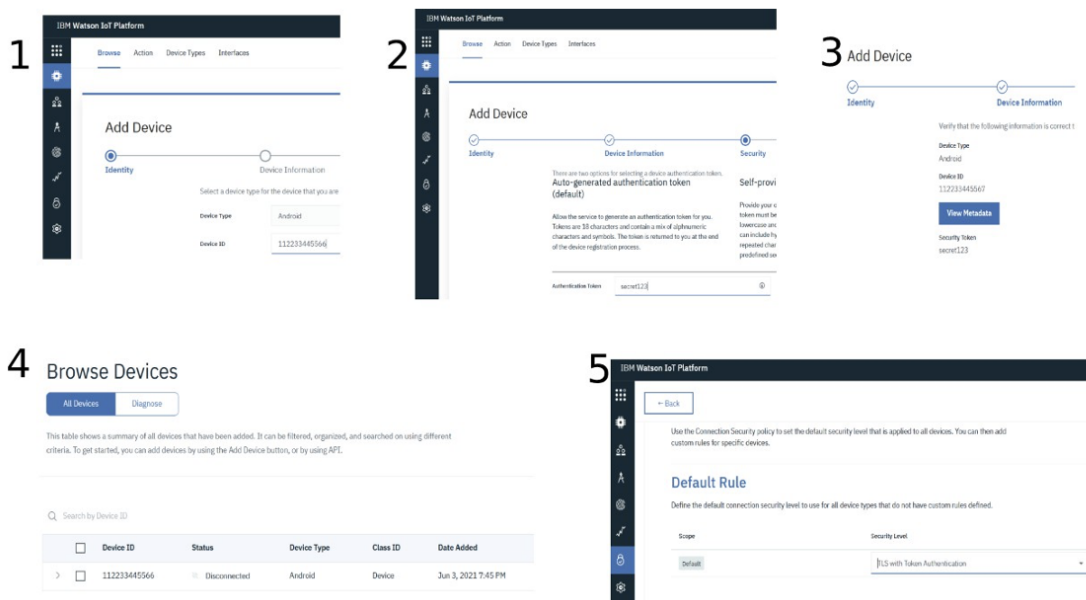


Рисунок 3.3 - Створення пристрою в IoT-платформі

Запровадження контролю доступу для пристроїв відображено на наведено нижче рисунку 3.4.

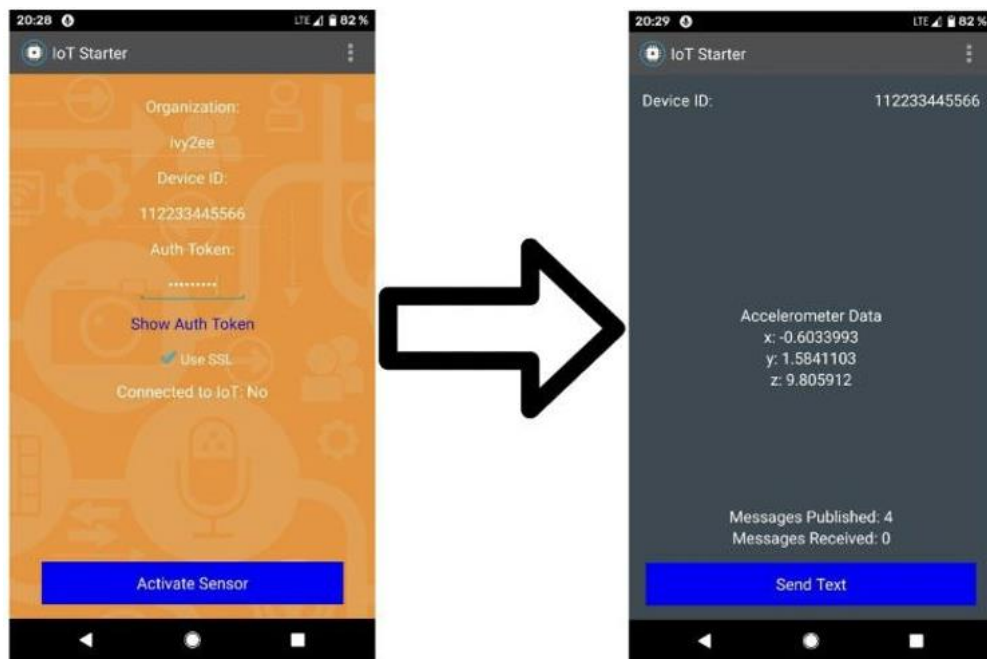


Рисунок 3.4 - Аутентифікація пристроя

Створюємо нову роль і надаємо їй відповідні права, змінюючи права доступу для шлюзу та користувача (рис.3.5).

