# ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ**

Кваліфікаційна робота магістра

# Методи забезпечення інформаційного захисту IoT-системи на базі технології Intel

Студента групи КСМм-21-1
Скорика Вадима Анатолійовича

Керівник:
доц. кафедри ЕОМ
Піскарьов О.М.

Харків 2022

1

## *Актуальність проблеми*

**Одною з найбільших проблем Інтернету речей у наш час є проблема забезпечення захисту та приватності, тому вкрай важливим є розуміння значення надійної системи безпеки IoT-рішень, а також видів загроз та атак, з якими їй доведеться боротися.**


2

# *Мета та задачі роботи*

- **Розробка методів та засобів забезпечення інформаційного захисту IoT-систем.**
- **Дослідження актуальних алгоритмів та кращих практик забезпечення захисту IoT-систем.**
- **Моделювання та побудова комплексної моделі безпеки системи на базі розроблених методів та засобів протидії різноманітним загрозам.**
- **Створення демонстраційної IoT-системи на базі побудованої моделі безпеки.**

3

# *Загальна структура системи безпеки IoT-рішень*


4

# РОЗРОБЛЕНА МОДЕЛЬ ЗАХИСТУ СИСТЕМИ

**Безпечне підключення периферійних пристроєв**

**Безпека пристроїв**
- Симетричний ключ
- X.509 сертифікат

**За допомогою захищенного з'єднання**

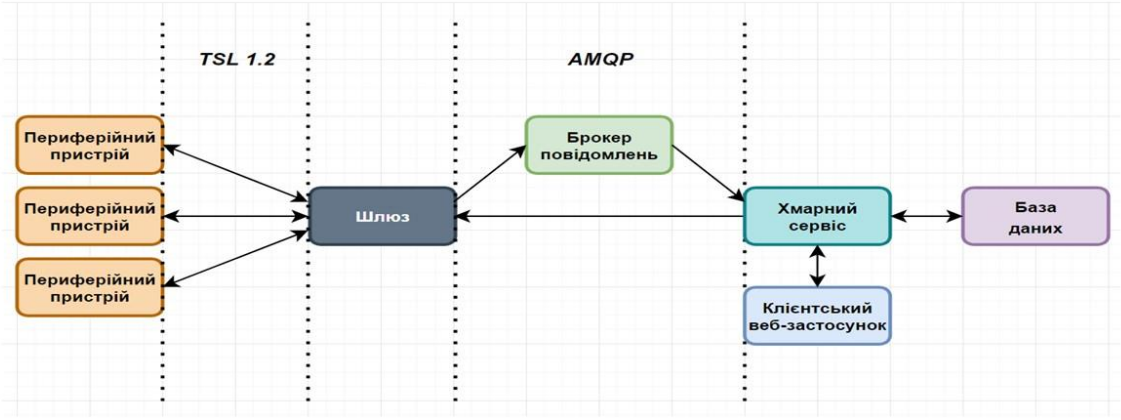
**Безпека з'єднання**
- Протокол рукостискання на базі протоколу TSL 1.2
- Шифрування та великий вибір шифрів

