Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра комп'ютерно-інтегрованих технологій
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Розробка автоматизованої системи керування доступом до офісних приміщень на базі мікроконтролерів та засобів міжмережевої інтеграції

Виконав: студент IV курсу, групи КТс-41

спеціальності 174 Автоматизація та комп'ютерно-інтегровані технології
(шифр і назва спеціальності)

_____ Вовчук М.О.
(підпис) (прізвище та ініціали)

_____ Жукевич В.Р.
(підпис) (прізвище та ініціали)

Керівник _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Чихіра І.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

Рецензент _____ Дмитрів О.Р.
(підпис) (прізвище та ініціали)

Тернопіль
2026

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра комп'ютерно-інтегрованих технологій
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Голотенко О.С.
(підпис) (прізвище та ініціали)
«_14_» _ квітня 2026 р.__

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)
за спеціальністю 174 Автоматизація та комп'ютерно інтегровані технології
(шифр і назва спеціальності)
Студенту Вовчуку Михайлу Олеговичу
(прізвище, ім'я, по батькові)
1. Тема роботи Розробка автоматизованої системи керування доступом до офісних приміщень на базі мікроконтролерів та засобів міжмережевої інтеграції.

Керівник роботи Голотенко Олександр Сергійович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від « 14 » квітня_ 2026 року № _*4/9-185*_
2. Термін подання студентом завершеної роботи 25 червня 2025р.
3. Вихідні дані до роботи Наукові публікації про автоматизованої системи керування доступом до офісних приміщень
4. Зміст роботи
Вступ. 1 Аналітична частина. 1.1 Характеристика об'єкта автоматизації 1.2 Аналіз сучасних систем контролю та керування доступом 1.3 Аналіз апаратних засобів 1.4 Програмні і мережеві технології міжсистемної інтеграції 1.5 Формування функціональних і нефункціональних вимог 1.6 Висновок до першого розділу 2 Проектна частина 2.1 Розроблення загальної архітектури системи 2.2 Вибір і проєктування апаратної частини дверного контролера 2.3 Розроблення алгоритмів функціонування системи 2.4 Розроблення ПЗ мікроконтролера та серверної частини 2.5 Проєктування міжмережевої інтеграції та інформаційного обміну 2.6 Висновок до другого розділу 3 Спеціальна частина 3.1 Розроблення та опис експериментального макета системи 3.2 Методика тестування та перевірка працездатності системи 3.3 Аналіз інформаційної та кібербезпеки системи 3.4 Оцінка надійності та експлуатаційної придатності 3.5 Техніко-економічне обґрунтування та експлуатація системи 3.6 Висновок до третього розділу. 4 Охорона праці та безпека в надзвичайних ситуаціях Висновки, Перелік джерел, Додатки
5. Перелік графічного матеріалу
1 Титульна сторінка. 2 Тема, Мета, Об'єкт, Предмет дослідження. 3 Завдання дослідження. 4 Актуальність дослідження. 5 Схема об'єкта автоматизації системи керування доступом 6 Варіанти мережевої інтеграції 7 Структурна схема АСК доступом 8 Функціональна схема дверного контролера 9 Блок-схема алгоритму обробки спроби доступу 10 Алгоритм автономного режиму роботи контролера 11 ER-діаграма БД системи керування доступом 12 Схема міжмережевої інтеграції системи керування доступом 13 Експериментальний макет системи 14 Макет вебінтерфейсу адміністратора 15 Схема життєвого циклу події доступу в системі15 Висновки. 16 Завершальний.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека в надзвичайних ситуаціях	к.т.н., доц. Сенчишин В.С.		

7. Дата видачі завдання 14 квітня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	14.04.2026	*Виконано*
2.	Підбір джерел про автоматизованої системи керування	02.06.2026	*Виконано*
3.	Вибір компонентної бази	04.06.2026	*Виконано*
4.	Розроблення автоматизованої системи керування	05.06.2026	*Виконано*
	доступом до офісних приміщень		
5.	Переклад та опрацювання джерел	06.06.2026	*Виконано*
6.	Розроблення прототипу системи керування	07.06.2026	*Виконано*
7.	Оформлення розділу «Аналітична частина»	10.06.2026	*Виконано*
8.	Оформлення розділу «Проектна частина»	13.06.2026	*Виконано*
9.	Оформлення розділу «Спеціальна частина»	15.06.2026	*Виконано*
10.	Виконання розділу «Охорона праці та безпека в НС»	16.06.2026	*Виконано*
11	Підготовка графічного матеріалу	17.06.2026	*Виконано*
12.	Оформлення кваліфікаційної роботи	18.06.2026	*Виконано*
13.	Нормоконтроль	19.06.2026	*Виконано*
14.	Перевірка на плагіат	20.06.2026	*Виконано*
15.	Попередній захист кваліфікаційної роботи	23.06.2026	*Виконано*
16.	Захист кваліфікаційної роботи	25.06.2026	

Студент _____ Вовчук М.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра комп'ютерно-інтегрованих технологій
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Голотенко О.С.
(підпис) (прізвище та ініціали)
«_14_» _ квітня 2026 р.__

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)
за спеціальністю 174 Автоматизація та комп'ютерно інтегровані технології
(шифр і назва спеціальності)
Студенту Жукевичу Віталію Романовичу
(прізвище, ім'я, по батькові)
1. Тема роботи Розробка автоматизованої системи керування доступом до офісних приміщень на базі мікроконтролерів та засобів міжмережевої інтеграції.

Керівник роботи Голотенко Олександр Сергійович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від « 14 » квітня_ 2026 року № _*4/9-185*_____
2. Термін подання студентом завершеної роботи 25 червня 2025р.
3. Вихідні дані до роботи Наукові публікації про автоматизованої системи керування доступом до офісних приміщень
4. Зміст роботи
Вступ. 1 Аналітична частина. 1.1 Характеристика об'єкта автоматизації 1.2 Аналіз сучасних систем контролю та керування доступом 1.3 Аналіз апаратних засобів 1.4 Програмні і мережеві технології міжсистемної інтеграції 1.5 Формування функціональних і нефункціональних вимог 1.6 Висновок до першого розділу 2 Проектна частина 2.1 Розроблення загальної архітектури системи 2.2 Вибір і проєктування апаратної частини дверного контролера 2.3 Розроблення алгоритмів функціонування системи 2.4 Розроблення ПЗ мікроконтролера та серверної частини 2.5 Проєктування міжмережевої інтеграції та інформаційного обміну 2.6 Висновок до другого розділу 3 Спеціальна частина 3.1 Розроблення та опис експериментального макета системи 3.2 Методика тестування та перевірка працездатності системи 3.3 Аналіз інформаційної та кібербезпеки системи 3.4 Оцінка надійності та експлуатаційної придатності 3.5 Техніко-економічне обґрунтування та експлуатація системи 3.6 Висновок до третього розділу. 4 Охорона праці та безпека в надзвичайних ситуаціях Висновки, Перелік джерел, Додатки
5. Перелік графічного матеріалу
1 Титульна сторінка. 2 Тема, Мета, Об'єкт, Предмет дослідження. 3 Завдання дослідження. 4 Актуальність дослідження. 5 Схема об'єкта автоматизації системи керування доступом 6 Варіанти мережевої інтеграції 7 Структурна схема АСК доступом 8 Функціональна схема дверного контролера 9 Блок-схема алгоритму обробки спроби доступу 10 Алгоритм автономного режиму роботи контролера 11 ER-діаграма БД системи керування доступом 12 Схема міжмережевої інтеграції системи керування доступом 13 Експериментальний макет системи 14 Макет вебінтерфейсу адміністратора 15 Схема життєвого циклу події доступу в системі15 Висновки. 16 Завершальний.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека в надзвичайних ситуаціях	к.т.н., доц. Сенчишин В.С.		

7. Дата видачі завдання 14 квітня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	14.04.2026	*Виконано*
2.	Підбір джерел про автоматизованої системи керування	02.06.2026	*Виконано*
3.	Вибір компонентної бази	04.06.2026	*Виконано*
4.	Розроблення автоматизованої системи керування	05.06.2026	*Виконано*
	доступом до офісних приміщень		
5.	Переклад та опрацювання джерел	06.06.2026	*Виконано*
6.	Розроблення прототипу системи керування	07.06.2026	*Виконано*
7.	Оформлення розділу «Аналітична частина»	10.06.2026	*Виконано*
8.	Оформлення розділу «Проектна частина»	13.06.2026	*Виконано*
9.	Оформлення розділу «Спеціальна частина»	15.06.2026	*Виконано*
10.	Виконання розділу «Охорона праці та безпека в НС»	16.06.2026	*Виконано*
11	Підготовка графічного матеріалу	17.06.2026	*Виконано*
12.	Оформлення кваліфікаційної роботи	18.06.2026	*Виконано*
13.	Нормоконтроль	19.06.2026	*Виконано*
14.	Перевірка на плагіат	20.06.2026	*Виконано*
15.	Попередній захист кваліфікаційної роботи	23.06.2026	*Виконано*
16.	Захист кваліфікаційної роботи	25.06.2026	

Студент _____ Жукевичу В.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка автоматизованої системи керування доступом до офісних приміщень на базі мікроконтролерів та засобів міжмережевої інтеграції (комплексна тема). // Кваліфікаційна робота освітнього рівня «Бакалавр» // Вовчук Михайло Олегович, Жукевич Віталій Романович // Тернопільський національний технічний університет імені Івана Пулюя, факультет прикладних інформаційних технологій та електроінженерії, кафедра автоматизації та комп'ютерно-інтегрованих технологій, група КТс-41 // Тернопіль, 2026 // С. 53, рис. – 9, табл. – 15, кресл. – 17, додат. – 9, бібліогр. – 32.

Ключові слова: автоматизована система керування, мікроконтролер, ESP32, міжмережева інтеграція, база даних, журнал подій.

Кваліфікаційна робота присвячена розробці автоматизованої системи керування доступом до офісних приміщень на базі мікроконтролерів і засобів міжмережевої інтеграції.

У першому розділі проаналізовано об'єкт автоматизації, сучасні системи доступу, апаратні засоби, RFID/NFC-технології, мікроконтролерні платформи та мережеві протоколи. Сформовано основні вимоги до системи.

У другому розділі розроблено архітектуру системи, обґрунтовано вибір ESP32, описано дверний контролер, алгоритми обробки доступу, автономний режим, структуру програмного забезпечення, базу даних.

У третьому розділі описано експериментальний макет, тестування системи, а також питання кібербезпеки, надійності, відмовостійкості, економічної доцільності та безпечної експлуатації;

В четвертому розділі кваліфікаційної роботи: висвітлено питання з Безпеки життєдіяльності та Основ охорони праці.

Об'єкт дослідження: процес керування доступом до офісних приміщень.

Предмет дослідження: апаратно-програмні засоби автоматизації доступу, мікроконтролерні пристрої, мережеві протоколи, алгоритми автентифікації користувачів і механізми журналювання подій.

ANNOTATION

Development of an automated access control system for office premises based on microcontrollers and network integration tools (complex topic). // The educational level " Bachelor " qualification work // Vovchuk Mykhailo Olehovych, Zhukevych Vitalii Romanovych // Ternopil Ivan Pulyuy National Technical University, Faculty of Applied Information Technologies and Electrical Engineering, Department of Computer-Integrated Technologies, KTs-41 group // Ternopil, 2026 // P. 53, fig. - 9, tables - 15, chair. - 17, annexes - 9, ref. - 32.

Key words: automated control system, microcontroller, ESP32, cross-network integration, database, event log.

This qualification work devoted to the development of an automated access control system for office premises based on microcontrollers and network integration tools.

The first chapter analyses the automation target, modern access control systems, hardware, RFID/NFC technologies, microcontroller platforms and network protocols. The key requirements for the system have been defined.

The second chapter outlines the system architecture, justifies the choice of the ESP32, and describes the door controller, access processing algorithms, standalone mode, software structure and database.

The third chapter describes the experimental prototype, system testing, as well as issues relating to cybersecurity, reliability, fault tolerance, economic viability and safe operation;

The fourth chapter of the qualification thesis covers issues relating to Life Safety and the Fundamentals of Occupational Health and Safety.

Object of study: the process of controlling access to office premises.

Subject of study: hardware and software tools for access automation, microcontroller-based devices, network protocols, user authentication algorithms and event logging mechanisms.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БД – база даних, призначена для зберігання користувачів, карток доступу, правил і журналу подій.

ESP32 – мікроконтролерна платформа з підтримкою Wi-Fi та Bluetooth, використана як основа дверного контролера.