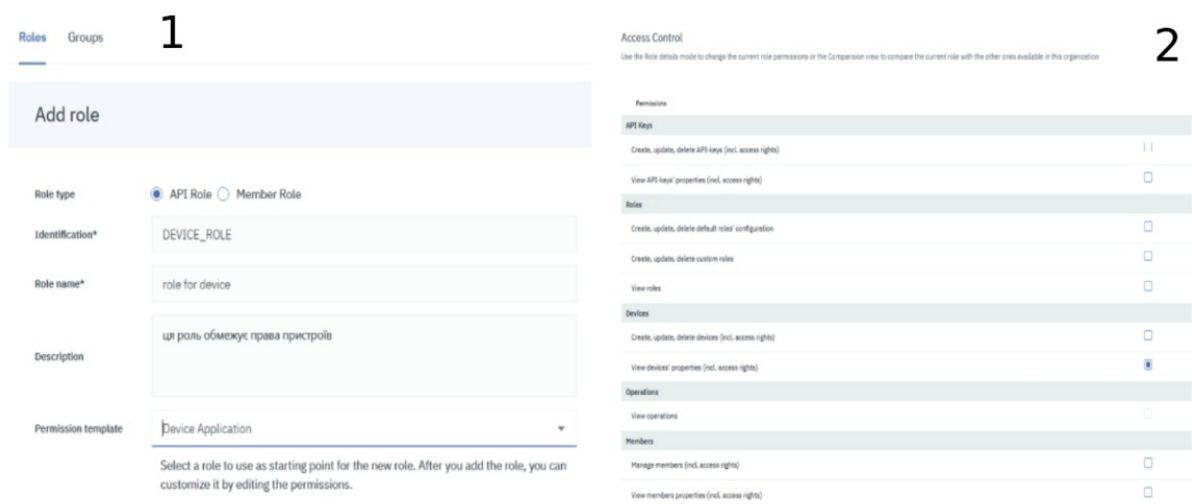


Рисунок 3.5 - Створення контролю доступу для пристроїв

Впровадження апаратного методу безпеки. Для підвищення рівня безпеки при обміні даними між пристроями Інтернету речей було інтегровано модуль для створення ключів шифрування, характеристика якого наведена у таблиці 3.5.

Таблиця 3.5 – Порівняльний аналіз використання TPM у системі

Критерій	IoT-система з TPM	IoT-система без TPM
Захист ключів шифрування	Ключі зберігаються всередині апаратного модуля і не покидають його фізично	Ключі зберігаються у файловій системі або оперативній пам'яті – легко вразливі
Автентифікація пристрою	Надійна апаратна автентифікація з унікальним TPM-ідентифікатором	ПЗ-ідентифікація, легко підробити або зламати
Захист від підміни прошивки	Підтримка secure boot і перевірки цілісності коду з використанням TPM	Відсутність апаратного захисту цілісності прошивки
Захист даних на диску / в пам'яті	Шифрування з апаратним зберіганням ключів TPM	Шифрування можливе, але ключі можуть бути викрадені або витягнуті
Стійкість до фізичного злому	Висока	Низька
Вартість впровадження	Дорожча	Дешевша
Складність реалізації	Складніша	Простіша
Відповідність стандартам безпеки	Висока	Не відповідає вимогам стандартів безпеки
Використання в критичних системах	Підходить	Не підходить для критичних або сертифікованих рішень

Оптимальним рішенням є використання TPM модуля, оскільки він має ряд важливих функцій (рис. 3.6):

- забезпечує цілісність пристрою;
- може працювати в безпечному режимі, знижуючи потенційний збиток від шкідливого ПЗ;
- встановлює корінь довіри.



Рисунок 3.6 - TPM модуль

У роботі було виділено основні рівні безпеки для систем Інтернету речей.

