ДОДАТОК А

Графічний матеріал атестаційної роботи

Харківський національній університет радіоелектроніки
Кафедра ЕОМ

Методи захисту інформації в IoT

Атестаційна робота
Другий (магістерський) рівень

Автор:
Польська Б.Ю.
Студентка гр. КСМзм-19-1

Керівник:
Голубничий Д.Ю.
доц. каф. ЕОМ

1

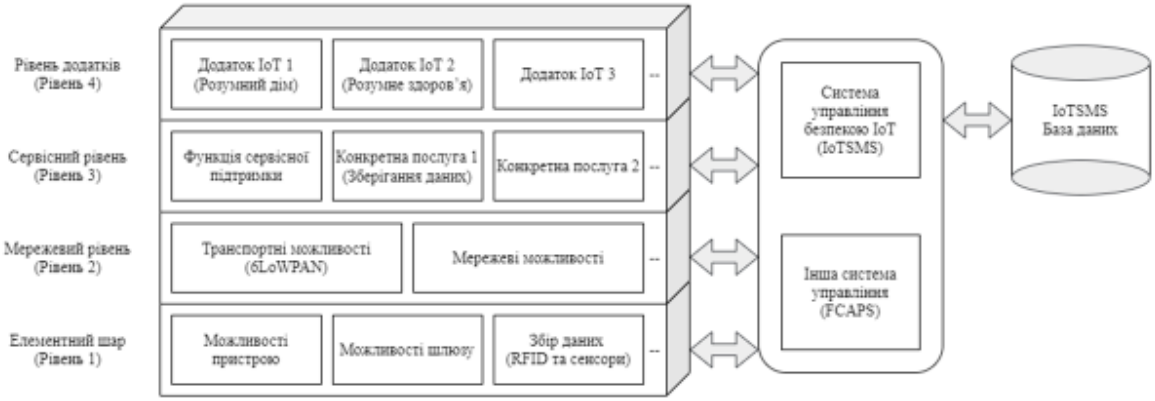
Мета і задачі роботи

Мета: аналіз методів захисту в IoT.

Задачі:
- аналіз існуючих методів захисту інформації в IoT;
- огляд еталонної моделі IoT;
- огляд заходів безпеки в IoT;
- аналіз існуючих загроз в мережі;
- розробка системи управління безпекою;
- розробка концепції сценарію розумного будинку.

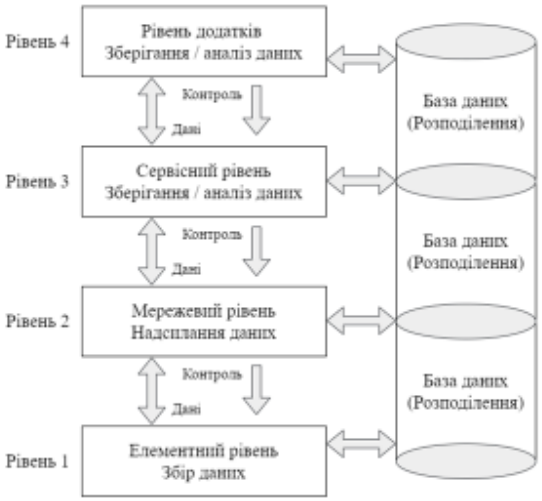
2

Еталонна модель IoT була розділена на чотири основні шари. Шари знизу вгору - це елементний рівень, мережевий рівень, рівень обслуговування та рівень додатків



3

Потік даних IoT можна розділити на чотири фази - збір даних, передача даних, зберігання даних та аналіз даних.



4

Розширений варіант загальної моделі Інтернету речей (IoT).