GPIO (англ. General Purpose Input/Output) – універсальні цифрові входи та виходи мікроконтролера.

HTTP (англ. HyperText Transfer Protocol) – протокол передавання даних у вебсередовищі.

JSON (англ. JavaScript Object Notation) – текстовий формат обміну структурованими даними між контролером і сервером.

MQTT (англ. Message Queuing Telemetry Transport) – легкий мережевий протокол обміну повідомленнями для IoT-пристроїв.

NFC (англ. Near Field Communication) – технологія безконтактної взаємодії пристроїв на малій відстані.

RFID (англ. Radio Frequency Identification) – технологія радіочастотної ідентифікації користувачів за картками або мітками.

REST API – архітектурний підхід до побудови вебінтерфейсу обміну даними між клієнтом і сервером.

SPI (англ. Serial Peripheral Interface) – послідовний інтерфейс для підключення периферійних пристроїв до мікроконтролера.

TLS (англ. Transport Layer Security) – криптографічний протокол для захисту мережевого обміну.

UID (англ. Unique Identifier) – унікальний ідентифікатор RFID/NFC-картки або мітки.

WebSocket – мережевий протокол для двостороннього обміну даними в реальному часі.

СКД – система контролю доступу, апаратно-програмний комплекс для ідентифікації користувачів, перевірки прав і керування доступом до приміщень.

ЗМІСТ

ВСТУП

Актуальність теми. Автоматизовані системи контролю та керування доступом є важливою складовою інженерної інфраструктури офісних приміщень, оскільки вони забезпечують регламентований доступ користувачів до окремих зон, фіксацію подій, централізоване адміністрування прав і можливість інтеграції з іншими інформаційними системами підприємства. Такі вимоги відповідають загальній логіці електронних систем контролю доступу, у яких поєднуються апаратні компоненти, програмна логіка, засоби ідентифікації, журналювання та адміністрування [1], [2].

Актуальність теми зумовлена потребою офісних об’єктів у системах, які мають бути одночасно автономними, масштабованими, економічно доцільними та захищеними від несанкціонованого втручання. Особливого значення набуває міжмережева інтеграція, оскільки дверний контролер повинен взаємодіяти з локальним сервером, базою даних, вебінтерфейсом адміністратора, журналом подій і, за потреби, віддаленим шлюзом або зовнішніми сервісами.

Використання мікроконтролерів у таких системах є доцільним завдяки можливості поєднати обробку сигналів від зчитувачів і датчиків, керування виконавчими пристроями та обмін даними через мережеві протоколи. Водночас система керування доступом є не лише вбудованим пристроєм, а й елементом інформаційної інфраструктури, тому для неї необхідно враховувати вимоги до кібербезпеки IoT-пристроїв, захисту обміну даними, автентифікації вузлів, оновлення програмного забезпечення та контролю доступу до адміністративних функцій [22], [23], [24].

Мета і задачі дослідження. Є є розробка автоматизованої системи керування доступом до офісних приміщень на базі мікроконтролерів із підтримкою мережевої взаємодії, адміністрування прав доступу, реєстрації подій та інтеграції з інформаційною інфраструктурою підприємства.

Для досягнення поставленої мети у роботі необхідно розв’язати такі основні завдання:

– Проаналізувати сучасні системи контролю та керування доступом до офісних приміщень.

– Визначити функціональні та нефункціональні вимоги до автоматизованої системи доступу.

– Обґрунтувати вибір мікроконтролерної платформи та основних апаратних компонентів системи.

– Розробити загальну архітектуру системи керування доступом з урахуванням апаратного, програмного та мережевого рівнів.

– Розробити алгоритми роботи системи у штатному, автономному та аварійному режимах.

– Спроєктувати програмне забезпечення мікроконтролера, серверну частину, базу даних і вебінтерфейс адміністратора.

– Спроєктувати засоби міжмережевої інтеграції та інформаційного обміну з використанням TCP/IP, MQTT, HTTP/REST API або WebSocket.

– Виконати оцінку працездатності, інформаційної безпеки, надійності, відмовостійкості та економічної доцільності запропонованого рішення.

Об’єкт дослідження: є процес керування доступом до офісних приміщень.

Предмет дослідження: апаратно-програмні засоби автоматизації доступу, мікроконтролерні пристрої, мережеві протоколи, алгоритми автентифікації користувачів і механізми журналювання подій.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає в удосконаленні підходу до побудови автоматизованої системи керування доступом до офісних приміщень шляхом поєднання мікроконтролерного дверного вузла, локальної автономної логіки прийняття рішень і засобів міжмережевої інтеграції з серверною частиною. На відміну від простих автономних електронних замків, запропоноване рішення передбачає не лише зчитування RFID/NFC-ідентифікатора та керування електрозамком, а й централізоване адміністрування прав доступу, журналювання подій, синхронізацію даних і роботу в умовах тимчасової втрати мережевого зв’язку.

У роботі набув подальшого розвитку підхід до організації гібридної архітектури системи доступу, у якій мікроконтролер ESP32 виконує функції локального контролера дверей, а серверна частина забезпечує зберігання користувачів, правил доступу, журналу подій і станів контролерів. Запропоновано логіку автономного режиму, що передбачає використання локального кешу дозволених ідентифікаторів, буферизацію подій при відсутності зв’язку та подальшу синхронізацію журналу після відновлення мережі.

Удосконалено структурну модель інформаційного обміну між дверним контролером і серверною частиною за рахунок поєднання MQTT для подієвого обміну, HTTP/REST API для адміністративних операцій і WebSocket для оперативного моніторингу стану системи. Такий підхід дозволяє розмежувати різні типи інформаційних потоків і підвищити гнучкість інтеграції системи з офісною інформаційною інфраструктурою.

Дістала подальшого розвитку модель безпечної експлуатації мікроконтролерної системи доступу, у якій одночасно враховано технічні, мережеві та організаційні аспекти: захист каналу обміну, автентифікацію контролерів, журналювання адміністративних дій, блокування втрачених ідентифікаторів, аналіз аварійних режимів, а також вибір режимів fail-safe і fail-secure залежно від призначення контрольованого приміщення.

Практичне значення одержаних результатів. Полягає в можливості використання запропонованої системи як прототипу для невеликого або середнього офісу, навчальної лабораторії, адміністративного приміщення чи окремої зони з обмеженим доступом. Завдяки використанню мікроконтролерної платформи, локального сервера, бази даних і відкритих мережевих протоколів система має потенціал для масштабування, модернізації та подальшої практичної реалізації.

1 АНАЛІТИЧНА ЧАСТИНА

Аналітична частина роботи спрямована на визначення технічних, функціональних та експлуатаційних передумов розроблення автоматизованої системи керування доступом до офісних приміщень. На цьому етапі необхідно дослідити об’єкт автоматизації, визначити характерні сценарії доступу, проаналізувати наявні технічні рішення, апаратні засоби та мережеві технології, які можуть бути використані для побудови системи.

Результатом аналітичної частини є формування вимог до майбутньої системи. Ці вимоги мають охоплювати не лише функції відкривання дверей за ідентифікатором, а й локальну автономність, журналювання подій, адміністрування користувачів, мережеву інтеграцію, кібербезпеку, масштабованість і придатність до експлуатації в умовах офісного середовища.

1.1 Характеристика об’єкта автоматизації

Об’єктом автоматизації у межах цієї роботи є офісне приміщення або група офісних приміщень, доступ до яких має здійснюватися за встановленими правилами. Для кожної контрольованої точки доступу може бути встановлений окремий режим роботи, оскільки вимоги до входу в загальну офісну зону, серверну кімнату або архів істотно відрізняються за рівнем безпеки, кількістю користувачів і допустимими аварійними сценаріями.

Система контролю та керування доступом у цьому випадку розглядається як апаратно-програмний комплекс, що виконує ідентифікацію користувача, перевірку його прав, керування виконавчим пристроєм, фіксацію події та передавання даних до серверної частини. Відповідно до загальних вимог до електронних систем доступу, така система повинна забезпечувати не лише фізичне блокування або розблокування дверей, а й контроль стану системи, реєстрацію подій, оброблення прав доступу та підтримку експлуатаційних процедур [1], [2].

Основними категоріями користувачів офісної системи доступу є працівники, адміністратори, відвідувачі, охорона та технічний персонал. Технічний персонал отримує доступ до інженерних або сервісних зон відповідно до регламенту обслуговування.

До процесів, що підлягають автоматизації, належать ідентифікація користувача за RFID/NFC-карткою або іншим ідентифікатором, перевірка прав доступу, керування електромеханічним або електромагнітним замком, фіксація часу входу, ведення журналу подій, адміністрування користувачів, блокування втрачених або недійсних ідентифікаторів, а також робота системи у штатному, автономному й аварійному режимах. Особливість автоматизованого підходу полягає в тому, що рішення про доступ ухвалюється не людиною, а програмною логікою на основі ідентифікатора, правил доступу, стану дверей, мережевого зв’язку та поточного режиму роботи системи.

Постановка задачі керування доступом полягає у створенні системи, яка забезпечує санкціонований доступ до офісних приміщень, знижує ризик несанкціонованого проникнення, мінімізує ручний контроль і формує достовірний журнал подій. Для цього дверний контролер повинен мати локальний кеш дозволених ідентифікаторів, а серверна частина — централізовано зберігати користувачів, правила доступу, події та службову інформацію.

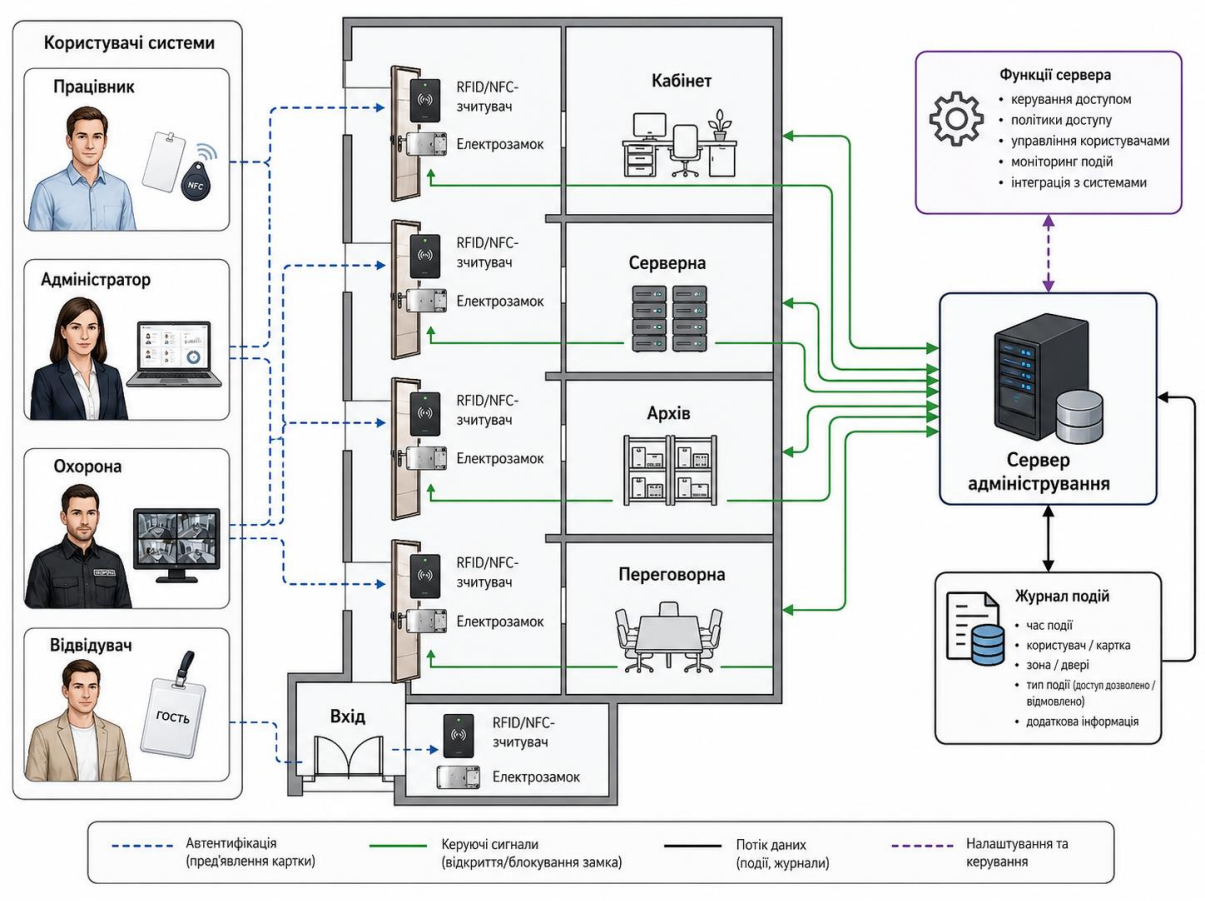


Рисунок 1.1 – Узагальнена схема об’єкта автоматизації офісної системи керування доступом

1.2 Аналіз сучасних систем контролю та керування доступом

Сучасні системи доступу можна поділити на кілька груп залежно від способу ідентифікації користувача, рівня автоматизації, наявності мережевої інтеграції та можливості централізованого адміністрування. Кодові панелі дають змогу відмовитися від механічного ключа, але мають ризик розголошення коду, спільного використання одного пароля кількома особами та обмежені можливості персоналізованого обліку доступу. RFID/NFC-системи є поширеним рішенням для офісного доступу, оскільки дозволяють ідентифікувати користувача за індивідуальною карткою або брелоком. Недоліком є потреба в належному захисті ідентифікаторів, оскільки прості UID-картки можуть бути недостатніми для високозахищених зон.