Забезпечення зв'язку. Дослідження показують, що більшість IoT-систем не використовують шифрування трафіку. Тому важливо впровадити:

- шифрування переданих даних;
- перевірку автентичності пристроїв.

Реалізація в IoT-системі:

- використано метод еліптичної криптографії для шифрування трафіку, що забезпечує високу швидкість роботи навіть на слабких пристроях;
- впроваджено сертифікати безпеки X.509 для унікальної ідентифікації пристроїв та контролю доступу до мережі.

Безпека пристроїв на рівні коду. Щоб уникнути використання IoT-пристроїв у ботнет-атаках, необхідно обмежити їх виконання лише визначеними функціями.

Реалізація в IoT-системі:

- використано бібліотеку OpenSSL для перевірки автентичності та підтвердження виконуваного коду пристроїв.

Безпека під час використання пристроїв. Кінцеві вузли IoT часто стають мішенню шкідливого ПЗ через вразливості пристроїв.

Реалізація в IoT-системі:

- впроваджено систему розмежування доступу, що обмежує взаємодію між мережевими підключеннями та додатками, підвищуючи захист від експлойтів.

Безпека управління пристроями. Незалежно від рівня захисту IoT-мережі, завжди існує ймовірність появи загроз.

Реалізація в IoT-системі:

- інтегровано систему аналітики безпеки UBA, яка виявляє аномальну поведінку користувачів, аналізуючи зібрані дані.

Додаткові заходи безпеки:

- регулярне оновлення IoT-пристроїв та перевірка прошивки перед завантаженням;

- використання антивірусного ПЗ (Symantec) для захисту від шкідливих програм;

- проведення щомісячних аудитів інфраструктури IoT за допомогою AWS IoT Device Defender;

- впровадження брандмауера для контролю вхідного та вихідного трафіку;

- створення надійних унікальних паролів та їх регулярна зміна;

- організація ізольованої IoT-мережі (192.168.25.0/24) для ускладнення несанкціонованого доступу.

На рис. 3.7 представлено зображення впроваджених заходів безпеки для IoT-системи.

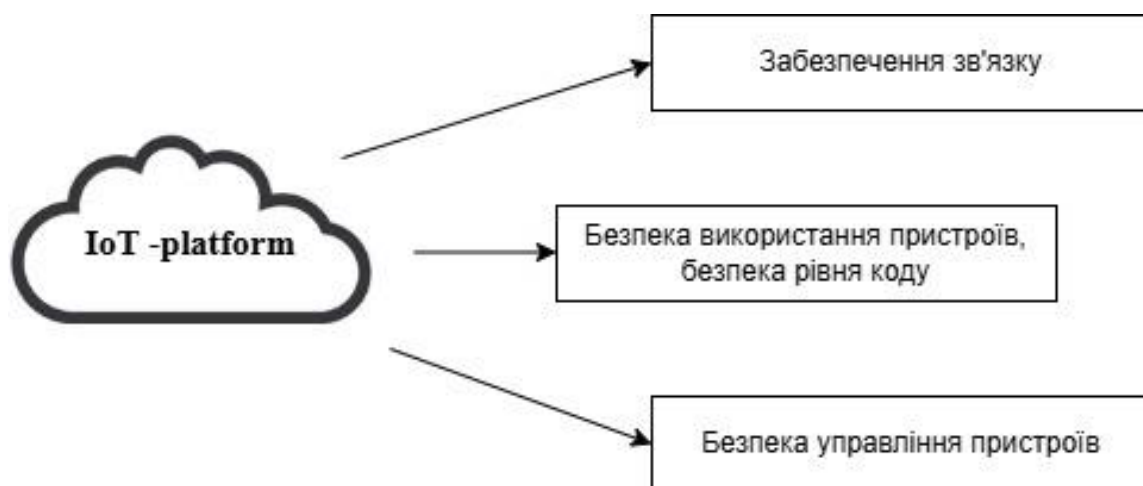


Рисунок 3.7 - Система методів безпеки для спроектованої системи IoT

3.4 Висновки до розділу

Кожна IoT-система потребує індивідуального підходу до забезпечення безпеки, оскільки на сьогодні не існує універсальних стандартів та вимог. Інформаційну безпеку необхідно розглядати комплексно, адже інакше зловмисники зможуть скористатися слабкими місцями системи.