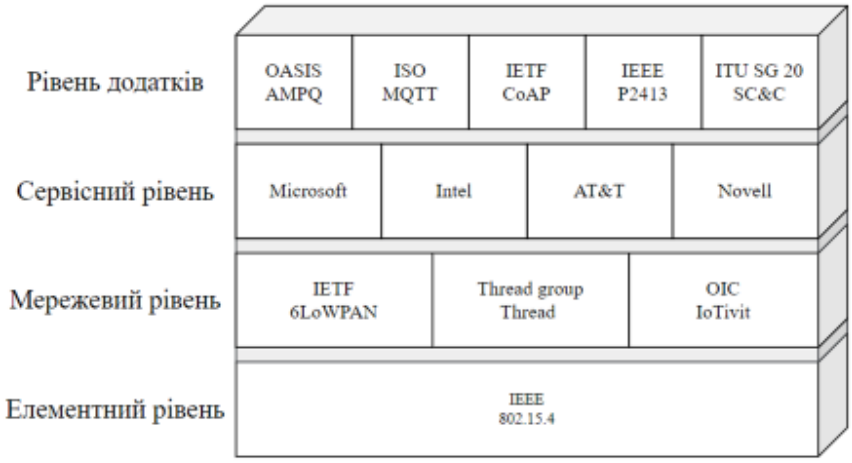
5

Політика безпеки та конфіденційності.

Пристрої IoT страждають від обчислювальної обробки, малої потужності та обмеженої пам'яті. Система IoT складається з трьох компонентів, таких як сенсорний блок, що має велику кількість датчиків, виконавчих механізмів та мобільних терміналів для виявлення фізичного середовища. Ця тендітна та проста структура IoT робить її більш вразливою до загроз, пов'язаних з безпекою IoT.

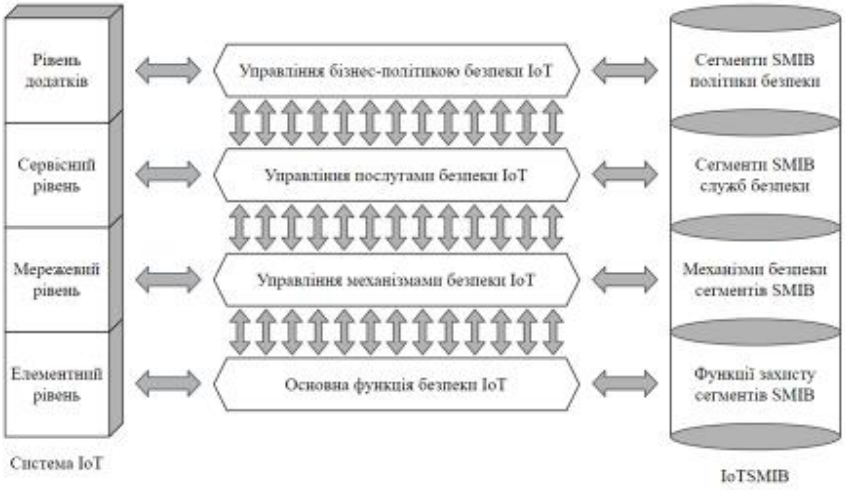
6

Стандарти та протоколи для IoT на кожному рівні



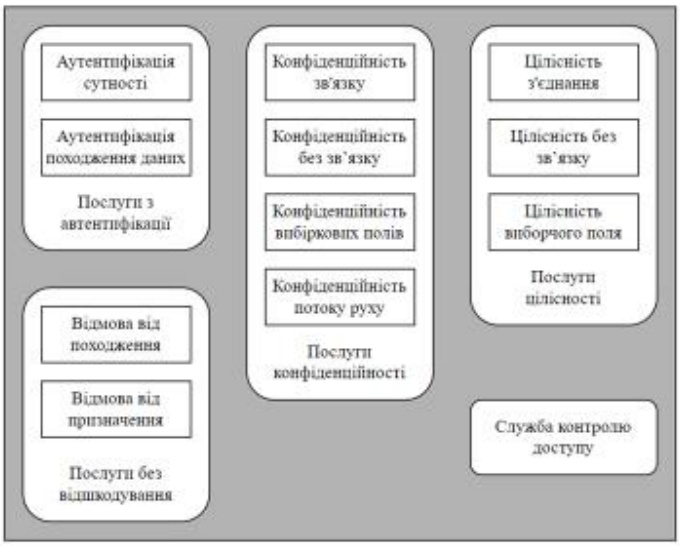
7

Система управління безпекою для IoT.