Біометричні системи забезпечують прив’язку доступу до фізіологічних характеристик людини, наприклад відбитка пальця або обличчя. Мобільні

ідентифікатори на основі смартфонів підвищують зручність користування, але залежать від мобільного пристрою, програмного застосунку та політики безпеки підприємства. IP-системи контролю доступу та хмарні системи адміністрування є більш функціональними, оскільки підтримують централізоване керування, віддалений моніторинг, журналювання подій і інтеграцію з іншими сервісами. Така архітектура поєднує локальну працездатність, централізоване керування та можливість подальшого масштабування.

Таблиця 1.1 – Порівняльна характеристика сучасних засобів контролю доступу

Тип системи	**Переваги**	**Недоліки**	**Доцільність для роботи**
Механічні ключі	Низька вартість, простота	Немає журналювання, складне відкликання доступу	Низька
Кодова панель	Простота монтажу, немає фізичного ключа	Ризик розголошення коду, слабка персоналізація	Обмежена
RFID/NFC	Швидка ідентифікація, індивідуальні картки, просте блокування	Потребує захисту ідентифікаторів	Висока
Біометрія	Складніше передати ідентифікатор іншій особі	Вища вартість, питання персональних даних	Середня
IP-система	Централізоване керування, журналювання, інтеграція	Вища складність і вартість	Висока
Хмарна система	Віддалене адміністрування, масштабованість	Залежність від інтернету та провайдера	Середня
Гібридна система	Поєднання автономності та серверного керування	Потребує продуманої архітектури	Найбільш доцільна

Для цієї бакалаврської роботи найбільш обґрунтованим є гібридне рішення на базі мікроконтролера з RFID/NFC-ідентифікацією та мережевою інтеграцією. Такий підхід відповідає вимогам до електронних систем доступу, а також узгоджується з принципами безпечного включення IoT-пристроїв до інформаційної інфраструктури [1], [22], [24].

1.3 Аналіз апаратних засобів

Апаратна частина автоматизованої системи керування доступом складається з пристроїв ідентифікації, оброблення сигналів, керування виконавчим механізмом, індикації, живлення та мережевого обміну. Центральним елементом дверного вузла є мікроконтролер, який отримує дані від RFID/NFC-зчитувача, аналізує стан кнопки виходу та датчика дверей, керує замком, формує індикацію, зберігає частину даних локально й обмінюється повідомленнями із сервером.

RFID/NFC-зчитувач забезпечує отримання ідентифікатора картки або брелока. У системах з підвищеними вимогами до безпеки доцільно використовувати не лише UID картки, а й додаткові криптографічні або серверні механізми перевірки, однак для бакалаврського прототипу достатньо реалізувати структуровану логіку зберігання та перевірки ідентифікаторів.

Виконавчим елементом є електромеханічний або електромагнітний замок. Для керування силовим колом замка мікроконтролер не може використовувати GPIO безпосередньо, тому необхідний релейний модуль або MOSFET-ключ із захистом від зворотної ЕРС, короткого замикання та перевантаження.

До складу дверного вузла також входять датчик стану дверей, кнопка виходу, світлова індикація, звуковий сигналізатор, блок живлення, резервне живлення, корпус і монтажні елементи. Світлодіодна й звукова індикація потрібні для інформування користувача про дозволений доступ, відмову, помилку зчитування або аварійний стан.

Окремого аналізу потребує вибір мікроконтролерної платформи. Arduino UNO R3 є простим для навчального прототипування, проте має обмежені ресурси й не містить вбудованого Wi-Fi [11].

Таблиця 1.2 — Порівняння мікроконтролерних платформ для системи керування доступом

Критерій	**ESP32**	**STM32**	**Arduino UNO R3**	**Промисловий контролер**
Мережеві можливості	Wi-Fi/Bluetooth вбудовано	Залежить від моделі або модуля	Потрібен зовнішній модуль	Часто Ethernet/RS-485
Продуктивність	Достатня для IoT-системи	Висока	Обмежена	Висока надійність
Кількість GPIO	Достатня	Залежить від моделі	Обмежена	Залежить від конфігурації
Вартість	Низька	Середня	Низька	Висока
Програмування	ESP-IDF, Arduino Core	STM32CubeIDE, HAL	Arduino IDE	Спеціалізоване ПЗ
Придатність для прототипу	Висока	Висока	Середня	Низька через вартість
Доцільність у роботі	Найвища	Альтернатива	Для спрощених макетів	Для промислової реалізації

З огляду на вимоги до мережевої інтеграції, вартості, доступності бібліотек і придатності до прототипування, базовою апаратною платформою для подальшого проєктування доцільно обрати ESP32. Такий вибір дає змогу реалізувати дверний контролер без додаткового Wi-Fi-модуля, підключити RFID/NFC-зчитувач, датчики, індикацію й виконавчий елемент, а також забезпечити обмін із серверною частиною через стандартні мережеві протоколи.

1.4 Програмні і мережеві технології міжсистемної інтеграції

Міжмережева інтеграція є ключовою ознакою проєктованої системи, оскільки дверний контролер не повинен працювати як ізольований електронний замок. Для цього необхідно визначити технології зв’язку, протоколи обміну та способи захисту інформаційних потоків.

На фізичному та канальному рівнях можуть використовуватися Ethernet, Wi-Fi або RS-485. RS-485 може бути доцільним для підключення декількох

контролерів на значних відстанях у межах будівлі, однак для інтеграції з сервером усе одно потрібен шлюз до TCP/IP-мережі.

На транспортному рівні базовим протоколом є TCP, який забезпечує надійну доставку даних між мережевими вузлами [13]. WebSocket забезпечує двосторонній канал зв'язку для відображення подій у реальному часі без постійного опитування сервера [16].

Для передавання структурованих даних доцільно використовувати JSON, оскільки цей формат є компактним, текстовим і широко підтримується серверними та вбудованими платформами [17]. Для авторизації адміністратора або сервісної взаємодії може застосовуватися JWT або API-ключ контролера [19].

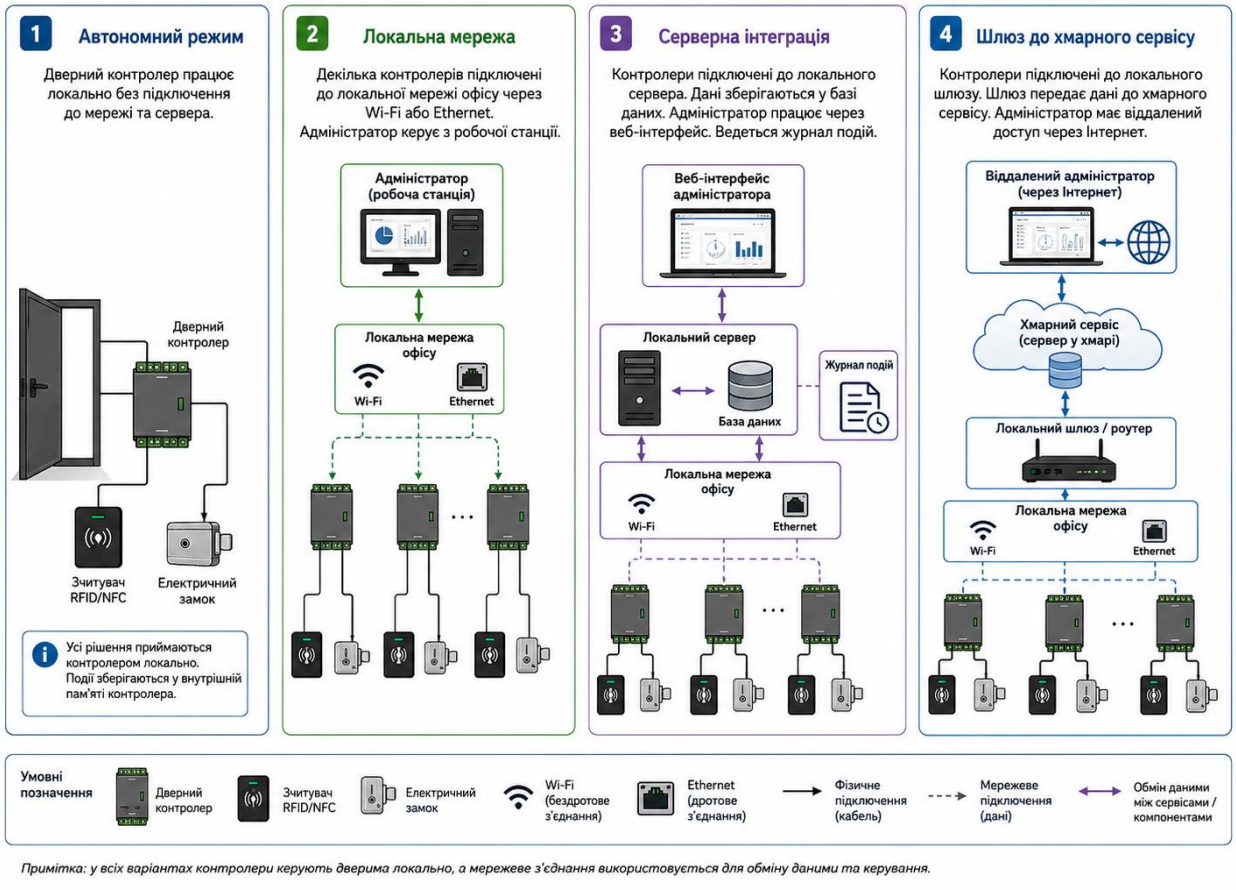


Рисунок 1.2 – Варіанти мережевої інтеграції дверних контролерів із серверною частиною

У межах проєктованої системи доцільною є комбінована мережева модель. Така логіка забезпечує баланс між автономністю, централізованим керуванням і мережевою інтеграцією.

1.5 Формування функціональних і нефункціональних вимог

Формування вимог є завершальним етапом аналітичної частини й основою для подальшого проєктування. Для систем доступу важливо, щоб функції ідентифікації, перевірки прав, керування замком і журналювання працювали узгоджено, а адміністрування не створювало додаткових ризиків безпеки [1], [2].

Функціональні вимоги визначають, які дії система має виконувати. Окремою вимогою є можливість блокування втраченого ідентифікатора, оскільки фізична картка може бути передана іншій особі або втрачена.

Нефункціональні вимоги визначають якісні характеристики системи. Серверна частина має враховувати типові ризики API, зокрема слабку автентифікацію, помилки авторизації, надмірне розкриття даних і недостатнє журналювання [20], [21].

З погляду інформаційної безпеки система повинна реалізовувати принцип мінімально необхідних прав, розділяти ролі адміністратора й користувача, зберігати паролі у захищеному вигляді, використовувати токени або API-ключі для контролерів, шифрувати мережевий обмін, вести журнал адміністративних дій і виконувати резервне копіювання бази даних. Для аналізу ризиків доцільно враховувати ймовірність втрати картки, підміни контролера, повторної передачі повідомлення, несанкціонованого доступу до вебінтерфейсу та відмови мережевого з’єднання [24], [28].