Основні аспекти розділу:

- проектування та створення IoT-системи;
- запропонування методів захисту в інтернеті речей.

У межах розробки безпечної IoT-мережі була сформована концепція інформаційної безпеки, що охоплює:

- захист зв'язку;
- безпеку пристроїв на рівні коду;
- захист під час використання пристроїв;
- управління безпекою IoT-пристроїв.

Крім того, розглянуто наявні рішення та додаткові заходи для підвищення рівня безпеки.

Виконані завдання:

- визначено ключові компоненти IoT;
- проведено аналіз загроз та вразливостей на кожному рівні системи;
- виконано порівняльний аналіз методів безпеки;
- розроблено IoT-систему та визначено методи її захисту;
- надано рекомендації щодо впровадження заходів безпеки в IoT.

ВИСНОВКИ

Дипломна робота присвячена методам захисту даних та пристроїв в Інтернеті речей для створеної IoT-системи. В ході роботи отримано такі результати:

- визначено ключові компоненти Інтернету речей, включаючи розгляд еталонної та SOA-архітектури;
- досліджено проблеми інформаційної безпеки: проаналізовано спектр загроз, визначено вимоги до безпеки IoT та розглянуто питання захисту на кожному рівні архітектури;
- проведено порівняльний аналіз існуючих методів безпеки IoT;
- спроектовано систему Інтернету речей та розроблено відповідні заходи безпеки;
- надано рекомендації щодо впровадження методів захисту в IoT-системах.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Internet of Things for Industry and Human Application. Fundamentals of Internet of Things /V.S. Kharchenko (ed.). – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 95 p.
2. Management information systems for the information age Stephen Haag, Maeve Cummings, Amy Phillips, McGraw-Hill/Irwin, Boston, 2020 – 672 p.
3. Послідовність обробки даних в хмарних сервісах IoT. URL: <https://pupenasan.github.io/TI40/%D0%9B%D0%B5%D0%BA%D1%86/cloudiot.html> (дата звернення 17.04.2025).
4. Сервіс-орієнтована архітектура IoT для SOA URL: <https://habr.com/companies/vk/articles/342526/> (дата звернення 07.04.2025).
5. Сторчак К.П., Тушич А.М., Срібна І.М., Яковенко Н.Д., Кравець Д.В. Технології Інтернет речей. Навч. посібник підготовлено для студентів вищих навчальних закладів– Київ: ДУТ, 2021.– 68 с.
6. Основи Інтернету Речей. URL: <http://edu.asu.in.ua/mod/book/tool/print/index.php?id=112> (дата звернення 25.03.2025).
7. Get facts and insights on topics that matter. URL: <https://statista.com> (Last of access: 23.04.2025).
8. Жураковський Б. Ю., Зенів І.О. Технології інтернету речей. Навчальний посібник.– Київ: КПІ ім. Ігоря Сікорського, 2021.– 271 с.
9. Загрози у світі речей інтернету (Безпека інтернетуей) URL: <https://hackyourmom.com/osvita/chastyna-1-zagrozy-u-sviti-rechej-internetu-bezpeka-internetu-rechej/> (дата звернення 28.04.2025).
10. Безпека IoT URL: https://iot-ssl.com.ua/iot_secure.html (дата звернення 05.04.2025).
11. Parker J. Principles of scientific research. 7th ed. London : Editorial, 2017. 301 p.

12. Все про сервісно-орієнтовану архітектуру. Принципи роботи, переваги та мікросервіси URL: <https://robotdreams.cc/uk/blog/520-vse-pro-servisno-oriyentovanu-arhitekturu> (дата звернення 18.04.2025).

13. 6LoWPAN протокол URL: <https://itmaster.biz.ua/directory/standarts/6lowpan.html> (дата звернення 25.04.2025).

14. Мережева модель OSI. URL: <https://kr-labs.com.ua/blog/model-osi> (дата звернення 30.04.2025).

15. Що таке шлюз IoT: визначення, приклади, функції URL: <https://www.dusuniot.com/uk/blog/what-is-an-iot-gateway/> (дата звернення 17.05.2025).