**До платформи**

**Хмарна безпека**
- Регистрація пристроїв
- Авторизація ключей

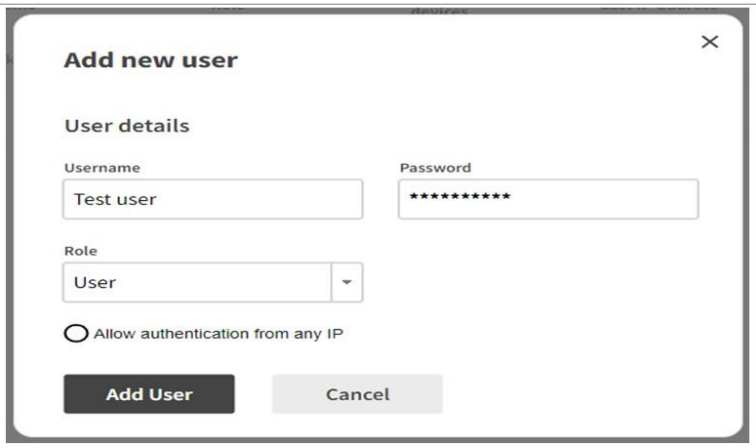
5

# ЗАГАЛЬНА СТРУКТУРНА МОДЕЛЬ ДЕМОНСТРАЦІЙНОЇ СИСТЕМИ



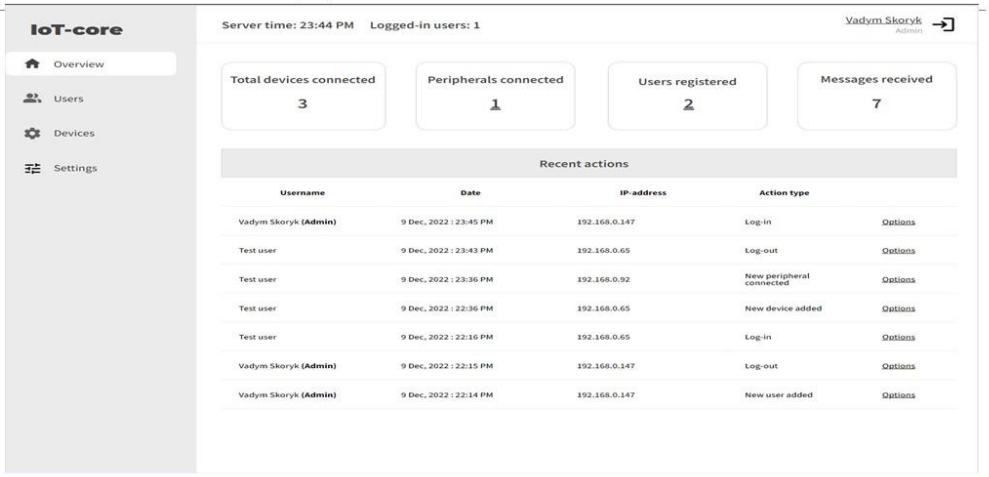

6

# ОГЛЯД РОЗРОБЛЕНОЇ ДЕМОНСТРАЦІЙНОЇ СИСТЕМИ – РЄЄСТРАЦІЯ ТА АВТЕНТИФІКАЦІЯ



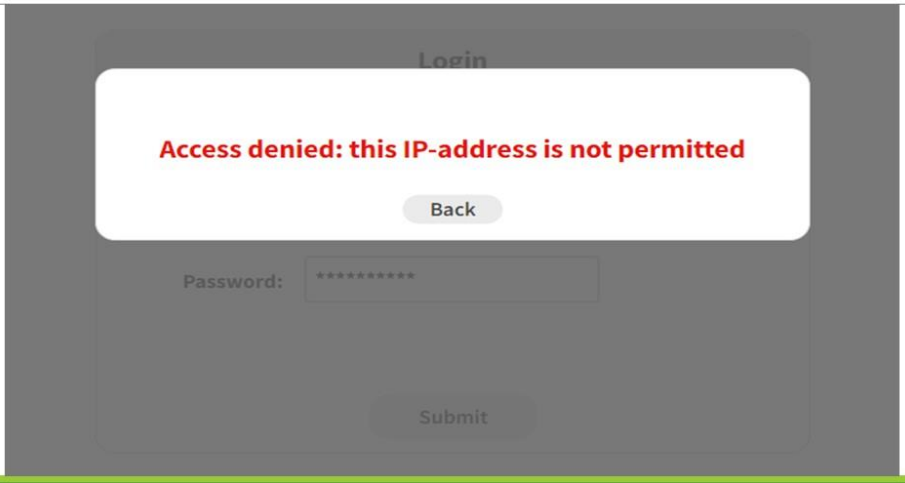

7

# ОГЛЯД РОЗРОБЛЕНОЇ ДЕМОНСТРАЦІЙНОЇ СИСТЕМИ – ПАНЕЛЬ МОНІТОРИНГУ АДМІНІСТРАТОРА



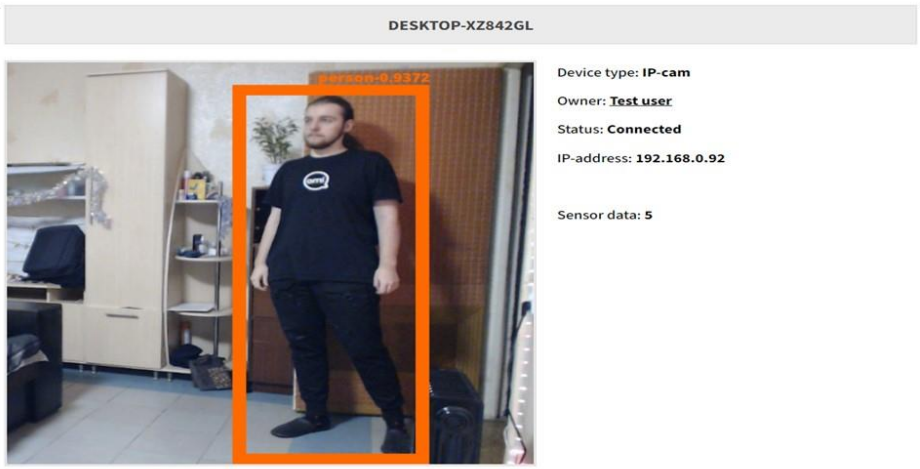

8

# ОГЛЯД РОЗРОБЛЕНОЇ ДЕМОНСТРАЦІЙНОЇ СИСТЕМИ – НАЛАШТУВАННЯ БЕЗПЕКИ




9

# ОГЛЯД РОЗРОБЛЕНОЇ ДЕМОНСТРАЦІЙНОЇ СИСТЕМИ – КОРИСТУВАЧІ ТА ЇХ ПРИСТРОЇ




10

# ПЛАТФОРМИ ТЕСТУВАННЯ СИСТЕМИ

Хмарний сервер було розгорнуто на наступній платформі:

- CPU – Intel Core i7-4770K @ 3.5 ГГц;
- RAM – 16 ГБ;
- GPU – NVIDIA GeForce GTX 1070;
- VRAM – 8 ГБ;
- OS – Windows 10.