Таблиця 1.3 — Функціональні та нефункціональні вимоги до автоматизованої системи керування доступом

Група вимог	**Вимога**	**Очікуваний результат**
Ідентифікація	Зчитування RFID/NFC-ідентифікатора	Система отримує унікальний код користувача
Авторизація	Перевірка прав доступу	Доступ надається лише дозволеним користувачам
Керування	Активація замка	Двері відкриваються на заданий час
Журналювання	Запис усіх спроб доступу	Події доступні для аналізу адміністратором
Адміністрування	Керування користувачами й картками	Права доступу змінюються централізовано
Автономність	Локальна перевірка при втраті мережі	Система не припиняє роботу повністю
Синхронізація	Передавання накопичених подій	Журнал відновлюється після появи зв’язку
Безпека	TLS, токени, ролі, журнал дій	Зменшується ризик несанкціонованого втручання
Надійність	Оброблення відмов і аварій	Система переходить у безпечний режим
Масштабованість	Додавання нових контролерів	Система може розширюватися на інші двері

Отже, майбутня система має бути побудована як поєднання локального дверного контролера, серверної частини, бази даних, вебінтерфейсу та засобів мережевого обміну. Такий склад дозволяє забезпечити автоматизовану перевірку прав доступу, журналювання, централізоване адміністрування, автономну роботу при втраті зв’язку та підготовку до подальшого масштабування.

1.6 Висновок до першого розділу

У першому розділі охарактеризовано офісне приміщення як об’єкт автоматизації та визначено основні процеси, які має виконувати система контролю та керування доступом: ідентифікацію користувача, перевірку прав, керування замком, журналювання подій, адміністрування користувачів і

підтримку аварійних режимів. Аналіз сучасних підходів показав, що механічні ключі й прості кодові пристрої не забезпечують достатнього рівня гнучкості та журналювання, тоді як RFID/NFC-рішення з мікроконтролерною основою і серверною інтеграцією є більш придатними для офісних систем середнього рівня складності.

За результатами аналізу обґрунтовано доцільність використання гібридної архітектури, у якій дверний контролер на базі ESP32 виконує локальні функції ідентифікації та керування замком, а серверна частина забезпечує централізоване адміністрування, зберігання журналу подій і мережеву інтеграцію. Сформовані функціональні та нефункціональні вимоги визначають основу для подальшої проєктної частини, де буде розроблено архітектуру системи, апаратний вузол дверного контролера, алгоритми роботи, програмне забезпечення та засоби міжмережевого обміну.

2 ПРОЕКТНА ЧАСТИНА

Проєктна частина роботи присвячена розробленню технічного рішення автоматизованої системи керування доступом до офісних приміщень. На основі вимог, сформованих в аналітичному розділі, необхідно визначити архітектуру системи, склад апаратного вузла, алгоритми функціонування, структуру програмного забезпечення, базу даних і механізми міжмережевої інтеграції.

Запропонована система розглядається як гібридне апаратно-програмне рішення, у якому дверний контролер виконує локальні функції зчитування ідентифікатора та керування замком, а серверна частина забезпечує централізоване адміністрування користувачів, зберігання правил доступу, журналювання подій і мережеву взаємодію. Такий підхід поєднує автономність мікроконтролерного вузла з перевагами централізованого керування, що відповідає вимогам до електронних систем контролю доступу [1], [2].

2.1 Розроблення загальної архітектури системи

Архітектуру автоматизованої системи керування доступом доцільно будувати за багаторівневим принципом. Це дає змогу розділити функції між виконавчими пристроями, дверним контролером, мережевою інфраструктурою та серверною частиною. Такий розподіл спрощує проєктування, тестування, модернізацію й подальше масштабування системи.

Перший рівень утворюють виконавчі та периферійні пристрої, які безпосередньо взаємодіють із дверима й користувачем. Електрозамок виконує фізичне блокування або розблокування дверей, датчик стану дверей дає змогу контролювати факт відкривання, кнопка виходу забезпечує санкціоноване відкривання з внутрішнього боку, а індикатори інформують користувача про результат операції.

Другий рівень становить дверний контролер. На цьому рівні реалізується первинна обробка подій: зчитування картки, перевірка локального стану, керування замком, формування повідомлення для сервера та збереження події у буфері при втраті зв’язку.

Третій рівень — рівень мережевої інтеграції. Для оперативного відображення стану дверей і подій у реальному часі може використовуватися WebSocket [16].

Четвертий рівень — серверне програмне забезпечення.

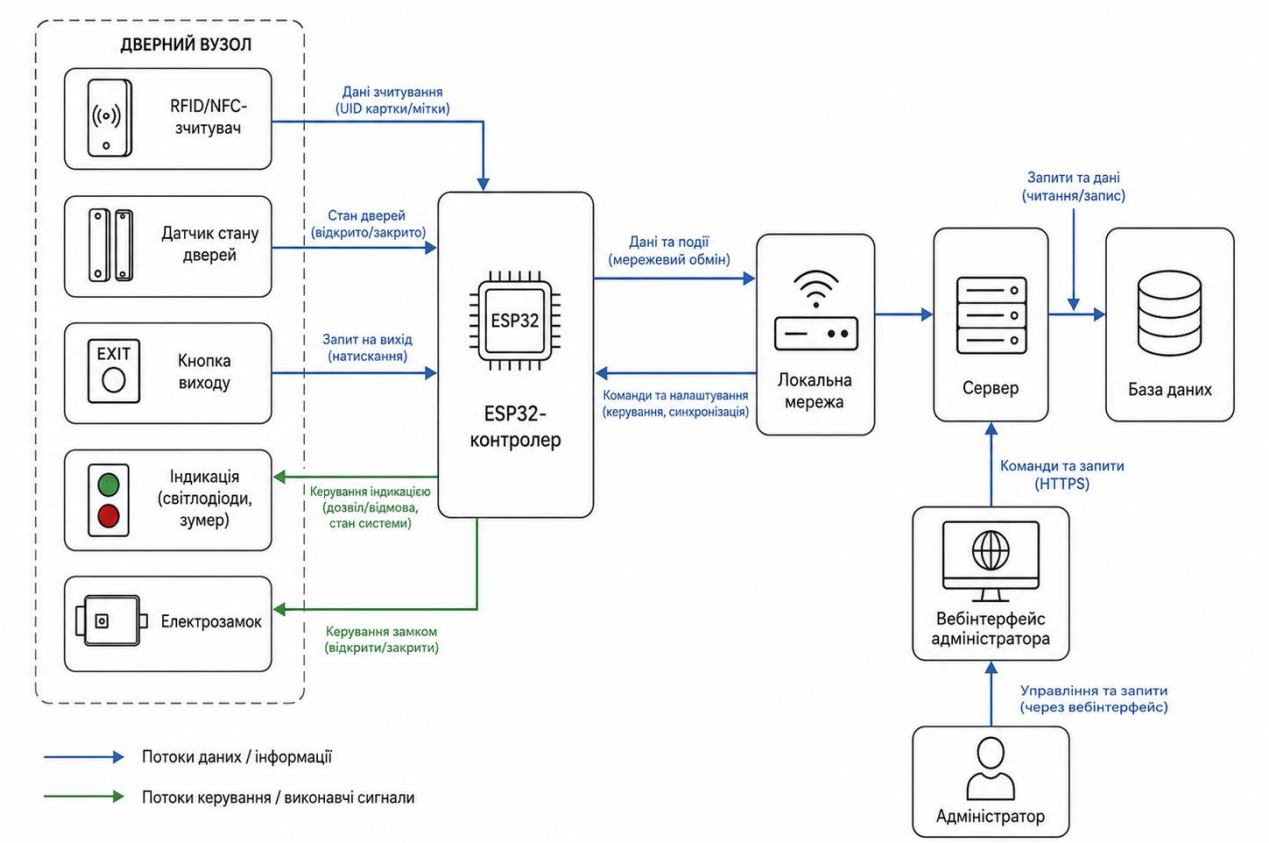


Рисунок 2.1 – Структурна схема автоматизованої системи керування доступом

У штатному режимі потік даних починається з прикладання RFID/NFC-картки до зчитувача. Усі події передаються до серверної частини у структурованому форматі JSON, який є стандартним форматом обміну даними для веб- і мережевих застосунків [17].

Архітектура передбачає, що дверний контролер не залежить повністю від постійної доступності сервера.

2.2 Вибір і проєктування апаратної частини дверного контролера

Дверний контролер є центральним апаратним вузлом системи. Цей мікроконтролер має достатні ресурси для реалізації IoT-вузла доступу, підтримує Wi-Fi, містить набір цифрових входів/виходів і може працювати з периферією через SPI, I2C та UART [7].

Для ідентифікації користувача доцільно застосувати RFID/NFC-зчитувач MFRC522 або сумісний модуль. Для промислової реалізації доцільно передбачити використання захищеніших ідентифікаторів, однак для бакалаврського проєкту достатньо реалізувати архітектуру з можливістю подальшої модернізації.

Керування електрозамком виконується через проміжний силовий елемент. У будь-якому випадку силове коло замка має бути захищене від зворотної ЕРС, короткого замикання та перевантаження.

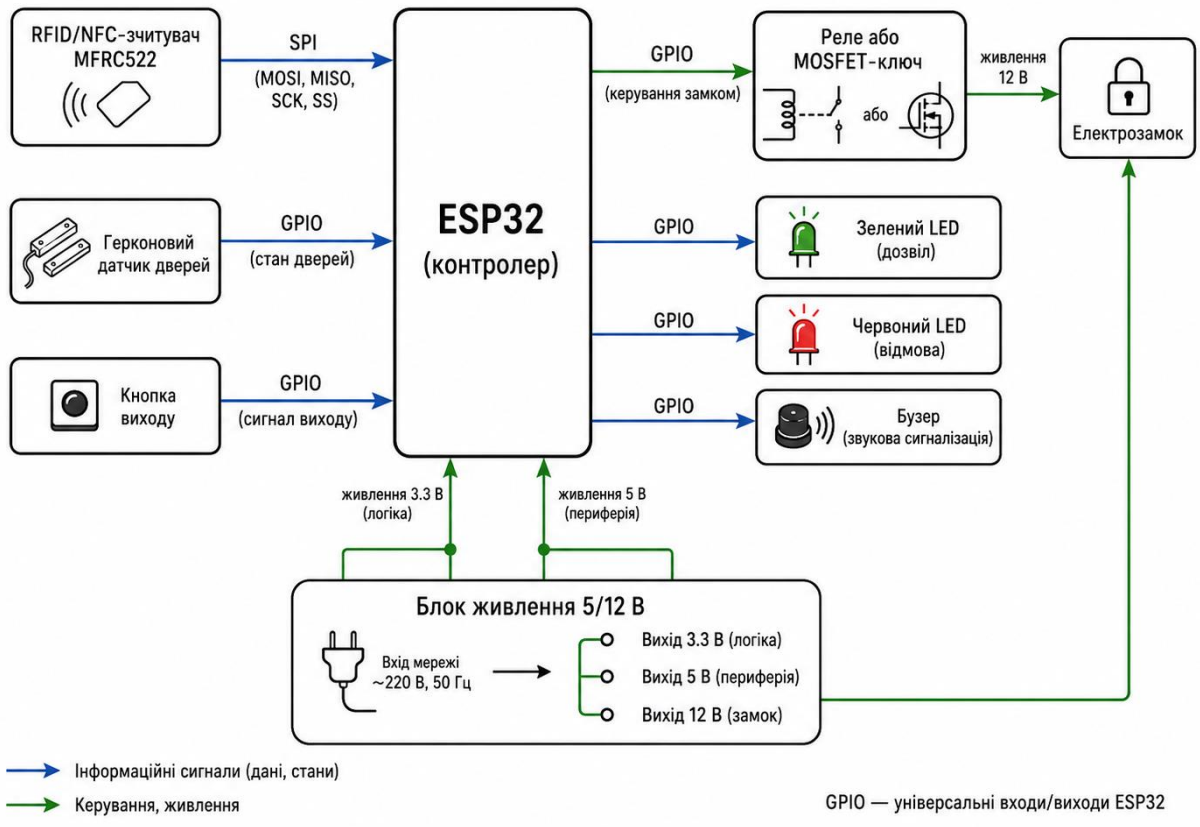


Рисунок 2.2 — Функціональна схема дверного контролера

До входів контролера підключаються кнопка виходу та датчик стану дверей. Світлова індикація може мати стани “очікування”, “доступ дозволено”, “доступ заборонено”, “помилка мережі” та “аварійний режим”.