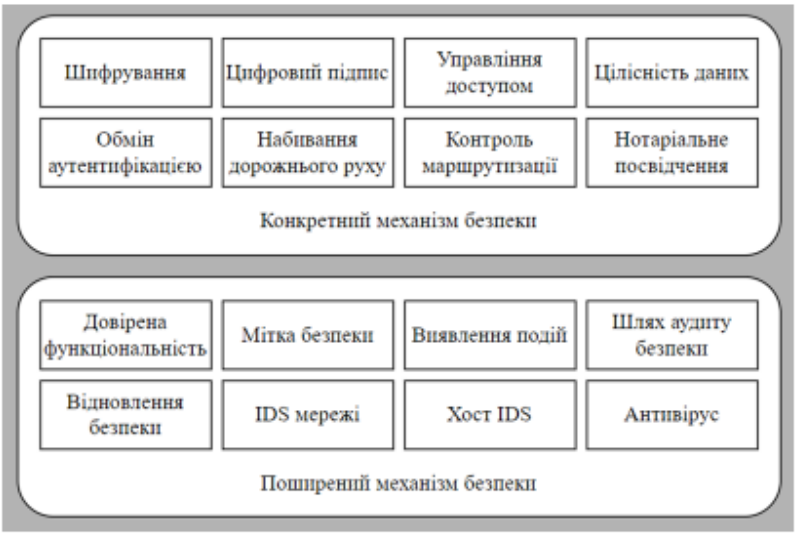
8

Рівень функціональності служб безпеки IoT.



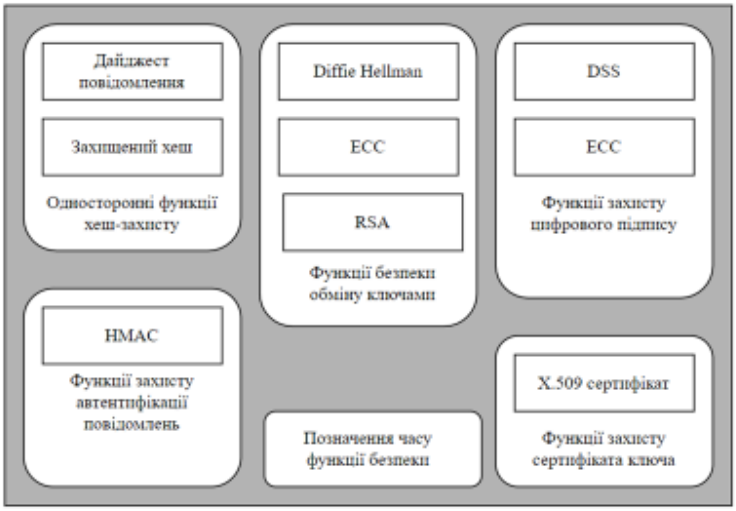
9

Функціональний рівень механізмів захисту IoT.



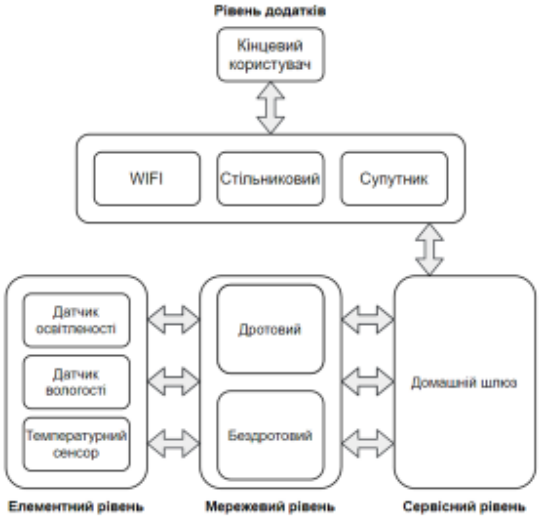
10

Фундаментальний рівень функціональної безпеки IoT.