СЛАЙДИ ПРЕЗЕНТАЦІЙ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Дипломний проєкт бакалавра

на тему: «РОЗРОБКА ІОТ-СИСТЕМИ З ПІДВИЩЕНИМ РІВНЕМ ЗАХИСТУ З
ВИКОРИСТАННЯМ ТРМ МОДУЛЯ»

Ст. групи КНТ – 511
Керівник

КОДАК І.В.
СКРУПСЬКИЙ С.Ю.

Метою даної дипломної роботи є розробка системи для забезпечення захисту даних і пристроїв у середовищі Інтернету речей.

Для досягнення мети, поставлені такі задачі:

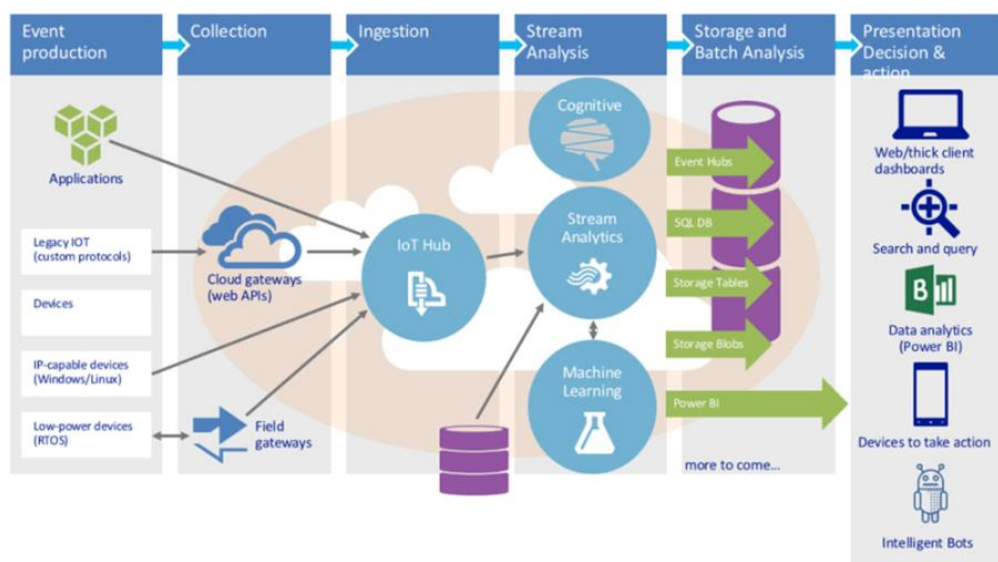
- визначити ключові компоненти Інтернету речей;
- розглянути еталонну архітектуру IoT;
- розглянути сервісно-орієнтовану архітектуру;
- провести порівняльний аналіз існуючих методів забезпечення безпеки в IoT-системах;
- спроектувати систему Інтернету речей із запропонованими методами забезпечення її безпеки.

Складові IoT

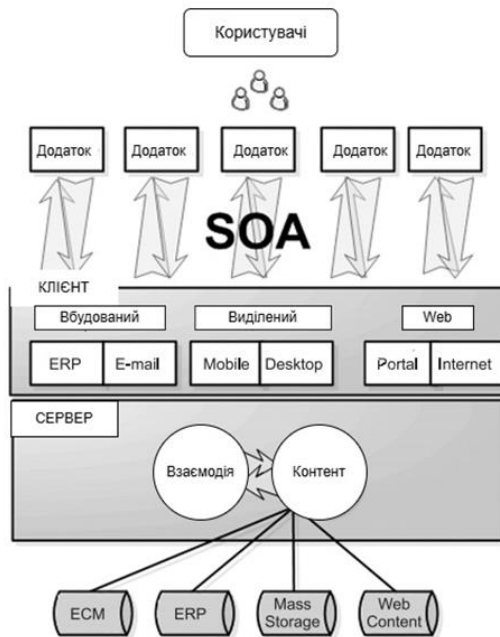
IoT = Сенсори (датчики) + Дані + Мережі + Послуги.