Таблиця 2.1 — Призначення входів і виходів мікроконтролера

Сигнал	**Напрям**	**Призначення**	**Приклад підключення**
SPI MOSI/MISO/SCK	Вхід/вихід	Обмін із RFID/NFC-зчитувачем	MFRC522
RFID SS	Вихід	Вибір RFID-модуля на SPI-шині	GPIO контролера
RFID RST	Вихід	Скидання RFID-модуля	GPIO контролера
LOCK_CTRL	Вихід	Керування реле або MOSFET-ключем	Модуль замка
DOOR_SENSOR	Вхід	Контроль стану дверей	Геркон
EXIT_BUTTON	Вхід	Кнопка виходу	Нормально розімкнений контакт
LED_GREEN	Вихід	Індикація дозволеного доступу	Світлодіод
LED_RED	Вихід	Індикація відмови або помилки	Світлодіод
BUZZER	Вихід	Звуковий сигнал	Активний бузер
UART/I2C резерв	Вхід/вихід	Можливе розширення	Дисплей, зовнішній модуль

Живлення системи доцільно розділити на логічну та силову частини. Для електрозамка типово застосовується окреме джерело 12 В, але конкретна напруга залежить від обраного замка.

Таблиця 2.2 — Орієнтовне енергоспоживання компонентів системи

Компонент	**Напруга живлення**	**Орієнтовний струм**	**Орієнтовна потужність**
ESP32	3,3 В	0,12–0,25 А	0,4–0,8 Вт
MFRC522	3,3 В	0,03–0,06 А	0,1–0,2 Вт
Релейний модуль	5 В	0,07–0,09 А	0,35–0,45 Вт
Світлодіоди та бузер	3,3–5 В	0,02–0,08 А	0,1–0,4 Вт
Електрозамок	12 В	0,4–0,8 А	4,8–9,6 Вт

Для оцінки резервного живлення можна прийняти максимальне споживання логічної частини близько 1,5 Вт і силової частини до 10 Вт під час активації замка. У реальному проєкті цей розрахунок уточнюється за характеристиками конкретного замка та блока живлення.

Проєктування апаратної частини має враховувати вимоги електробезпеки. Загальні принципи безпечної експлуатації електронного та інформаційно-комунікаційного обладнання, а також захисту від ураження електричним струмом визначаються відповідними стандартами безпеки [26], [27].

2.3 Розроблення алгоритмів функціонування системи

Алгоритми функціонування системи мають забезпечити узгоджену роботу апаратної та програмної частин у різних режимах.

Алгоритм штатного доступу починається з переходу контролера в режим очікування. Після позитивної перевірки активується замок на заданий час, подається зелена індикація, контролюється відкриття дверей і формується подія журналу.

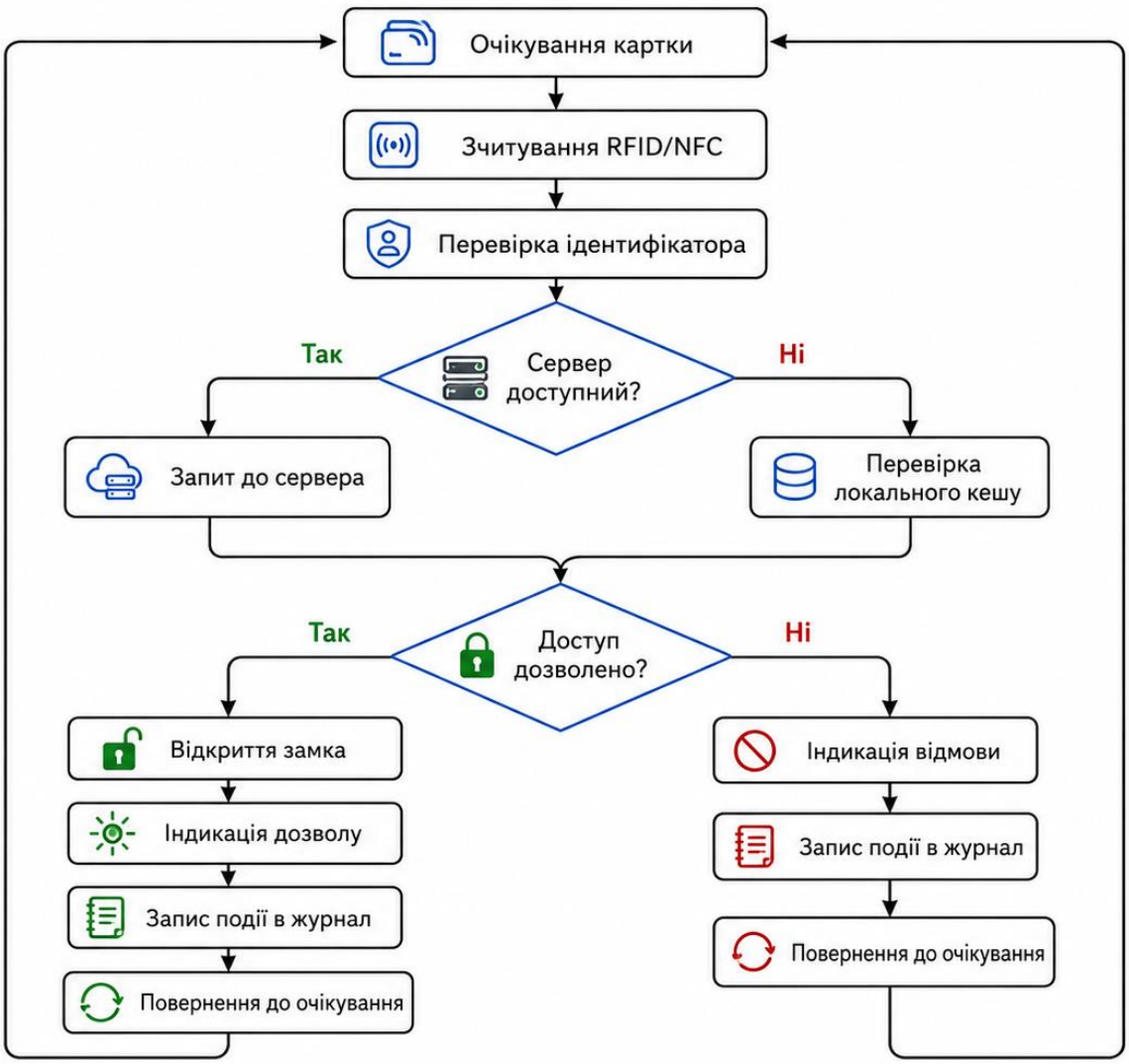


Рисунок 2.3 — Блок-схема алгоритму обробки спроби доступу

У разі відмови в доступі контролер не активує замок, а формує звуковий або світловий сигнал відмови. Якщо протягом короткого часу зафіксовано кілька невдалих спроб, система може тимчасово заблокувати повторні запити з цього ідентифікатора або сформувати попередження для адміністратора.

Алгоритм автономної роботи активується при втраті зв’язку з сервером або MQTT-брокером. Для запобігання дублюванню кожна подія повинна мати унікальний локальний номер або UUID.

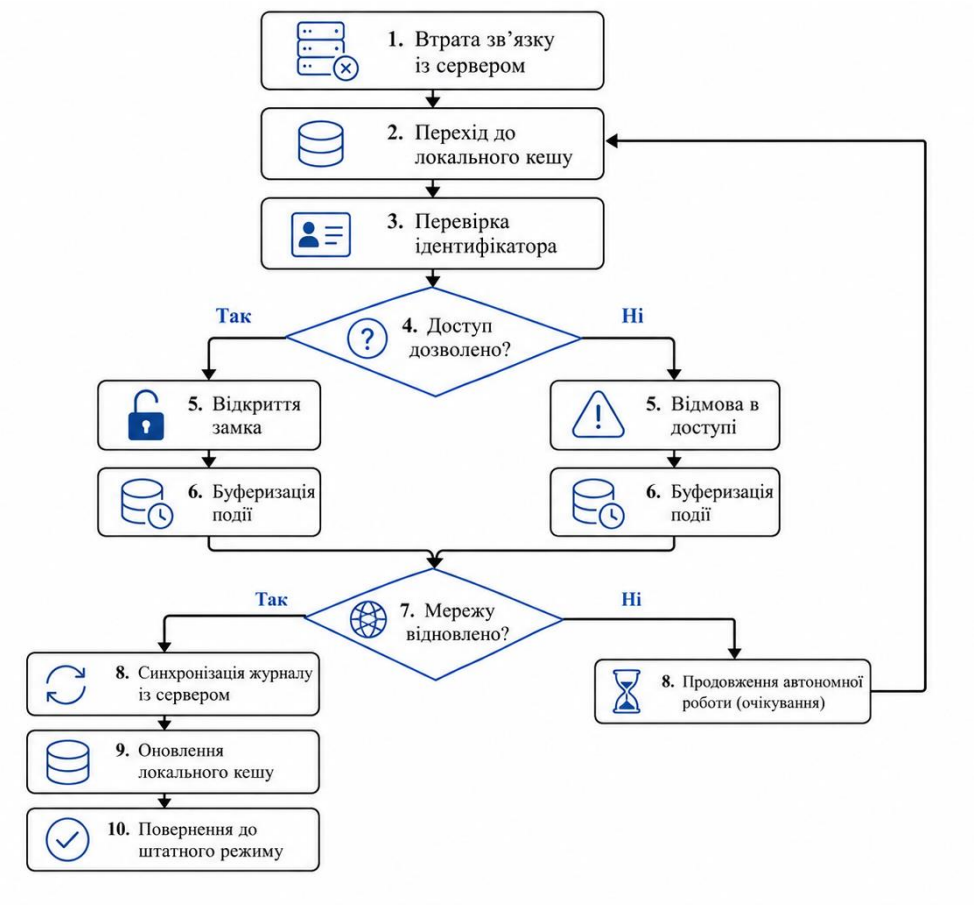


Рисунок 2.4 — Алгоритм автономного режиму роботи дверного контролера

Аварійний алгоритм повинен враховувати втрату основного живлення, некоректний стан дверей, відмову зчитувача, зависання мікроконтролера та тривале незачинення дверей. Вибір режиму залежить від функціонального призначення приміщення та вимог безпечної експлуатації.

Алгоритм адміністрування користувачів реалізується на серверній частині. Для забезпечення цілісності синхронізації список може мати номер версії, дату оновлення й контрольну суму.

2.4 Розроблення ПЗ мікроконтролера та серверної частини

Програмне забезпечення системи складається з двох основних частин: вбудованої програми дверного контролера та серверного програмного забезпечення. Вбудоване програмне забезпечення відповідає за взаємодію з апаратними компонентами й первинне прийняття рішень, а серверна частина

забезпечує централізовану логіку, збереження даних, адміністрування та інтеграцію з іншими сервісами.

Програма мікроконтролера має модульну структуру. Модуль журналювання формує події та передає їх до мережевого модуля або записує в локальний буфер при втраті зв’язку.

ESP-IDF дає змогу реалізувати задачі вбудованого програмного забезпечення з використанням мережевих бібліотек, системних таймерів, файлового сховища та механізмів захисту платформи [8], [9]. Локальні дані, зокрема кеш дозволених ідентифікаторів і черга подій, повинні зберігатися у структурованому вигляді з контролем версії.

Серверна частина виконує функції обліку користувачів, збереження ідентифікаторів, формування правил доступу, приймання подій, моніторингу контролерів і надання адміністративного інтерфейсу. Вебінтерфейс адміністратора взаємодіє із сервером через REST API, а події від контролерів можуть надходити через MQTT або HTTP-запити.