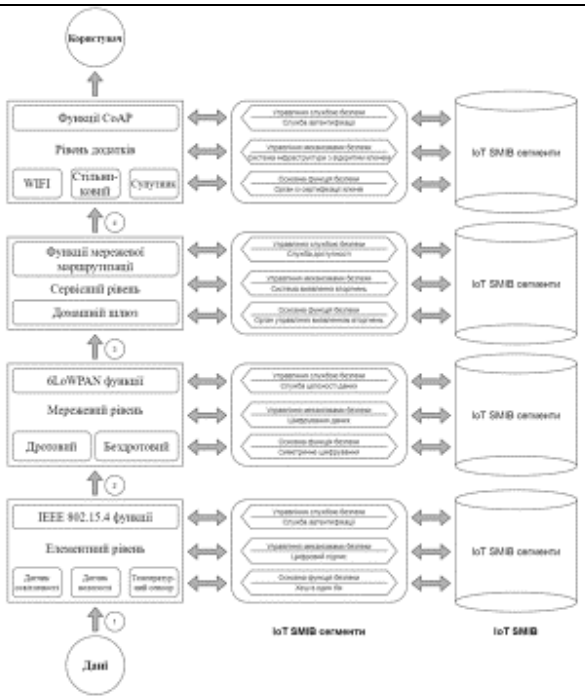


11

Концепція сценарію розумного будинку.



12



Потік даних сценарію розумного будинку.

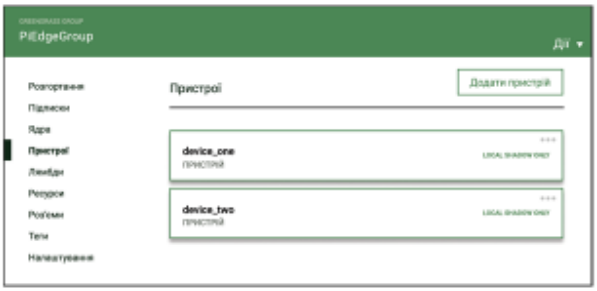
13

Впровадження запропонованої шаруватої моделі

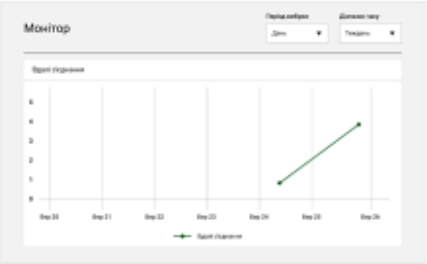
14

Сертифікат, приватні та відкриті ключі

Вузли з підтримкою IoT



Успішне з'єднання та обмін даними між вузлами. Вісь x представляє дні місяця, а вісь y – кількість з'єднань.



15

Висновки

У цій роботі було запропоновано нові багатошарові моделі IoT: загальні та розширені з ідентифікацією компонентів конфіденційності та безпеки. Запропонована система IoT, була впроваджена та оцінена.

Нижній рівень представлений IoT–вузлами, створеними з AmazonWeb Service (AWS).

Середній рівень (Edge) реалізований як апаратний комплект Raspberry Pi 4 за підтримки середовища Greengrass Edge в AWS.

Верхній рівень реалізований із використанням хмарного середовища IoT в AWS.

Протоколи безпеки та критичні сеанси управління знаходились між кожним із цих рівнів, щоб забезпечити конфіденційність інформації користувачів.

Було впроваджено сертифікати безпеки, щоб дозволити передачу даних між рівнями запропонованої моделі IoT.

16