Базова архітектура IoT

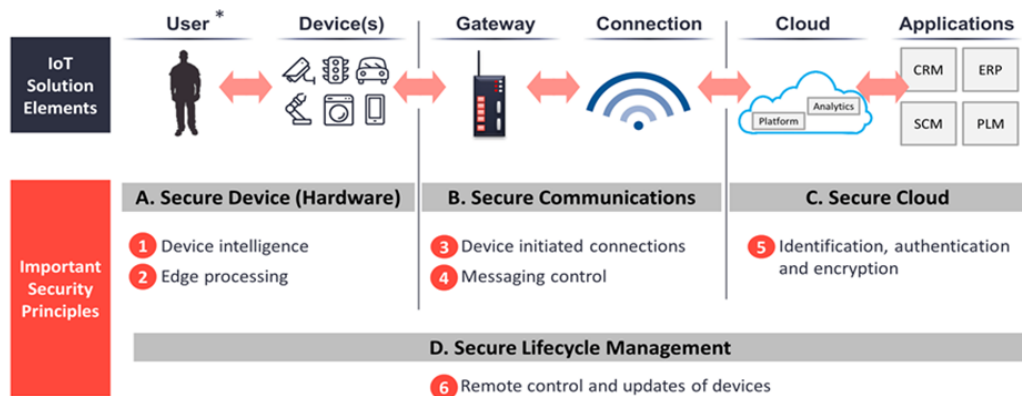


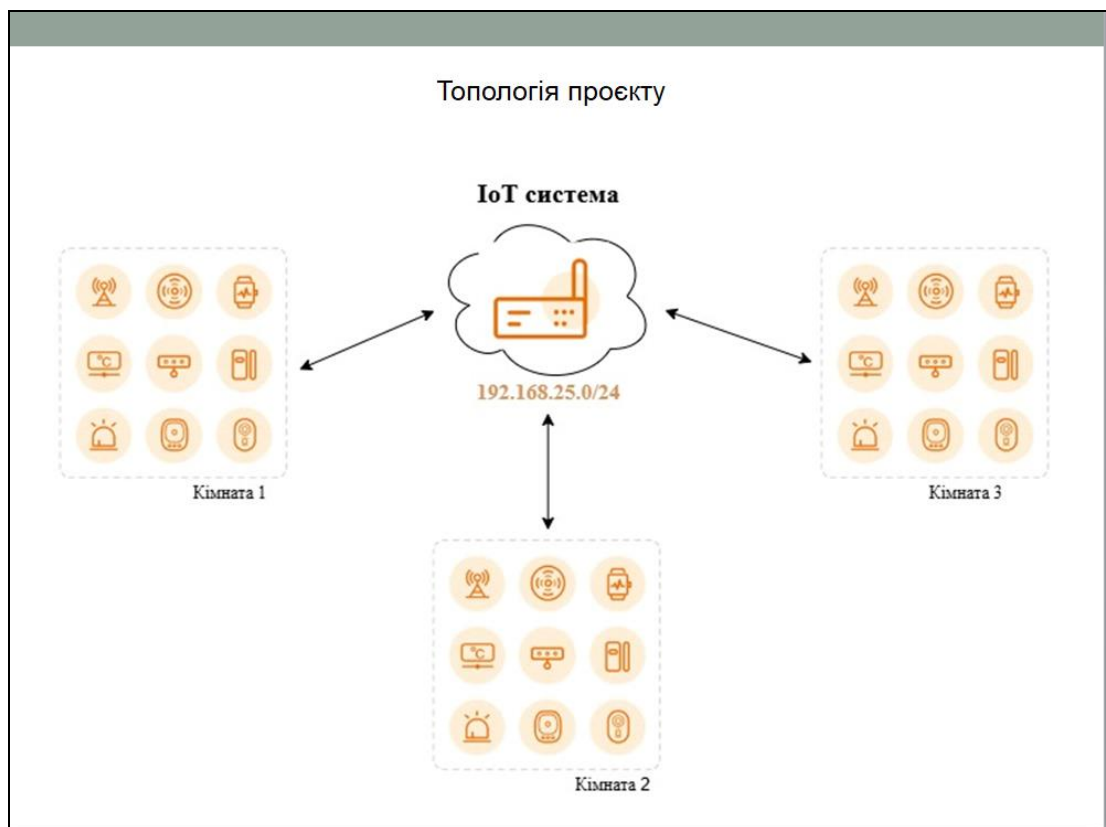
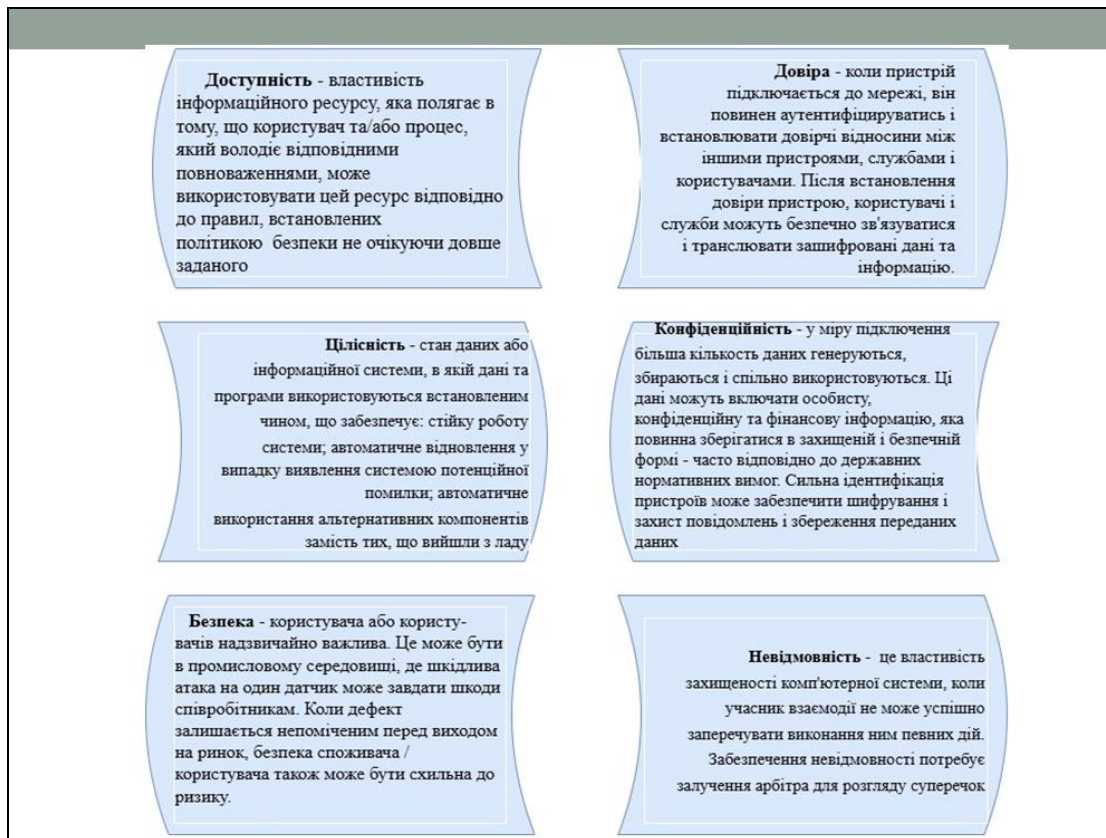
Сервіс-орієнтована архітектура IoT



Типові проблеми безпеки IoT

Six principles of IoT Cyber Security across the stack





Створення пристрою в IoT-платформі

1

2

3 Add Device

4 Browse Devices

All Devices Diagnose

This table shows a summary of all devices that have been added. It can be filtered, organized, and searched on using different criteria. To get started, you can add devices by using the Add Device button, or by using APT.

Search by Device ID

Device ID	Status	Device Type	Class ID	Date Added
112233445566	Disconnected	Android	Device	Jun 3, 2021 7:45 PM

5



TPM модуль



Система методів безпеки для спроектованої системи IoT

Висновки:

- визначено ключові компоненти Інтернету речей, включаючи розгляд еталонної та SOA-архітектури;
- досліджено проблеми інформаційної безпеки: проаналізовано спектр загроз, визначено вимоги до безпеки IoT та розглянуто питання захисту на кожному рівні архітектури;
- проведено порівняльний аналіз існуючих методів безпеки IoT;
- спроектовано систему Інтернету речей та розроблено відповідні заходи безпеки;
- надано рекомендації щодо впровадження методів захисту в IoT-системах.