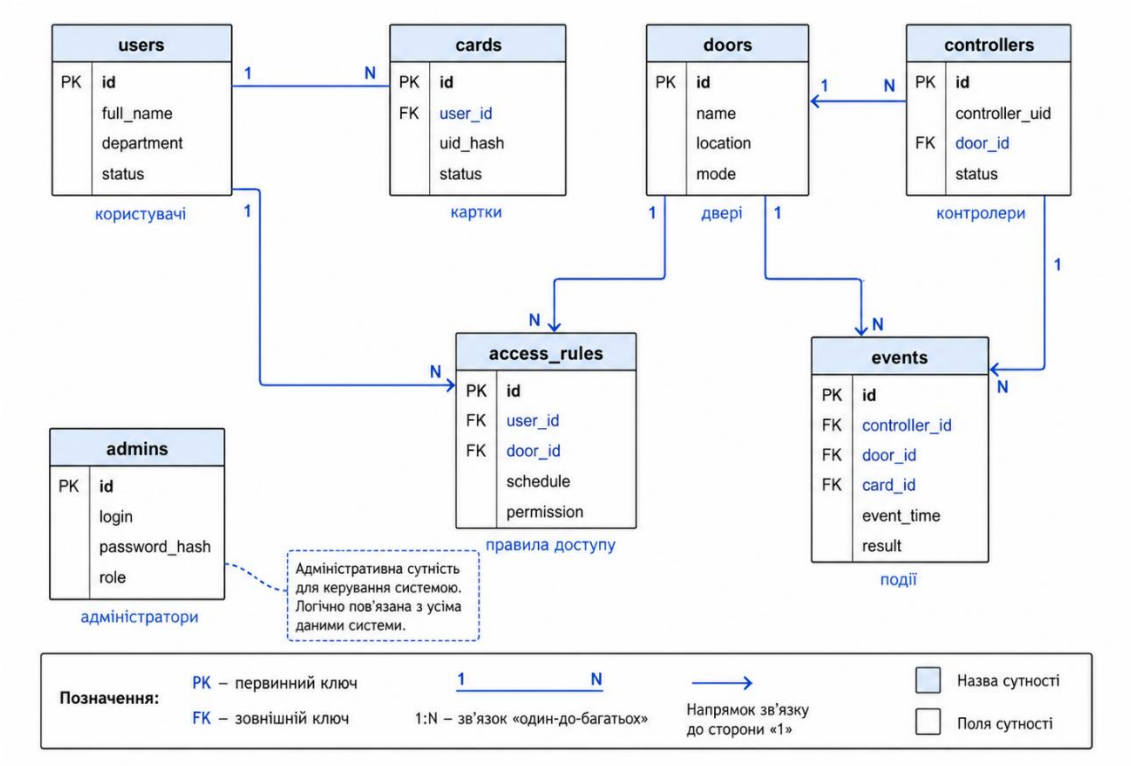


Рисунок 2.5 — ER-діаграма бази даних системи керування доступом

Таблиця 2.3 — Основні таблиці бази даних та їх призначення

Таблиця	**Призначення**	**Основні поля**
users	Зберігання користувачів системи	id, full_name, department, status
cards	Облік RFID/NFC-ідентифікаторів	id, uid_hash, user_id, status
doors	Опис контрольованих точок доступу	id, name, location, mode
controllers	Облік мікроконтролерних вузлів	id, device_key, ip_address, status
access_rules	Правила доступу користувачів	id, user_id, door_id, schedule, permission
events	Журнал подій доступу	id, controller_id, card_id, door_id, time, result
admins	Облікові записи адміністраторів	id, login, password_hash, role

Структура бази даних має забезпечувати зв’язок між користувачем, карткою, дверима та подією.

Таблиця 2.4 — Формат повідомлення про спробу доступу

Поле	**Тип**	**Призначення**
event_id	string	Унікальний ідентифікатор події
controller_id	string	Ідентифікатор дверного контролера
door_id	string	Ідентифікатор дверей
card_uid_hash	string	Хеш ідентифікатора картки
timestamp	string	Час події
event_type	string	Тип події: access_request, door_open, error
result	string	Результат: granted, denied, offline
reason	string	Причина рішення або код помилки
signature	string	Контроль автентичності повідомлення

Приклад логічної структури повідомлення може мати вигляд:

```
{
  "event_id": "ev-2026-000145",
  "controller_id": "ctrl-door-01",
  "door_id": "office-main",
  "card_uid_hash": "9f2a4c...",
  "timestamp": "2026-06-07T10:25:18Z",
  "event_type": "access_request",
  "result": "granted",
  "reason": "valid_rule",
  "signature": "hmac-value"
}
```

Захист програмної частини має враховувати типові загрози для API та вебзастосунків. Для авторизації адміністративних запитів або сервісних операцій можуть застосовуватися JWT або API-ключі контролерів [19].

2.5 Проєктування міжмережевої інтеграції та інформаційного обміну

Міжмережева інтеграція визначає спосіб взаємодії дверних контролерів із серверною частиною, адміністративним інтерфейсом і, за потреби, зовнішніми інформаційними сервісами. Для системи керування доступом важливо забезпечити не лише передавання подій, а й синхронізацію правил доступу, контроль стану контролерів, підтвердження отримання даних, захист каналу та відновлення після збоїв.

У запропонованій архітектурі дверні контролери підключаються до локальної мережі через Wi-Fi. Вебінтерфейс адміністратора звертається до серверної частини через HTTPS, а моніторинг подій у реальному часі реалізується через WebSocket.

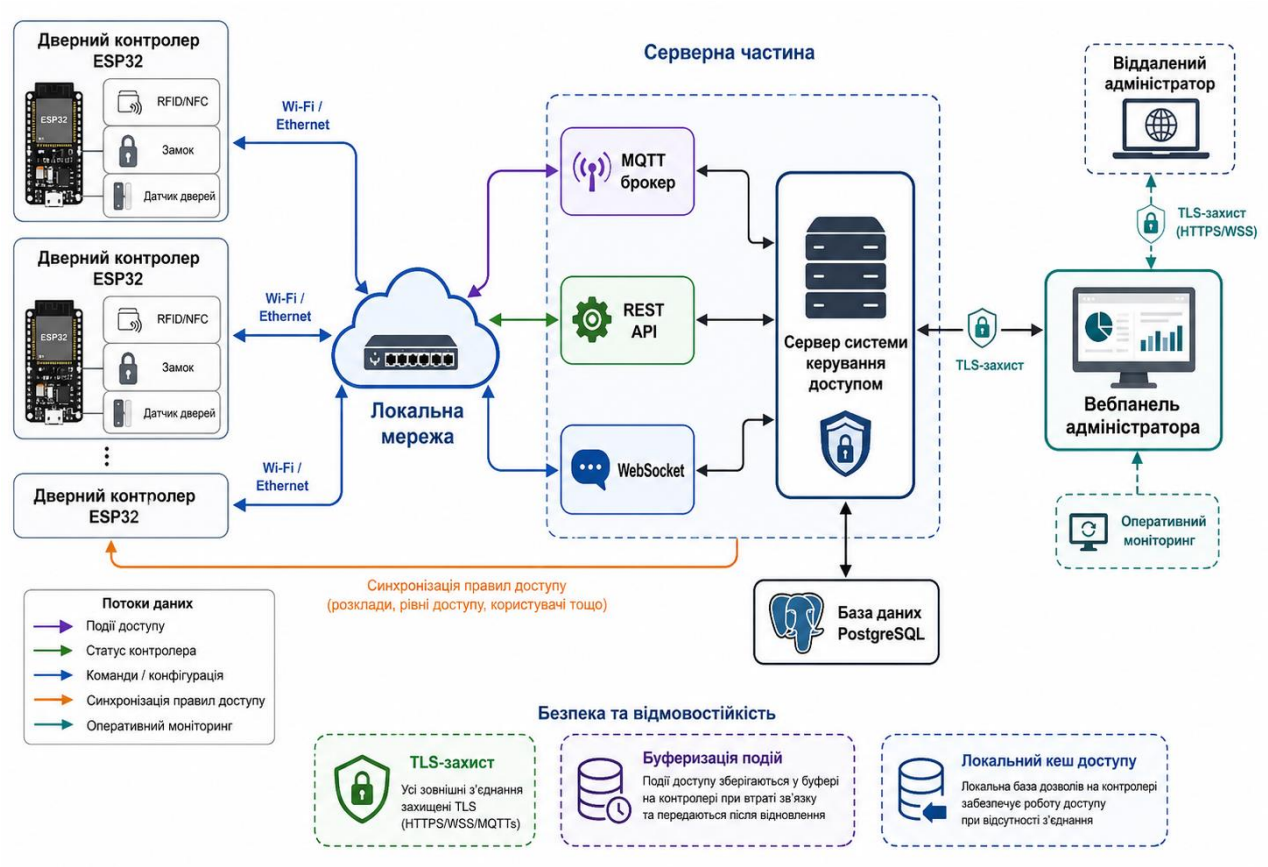


Рисунок 2.6 — Схема міжмережевої інтеграції системи керування доступом

MQTT доцільно використовувати для подій, які генерує контролер: спроба доступу, відкриття дверей, тривале незачинення, втрата зв'язку, перехід в автономний режим, відновлення з'єднання. Модель publish/subscribe зменшує зв'язаність між вузлами й дає змогу підключати додаткові модулі моніторингу без зміни прошивки контролера [12].

HTTP/REST API доцільно застосовувати для операцій, які ініціює адміністратор: створення користувача, додавання картки, зміна прав доступу, блокування ідентифікатора, перегляд журналу та формування звітів. Для захисту адміністративної взаємодії всі запити мають виконуватися через HTTPS, а доступ до методів повинен залежати від ролі адміністратора.

WebSocket використовується для задач, де потрібне оперативне відображення змін без постійного опитування сервера.

Таблиця 2.5 — Порівняння протоколів MQTT, HTTP/REST API та WebSocket

Критерій	**MQTT**	**HTTP/REST API**	**WebSocket**
Основне призначення	Подієвий обмін IoT-вузлів	Адміністративні операції	Моніторинг у реальному часі
Модель взаємодії	Publish/subscribe	Запит/відповідь	Постійний двосторонній канал
Доцільний відправник	Контролер або сервер	Вебінтерфейс або сервер	Сервер і клієнт
Приклад використання	Подія доступу	Створення користувача	Онлайн-журнал подій
Перевага	Легкість і асинхронність	Простота інтеграції	Швидке оновлення стану
Обмеження	Потребує брокера	Не оптимальний для потокових подій	Потребує постійного з’єднання

Для забезпечення достовірності обміну кожне повідомлення контролера має містити часову мітку, унікальний номер події та контроль автентичності. Передавання службових ключів у відкритому вигляді є неприпустимим; для захисту каналу потрібно використовувати TLS [18]. Синхронізація локального списку доступу виконується за версіями. У разі втрати зв’язку контролер не повинен видаляти події або припиняти виконання базових функцій. Якщо буфер заповнюється, система повинна або перезаписувати найменш критичні службові події, або переходити в режим попередження, зберігаючи насамперед спроби доступу, відмови та аварійні повідомлення. Розмежування локального та віддаленого доступу адміністратора також є важливою частиною міжмережевої інтеграції. Вимоги до безпеки IoT-пристроїв і API передбачають автентифікацію, контроль доступу, безпечне оновлення, журналювання та обмеження службових інтерфейсів [20], [22], [23].

Таким чином, міжмережева інтеграція проєктованої системи базується на поєднанні MQTT, HTTP/REST API, WebSocket, JSON, TLS і серверної бази даних. MQTT забезпечує подієвий обмін між контролерами та сервером, REST API — адміністрування, WebSocket — оперативний моніторинг, TLS — захист каналу, а локальна буферизація і синхронізація версій — стійкість до тимчасових мережевих збоїв.

2.6 Висновок до другого розділу

У другому розділі розроблено проєктну структуру автоматизованої системи керування доступом до офісних приміщень. Обґрунтовано вибір RFID/NFC-зчитувача, електрозамка, силового ключа, датчика стану дверей, кнопки виходу, індикації та резервного живлення.

Також розроблено алгоритми штатного доступу, відмови, автономної роботи, аварійного режиму й адміністрування користувачів. Запропоновані рішення створюють технічну основу для подальшої спеціальної частини, у якій буде розглянуто макетування, тестування, кібербезпеку, надійність і експлуатаційну придатність системи.

3 СПЕЦІАЛЬНА ЧАСТИНА

Спеціальна частина роботи спрямована на перевірку практичної придатності запропонованої автоматизованої системи керування доступом. Якщо в проєктній частині було визначено архітектуру, апаратну структуру, алгоритми та засоби міжмережевої інтеграції, то в цьому розділі розглядаються питання макетної реалізації, тестування, кібербезпеки, надійності, економічної доцільності та безпечної експлуатації.

Розроблена система повинна бути оцінена не лише за фактом відкривання дверей після зчитування ідентифікатора. Саме тому спеціальна частина поєднує технічну перевірку макета, аналіз інформаційної безпеки, оцінку відмовостійкості та вимоги до безпечного використання системи.

3.1 Розроблення та опис експериментального макета системи

Експериментальний макет системи керування доступом призначений для перевірки основних функцій, закладених у проєктній частині: зчитування RFID/NFC-ідентифікатора, перевірка прав доступу, керування замком або його імітатором, реєстрація подій, передавання даних на сервер і робота в автономному режимі. Макет є мінімальним працездатним варіантом системи, який може бути розширений до багатодверної конфігурації шляхом додавання нових контролерів.

Основним апаратним вузлом макета є дверний контролер на базі ESP32. RFID/NFC-зчитувач MFRC522 застосовується для отримання ідентифікатора картки через SPI-інтерфейс [6].

Серверна частина макета розгортається на локальному комп’ютері або одноплатному сервері в межах офісної мережі. Події від контролера передаються у форматі JSON, а для подієвого обміну може застосовуватися MQTT [12], [17].

