

АНОТАЦІЯ

Кваліфікаційна робота включає пояснювальну записку (87 с., 30 рис. 3 табл., 4 додатки, 16 аркушів презентації).

Об'єкт розробки – комп'ютерна система для дистанційного керування доступом.

Система дозволяє надійно управляти доступом до об'єктів (наприклад, дверей або шлюзів) у віддаленому режимі за допомогою мікроконтролера. У процесі розробки було реалізовано:

- проведено аналіз можливих рішень та технологій для побудови системи;
- сформульовано вимоги до системи. Оцінено необхідний рівень надійності та стабільності системи;
- створено скрипт для генерації сертифікатів захищеного з'єднання між пристроєм і сервером;
- реалізовано автоматичне постачання сертифікатів до пристрою;
- розроблено веб-застосунок для реєстрації користувачів, управління пристроями та перегляду історії виконаних і активних команд.

Для реалізації системи було використано хмарну платформу Amazon Web Services (AWS). Серверна частина та генерація сертифікатів реалізовані на основі DOTNET (C#). Для автентифікації та авторизації використано Keycloak як провайдер ідентифікації. Зберігання даних забезпечується базою даних PostgreSQL. Для клієнтської частини використано Node.js та бібліотеку React. Програмування пристрою здійснювалося за допомогою Arduino Framework мовами C/C++.

Ключові слова: мікроконтролер, ESP32, IoT, система захисту, identity provider, cloud, PostgreSQL, AWS, Keycloak, автоматична реєстрація пристроїв, Device Shadow, ASP.NET, Node.js, React, Arduino, MQTT.

ABSTRACT

The qualification project includes an explanatory report (87 pages, 30 figures, 3 tables, 4 appendices, 16 slides of presentation).

Object of development – a computer system for remote access control.

The system enables secure remote management of access to physical objects (such as doors or gateways) using a microcontroller-based device. During the development process, the following components were implemented:

- analysis of existing solutions and technologies for building the system;
- formulation of system requirements regarding reliability and stability;
- development of a script for generating security certificates for device-server communication;
- implementation of automatic certificate provisioning to the device;
- creation of a web application for user registration, device management, and monitoring of executed and active commands.

The system is built using the Amazon Web Services (AWS) cloud platform. The backend services and certificate generator are developed using DOTNET (C#). For authentication and authorization, Keycloak is used as the identity provider. PostgreSQL is used for data storage. The client-side application is developed with Node.js and React. The device firmware is written using the Arduino Framework in C/C++.

Keywords: microcontroller, ESP32, IoT, security system, identity provider, cloud, PostgreSQL, AWS, Keycloak, just-in-time device provisioning, device shadowing, ASP.NET, Node.js, React, Arduino, MQTT.