У якості периферійного пристрою було використано платформу з наступною конфігурацією:

CPU – Intel Core i7-1065G7 @ 2.5 ГГц;
RAM – 16 ГБ;
GPU – Intel Iris Integrated Graphics;
OS – Windows 11.
Роздільна здатність – Full HD (1920x1080);
Фокусування – Авто;
Частота кадрів в секунду – 30;
Інтерфейс – USB 2.0.

11

# ВИСНОВКИ

У ході виконання кваліфікаційної роботи був проведений всебічний аналіз актуальних методів та кращих практик забезпечення захисту IoT-систем на кожному рівні, проведені дослідження щодо побудови комплексної моделі захисту системи на базі розроблених методів протидії різноманітним загрозам та атакам на усіх рівнях.

За підсумками огляду та проведених досліджень була побудована модель комплексної системи забезпечення захисту, яка здатна впоратися с більшістю розповсюджених у наш час загроз. Ця модель забезпечує захист усіх елементів системи на усіх рівнях – від периферійних пристроїв до хмарного сервісу та каналі обміну інформацією. На базі запропонованої моделі була створена демонстраційна IoT-система, що складається з хмарного серверу, клієнтського веб-застосунку для контролю та моніторингу стану системи та периферійного пристрою – IP-камери.

Серед можливих подальших напрямів удосконалення та розвитку системи – додавання системи детекції втручань, розширення функціоналу додаткових налаштувань безпеки та розширення спектру типів периферійних пристроїв, що підтримуються.

12

ДОДАТОК Б

Наукові публікації за темою кваліфікаційної роботи

Черкаський державний
технологічний університет

Військова Академія Збройних Сил
Азербайджанської республіки

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

ДП «Південний державний проектно-конструкторський
та науково-дослідний інститут авіаційної промисловості»

# ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

ТЕЗИ ДОПОВІДЕЙ ДЕСЯТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

24 – 25 листопада 2022 року

**Том 2:** секція 4

**Черкаси – Баку – Бельсько-Бяла – Харків – 2022**

# МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ ІОТ-СИСТЕМ

Скорик В.А., Піскарьов О.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Необхідність забезпечення якісної інформаційної безпеки будь якої мережі або системи важко переоцінити у наш час, вона виступає однією з найголовніших вимог до будь-якої інформаційної системи. Причиною цього є наявність нерозривного зв'язку між інформаційними технологіями та основними бізнес-процесами в усіх організаціях, державних службах, промислових підприємствах, фінансових структурах, операторах телекомунікацій тощо. Забезпечення інформаційної безпеки – актуальна тема і одночасно величезна проблема. Ніхто поки не вирішив її в загальному випадку, не існує універсальних алгоритмів рішення, які б підійшли до усіх можливих випадків, але існує велика кількість різноманітних методів та рішень, які здатні вирішити окремі випадки цього завдання.

Метою доповіді є аналіз актуальних архітектур IoT-систем [1], методів та алгоритмів їх захисту [2] та порівняння, розгляд їх застосування в існуючих провідних комерційних рішеннях [3] та побудова власної моделі інформаційного захисту на прикладі демонстраційної IoT-системи на базі Intel.

В доповіді аналізуються та порівнюються актуальні рішення, робляться висновки щодо доцільності тих чи інших методів та алгоритмів у рішенні проблеми забезпечення інформаційної безпеки. Будується блок-схема запропонованої системи, проводиться її моделювання [4]. Після аналізу стають очевидними сильні сторони таких комерційних систем, як AWS IoT та Azure IoT, що дозволяє застосувати деякі з їх алгоритмів у створенні власної моделі інформаційного захисту IoT-системи. Особливу увагу слід приділяти новим протоколам передачі даних, зокрема, стандарту 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) та іншим мережевим технологіям із криптографічними засобами, які забезпечують захищену передачу даних у IoT-системах.

**Список літератури**

1. Ahmed El Hakim // Internet of Things (IoT) System Architecture and Technologies // March 2018 // Researchgate DOI:10.13140/RG.2.2.17046.19521 – 5c.

2. Vint Cerf, Patrick Ryan, Max Senges, Richard Whitt // IoT safety and security as shared responsibility // March 2016 // Researchgate DOI:10.17323/1998-0663.2016.1.7.19 – 19 c.

3. Amazon Web Services // Securing Internet of Things (IoT) with AWS // 2022 // https://aws.amazon.com/ - 37c.

4. Maria Geller, Anderson Alvarenga // Modelling IoT Systems with UML: A Case Study for Monitoring and Predicting Power Consumption // January 2021 // Researchgate DOI:10.3844/ajeassp.2021.81.93–92c.