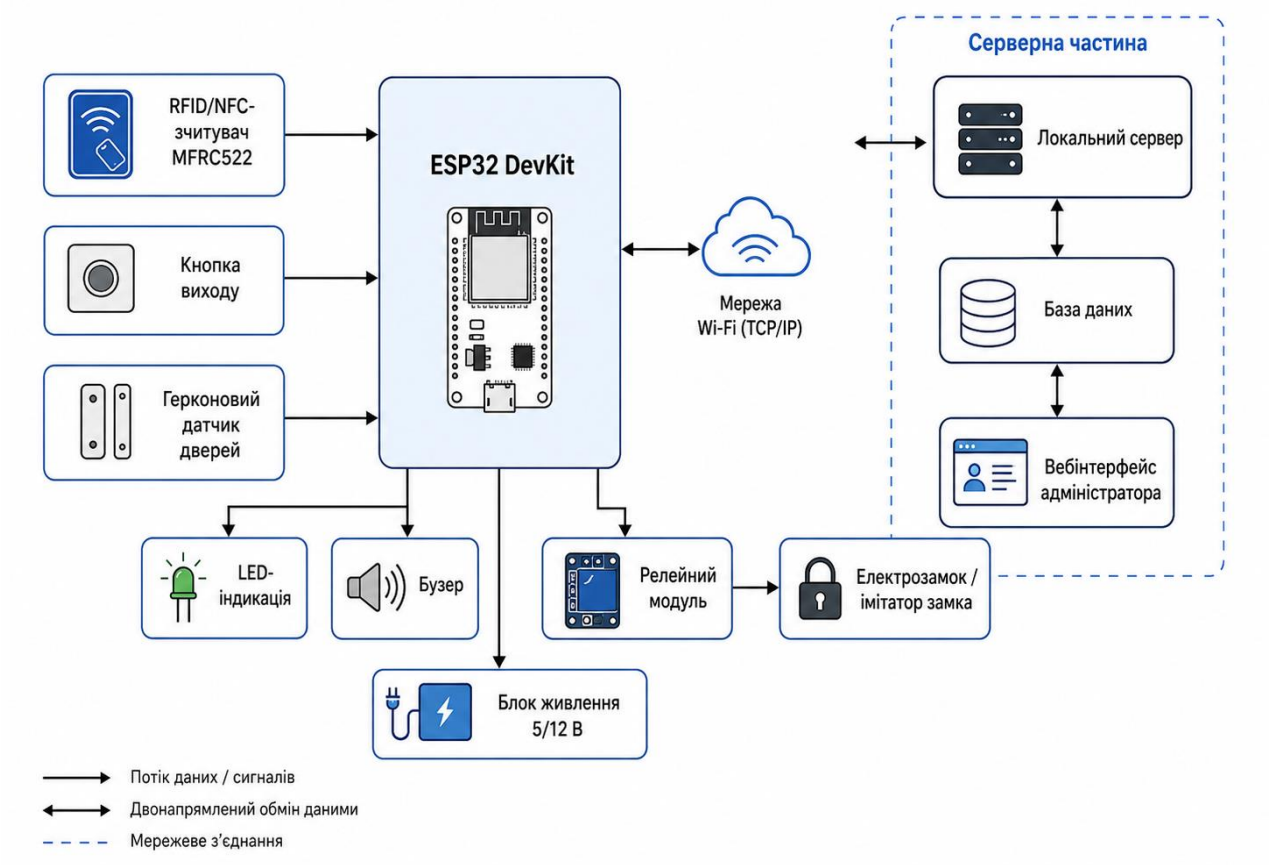


Рисунок 3.1 — Склад експериментального макета системи керування доступом

Таблиця 3.1 — Перелік компонентів експериментального стенда

Компонент	**Призначення в макеті**
ESP32 DevKit	Центральний мікроконтролерний вузол дверного контролера
MFRC522	Зчитування RFID/NFC-ідентифікаторів
Релейний модуль або MOSFET-ключ	Керування електрозамком або його імітатором
Електрозамок або імітатор навантаження	Перевірка керування виконавчим пристроєм
Герконовий датчик	Контроль стану дверей
Кнопка виходу	Локальне відкривання з внутрішнього боку
Світлодіоди та бузер	Індикація дозволу, відмови й аварійних станів
Блок живлення	Живлення логічної та силової частин
Локальний сервер	Оброблення подій, API, вебінтерфейс
PostgreSQL	Збереження користувачів, правил і журналу подій

Програмна структура макета поділяється на кілька модулів. На сервері реалізуються модулі обліку користувачів, керування правилами доступу, приймання повідомлень, перегляду журналу та контролю стану контролерів.

Макет дозволяє перевірити типові сценарії використання: вхід працівника за дозволеною карткою, відмова невідомому ідентифікатору, відкриття дверей кнопкою виходу, блокування втраченої картки, робота при недоступному сервері та синхронізація подій після відновлення мережі. Отже, макет підтверджує, що розроблене рішення не є лише теоретичною моделлю, а може бути реалізоване як функціональний прототип офісної системи доступу.

3.2 Методика тестування та перевірка працездатності системи

Тестування системи має підтвердити відповідність розробленого макета функціональним і нефункціональним вимогам. Методика перевірки охоплює функціональні, мережеві, аварійні та адміністративні сценарії. Для кожного тесту визначається початкова умова, очікуваний результат, фактичний результат і висновок про працездатність.

Функціональне тестування перевіряє базові операції доступу: зчитування картки, прийняття рішення, активацію замка, індикацію, запис події та відкривання кнопкою виходу. Адміністративні тести підтверджують можливість додавання, блокування й редагування користувачів через вебінтерфейс.

Таблиця 3.2 — Результати функціонального тестування системи

№	Умова тестування	Очікуваний результат	Фактичний результат	Висновок
1	Прикладено дозволену картку	Замок активується, подія записується	Відповідає очікуваному	Пройдено
2	Прикладено невідому картку	Доступ заборонено, подія записується	Відповідає очікуваному	Пройдено
3	Картку заблоковано адміністратором	Доступ заборонено	Відповідає очікуваному	Пройдено

№	Умова тестування	Очікуваний результат	Фактичний результат	Висновок
4	Натиснуто кнопку виходу	Замок активується з внутрішнього боку	Відповідає очікуваному	Пройдено
5	Двері залишено відчиненими	Формується попередження	Відповідає очікуваному	Пройдено
6	Змінено права користувача	Нові права застосовуються після синхронізації	Відповідає очікуваному	Пройдено

Під час функціональної перевірки особливу увагу потрібно приділяти коректності журналювання.

Таблиця 3.3 — Результати перевірки мережевих та аварійних режимів

№	Сценарій	Очікуваний результат	Висновок
1	Втрата зв’язку із сервером	Перехід до локальної перевірки за кешем	Працездатність збережено
2	Відновлення мережі	Передавання накопичених подій	Синхронізація виконана
3	Недоступність MQTT-брокера	Повторні спроби підключення, буферизація	Критичної відмови немає
4	Некоректне зчитування картки	Відмова без активації замка	Безпечна реакція
5	Серія невдалих спроб	Формування попередження	Подію зафіксовано
6	Втрата живлення	Перехід до режиму, визначеного типом замка	Потребує резервного живлення

Результати тестування показують, що система зберігає базову працездатність при типових збоях. Вимоги до безпеки API та IoT-пристроїв передбачають, що тестування повинно охоплювати не лише функції, а й авторизацію, обмеження доступу, журналювання службових операцій та захищене оновлення [20], [21], [22], [23].

3.3 Аналіз інформаційної та кібербезпеки системи

Система керування доступом поєднує фізичну безпеку приміщення та інформаційну безпеку мережевої інфраструктури. Компрометація такої системи може призвести не лише до втрати даних, а й до несанкціонованого фізичного доступу. Тому захист має реалізовуватися на кількох рівнях: апаратному, програмному, мережевому, організаційному та експлуатаційному.

Основними загрозами є використання втраченої картки, копіювання ідентифікатора, несанкціонований доступ до вебінтерфейсу адміністратора, перехоплення мережевого трафіку, повторна передача раніше перехопленого повідомлення, підміна контролера, несанкціонована зміна бази даних, відмова в обслуговуванні та фізичний доступ до корпусу контролера. У макетній реалізації використання UID картки є допустимим для перевірки логіки, але в реальній системі бажано застосовувати захищеніші картки або додаткові механізми автентифікації.

Таблиця 3.4 — Основні загрози безпеці системи та запропоновані заходи захисту

Загроза	**Потенційний наслідок**	**Захід захисту**
Втрата картки	Доступ сторонньої особи	Оперативне блокування ідентифікатора
Копіювання UID	Обхід перевірки доступу	Захищені картки, хешування, додаткова серверна перевірка
Доступ до вебінтерфейсу	Зміна прав користувачів	Ролі, складні паролі, MFA за потреби
Перехоплення трафіку	Розкриття подій і службових ключів	TLS для мережевого обміну
Replay-атака	Повторення старого повідомлення	Timestamp, nonce, event_id, контроль дублювання
Підміна контролера	Надсилання фальшивих подій	API-ключ або сертифікат контролера
Зміна бази даних	Викривлення правил доступу	Ролі БД, аудит, резервне копіювання
DoS-атака	Недоступність серверної частини	Локальний кеш і автономний режим
Доступ до корпусу	Підключення до ліній керування	Захищений корпус, тампер-контакт

Для захисту адміністративної частини необхідно реалізувати автентифікацію адміністратора, розмежування ролей, перевірку авторизації для кожної операції, журналювання змін і обмеження доступу до критичних методів API. Тому серверна частина має перевіряти не лише факт входу адміністратора, а й право виконувати конкретну дію: створювати користувача, змінювати правила, блокувати картку або переглядати журнал.

Захист мережевого обміну повинен базуватися на TLS, що забезпечує шифрування каналу та знижує ризик перехоплення даних [18]. Сервер має відхиляти дублікати, події з некоректним часом і повідомлення від невідомих пристроїв.

Для IoT-пристроїв важливими є унікальна ідентифікація пристрою, захист конфігурації, безпечне оновлення прошивки, обмеження сервісних інтерфейсів і контроль життєвого циклу пристрою [22], [23]. Організаційний рівень безпеки включає регламент видачі карток, порядок блокування втрачених ідентифікаторів, резервне копіювання бази даних, обмеження доступу до сервера та періодичний перегляд журналів [24], [28].

Отже, безпека системи не може забезпечуватися одним окремим механізмом. Захищеність досягається поєднанням криптографічного захисту каналу, автентифікації пристроїв, контролю ролей, журналювання, фізичного захисту контролера, резервного копіювання та організаційних правил експлуатації.

3.4 Оцінка надійності та експлуатаційної придатності

Надійність системи керування доступом визначається її здатністю зберігати контрольований стан при відмовах окремих компонентів. Для офісної системи критично важливо, щоб збій мережі, сервера або зчитувача не створював неконтрольованого доступу та не блокував евакуаційні можливості. Тому система повинна мати передбачені реакції на типові несправності.

Таблиця 3.5 — Аналіз відмов системи та способи їх усунення

Відмова	**Можливий наслідок**	**Спосіб виявлення**	**Реакція системи**	**Відновлення**
Відмова зчитувача	Неможливість входу за карткою	Немає відповіді RFID-модуля	Повідомлення про помилку	Заміна або перевірка підключення
Відмова ESP32	Зупинка контролера	Відсутність heartbeat	Перехід до регламентної процедури	Перезапуск, заміна контролера
Втрата мережі	Немає зв’язку із сервером	Тайм-аут з’єднання	Локальний кеш, буфер подій	Автосинхронізація після відновлення
Відмова сервера	Немає централізованої перевірки	Недоступність API/MQTT	Автономний режим	Відновлення сервера з резервної копії
Втрата живлення	Зупинка вузла або зміна стану замка	Контроль напруги	Резервне живлення або fail-режим	Відновлення живлення
Зависання ПЗ	Некоректна реакція контролера	Watchdog-таймер	Автоперезапуск	Аналіз логів і оновлення прошивки
Двері не зачинено	Порушення режиму доступу	Герконовий датчик	Попередження адміністратору	Перевірка дверей і замка
Переповнення буфера	Втрата частини подій	Контроль заповнення пам’яті	Пріоритезація критичних подій	Передавання після відновлення мережі
Пошкодження БД	Втрата журналу або правил	Помилки запитів	Блокування змін, сповіщення	Відновлення з резервної копії

Особливе значення мають режими fail-safe і fail-secure. Вибір режиму повинен виконуватися для кожних дверей окремо з урахуванням функції приміщення, маршруту евакуації та вимог електробезпеки [26], [27].

Експлуатаційна придатність системи залежить від можливості технічного обслуговування. Для IoT-пристроїв також важливо враховувати життєвий цикл пристрою, оновлення безпеки та контроль конфігурації [22], [23].

З позиції управління ризиками система повинна не лише виявляти відмову, а й переходити до передбаченого безпечного стану. Такий підхід відповідає загальній логіці ризик-орієнтованого керування, за якої для кожної загрози визначаються ймовірність, наслідок, спосіб виявлення та захід реагування [28].

3.5 Техніко-економічне обґрунтування та експлуатація системи

Техніко-економічна доцільність запропонованої системи полягає в тому, що її можна реалізувати на доступній мікроконтролерній платформі з використанням недорогих периферійних модулів і локального сервера. Такий підхід є особливо придатним для невеликих офісів, навчальних лабораторій або адміністративних приміщень, де потрібне журналювання доступу, але немає потреби у дорогій промисловій системі з надлишковим функціоналом.

Основними статтями витрат є дверний контролер, RFID/NFC-зчитувач, виконавчий замок, блок живлення, корпус, монтажні матеріали, серверна частина та програмна реалізація.

Таблиця 3.6 — Орієнтовна вартість компонентів системи

Компонент	**Кількість**	**Орієнтовна частка в бюджеті одного вузла**
ESP32 DevKit	1	10–15 %
RFID/NFC-зчитувач	1	3–7 %
Реле або MOSFET-модуль	1	3–5 %
Електрозамок	1	30–45 %
Датчик дверей і кнопка виходу	1 комплект	5–8 %
Індикація та бузер	1 комплект	2–4 %
Блок живлення та захист	1 комплект	15–20 %
Корпус і монтажні матеріали	1 комплект	10–15 %
Серверна частина	1	залежить від наявної інфраструктури

Порівняно з готовими комерційними системами, власна мікроконтролерна розробка має переваги у гнучкості логіки, відкритості структури даних, можливості модифікації алгоритмів і зниженні вартості навчального або маломасштабного впровадження. Тому запропоноване рішення доцільно розглядати як прототип або основу для малих об’єктів, а не як заміну сертифікованим промисловим системам для об’єктів із високими вимогами безпеки.

Безпечна експлуатація системи передбачає дотримання вимог електробезпеки, правильне розділення логічних і силових кіл, використання захисту від короткого замикання, якісне прокладання кабелів, надійне кріплення корпусів і недопущення відкритого доступу до силових контактів. Блок живлення повинен мати захист від перевантаження, а монтаж має виконуватися з урахуванням вимог до електронного та інформаційно-комунікаційного обладнання [26], [27].

Таблиця 3.7 — Заходи безпечної експлуатації системи

Напрям	**Захід**
Електробезпека	Розділення логічного та силового живлення, ізоляція контактів
Захист силового кола	Запобіжник, діод захисту, правильний вибір реле або MOSFET
Пожежна безпека	Використання справного блока живлення та негорючого корпусу
Монтаж	Захищене прокладання кабелів, маркування ліній, фіксація з’єднань
Обслуговування	Перевірка живлення, замка, датчика дверей і резервного акумулятора
Інформаційна безпека	Контроль облікових записів, резервне копіювання, аудит подій
Аварійні дії	Регламент дій при втраті живлення, мережі або відмові контролера

Під час експлуатації персонал повинен знати порядок дій у разі аварійної ситуації: втрати живлення, відмови контролера, заблокованих дверей, помилкового спрацювання або втрати картки.

Таким чином, запропонована система є економічно доцільною для малих і середніх офісних об’єктів за умови правильного монтажу, захисту мережевого обміну, регламентного обслуговування та врахування режимів безпечної роботи. Її перевагою є поєднання локальної автономності, серверного адміністрування, журналювання та можливості подальшої модернізації.

3.6 Висновок до третього розділу

У третьому розділі розглянуто практичну реалізацію експериментального макета автоматизованої системи керування доступом.

Також виконано аналіз інформаційної безпеки, надійності, відмовостійкості та безпечної експлуатації системи. Отримані результати підтверджують практичну придатність запропонованого рішення як прототипу системи керування доступом із можливістю подальшого масштабування та модернізації.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Питання щодо охорони праці

Під час розроблення та експлуатації автоматизованої системи керування доступом до офісних приміщень необхідно враховувати вимоги охорони праці, оскільки система поєднує електронні компоненти, джерела живлення, виконавчі пристрої, мережеве обладнання та програмно-апаратні засоби адміністрування. Основною метою дотримання вимог охорони праці є забезпечення безпечних умов для персоналу, який виконує монтаж, налаштування, обслуговування та використання системи.

У процесі експлуатації системи керування доступом основними потенційно небезпечними чинниками є ураження електричним струмом, коротке замикання, перегрівання блока живлення, пошкодження ізоляції провідників, неправильне підключення електрозамка, механічне травмування під час монтажу обладнання, а також помилки під час технічного обслуговування. Особливу увагу потрібно приділяти розділенню логічної та силової частин системи. Логічна частина, до якої належать мікроконтролер ESP32, RFID/NFC-зчитувач, датчики, світлодіодна індикація та бузер, повинна працювати на безпечних низьких напругах. Силова частина, яка забезпечує живлення електрозамка, має бути підключена через релейний модуль або MOSFET-ключ із відповідним захистом.

Блок живлення системи повинен відповідати навантаженню, яке створюють мікроконтролер, периферійні пристрої та електрозамок. Не допускається використання пошкоджених адаптерів, неізольованих з’єднань, тимчасових скруток або відкритих контактів. Провідники мають бути підібрані за струмовим навантаженням, а місця з’єднань — надійно закріплені та ізольовані. Для запобігання пошкодженню обладнання і виникненню аварійних ситуацій доцільно передбачити захист від короткого замикання, перевантаження та переполюсування. Якщо електрозамок працює від окремого

джерела живлення 12 В, його силове коло не повинно безпосередньо навантажувати виходи мікроконтролера.

Монтаж компонентів системи потрібно виконувати лише за знеструмленого обладнання. Перед початком робіт необхідно перевірити відсутність напруги на ділянках, з якими працює виконавець, справність інструменту та цілісність ізоляції кабелів. Під час монтажу зчитувачів, кнопок виходу, датчиків стану дверей і електрозамків слід уникати прокладання кабелів у місцях, де вони можуть бути пошкоджені дверними полотнами, меблями або іншими рухомими елементами. Кабельні лінії доцільно прокладати у кабель-каналах або захисних коробах, що зменшує ризик механічного пошкодження й покращує загальну безпеку експлуатації.

Робоче місце адміністратора системи також повинно відповідати вимогам безпечної організації праці. Персональний комп’ютер або ноутбук, з якого здійснюється адміністрування системи, має бути підключений до справної електромережі, а робоче місце повинно мати достатнє освітлення, зручне розміщення монітора, клавіатури та миші. Тривала робота з вебінтерфейсом адміністратора потребує дотримання режиму праці та відпочинку, оскільки навантаження на зір і опорно-руховий апарат може негативно впливати на працездатність користувача.

Під час експлуатації системи потрібно проводити періодичний огляд її основних компонентів. До таких робіт належать перевірка справності блока живлення, стану електрозамка, надійності кріплення зчитувача, працездатності кнопки виходу, датчика стану дверей, світлової та звукової індикації. Також необхідно контролювати стан резервного живлення, якщо воно передбачене проєктом. Акумуляторні батареї не повинні мати ознак здуття, перегрівання, витоку електроліту або механічних пошкоджень.

Окрему увагу слід приділяти організаційним заходам безпеки. Доступ до електронних компонентів, блока живлення, серверної частини та адміністративного інтерфейсу повинен мати лише уповноважений персонал. Не допускається самовільна зміна схеми підключення, заміна компонентів без перевірки їхніх параметрів, вимкнення захисних елементів або використання

обладнання з ознаками несправності. У разі виявлення нестабільної роботи системи, перегрівання, запаху гару, іскріння або некоректного спрацювання електрозамка експлуатацію потрібно припинити до усунення несправності.

Таким чином, дотримання вимог охорони праці під час розроблення, монтажу та експлуатації автоматизованої системи керування доступом передбачає безпечну організацію електроживлення, правильне підключення виконавчих пристроїв, захист силових кіл, безпечне прокладання кабелів, регламентне технічне обслуговування та обмеження доступу до критичних компонентів системи. Виконання цих вимог забезпечує безпечну роботу персоналу та підвищує надійність функціонування системи в умовах офісного середовища.

4.2 Питання щодо безпеки в надзвичайних ситуаціях

Автоматизована система керування доступом до офісних приміщень має не лише забезпечувати санкціонований доступ у штатному режимі, а й коректно працювати або переходити до безпечного стану в умовах надзвичайних ситуацій. До таких ситуацій можуть належати пожежа, задимлення, евакуація персоналу, відмова електроживлення, пошкодження мережевої інфраструктури, аварійне блокування дверей, несправність електрозамка, коротке замикання або несанкціоноване втручання в роботу системи. У таких умовах пріоритетом є збереження життя і здоров’я людей, а вже після цього — збереження майна та контроль доступу до приміщень.

Найважливішою вимогою до системи керування доступом у надзвичайних ситуаціях є забезпечення можливості безпечної евакуації людей. Двері, які розташовані на шляхах евакуації або використовуються як аварійні виходи, не повинні залишатися заблокованими у разі пожежі, втрати живлення або аварійного сигналу. Для таких дверей доцільно використовувати режим fail-safe, за якого замок переходить у розблокований стан при втраті живлення або надходженні аварійної команди. Натомість для приміщень із підвищеними вимогами до захисту, наприклад серверних кімнат або архівів, може

застосовуватися режим fail-secure, за якого двері залишаються заблокованими при збої. Вибір режиму повинен здійснюватися з урахуванням призначення дверей і вимог евакуаційної безпеки.

У разі пожежі або задимлення система доступу не повинна створювати перешкод для виходу людей із приміщення. Якщо система інтегрується з пожежною сигналізацією, вона має отримувати аварійний сигнал і переводити відповідні двері у безпечний режим. Для дверей, що використовуються як евакуаційні, необхідно передбачити можливість ручного аварійного відкривання, незалежного від стану сервера, мережі або програмного забезпечення. Кнопка виходу повинна бути розміщена у доступному місці, мати зрозуміле позначення та забезпечувати швидке відкривання дверей з внутрішнього боку.

Втрата електроживлення є одним із найімовірніших аварійних сценаріїв. У такому випадку система повинна або перейти на резервне живлення, або перевести двері у заздалегідь визначений безпечний стан. Резервне живлення доцільно застосовувати для підтримання роботи мікроконтролера, зчитувача, сервера або комунікаційного обладнання протягом часу, достатнього для коректного завершення операцій, збереження подій і забезпечення контрольованого доступу. Водночас резервне живлення не повинно перешкоджати аварійному відкриванню евакуаційних дверей.

Пошкодження мережевої інфраструктури або втрата зв’язку із сервером не повинні повністю блокувати роботу системи. У таких умовах дверний контролер має переходити в автономний режим, у якому перевірка доступу виконується за локальним кешем дозволених ідентифікаторів. Події доступу при цьому зберігаються у внутрішньому буфері контролера і передаються на сервер після відновлення зв’язку. Такий підхід дозволяє уникнути повної зупинки системи при короткочасних збоях мережі, але водночас потребує обмеження адміністративних змін до моменту синхронізації.

У випадку відмови електрозамка або мікроконтролера персонал повинен діяти за визначеним регламентом. Якщо двері заблоковані й перешкоджають евакуації, необхідно застосувати ручний аварійний механізм відкривання або

інший передбачений спосіб розблокування. Якщо ж збій стосується дверей до приміщень з обмеженим доступом, наприклад серверної, необхідно забезпечити контроль з боку відповідальної особи або охорони до відновлення працездатності системи. Усі аварійні дії мають бути зафіксовані в журналі подій або в окремому експлуатаційному журналі.

Під час надзвичайних ситуацій важливою є також інформаційна безпека. Зловмисник може використати аварійний режим для спроби несанкціонованого доступу, підміни контролера або втручання в серверну частину. Тому система повинна зберігати журнал критичних подій, фіксувати переходи в автономний або аварійний режим, реєструвати відмови зв’язку, спроби доступу заблокованими картками та ручні адміністративні дії. Після завершення аварійної ситуації адміністратор повинен перевірити журнал, стан контролерів, актуальність правил доступу та цілісність бази даних.

Для підвищення готовності до надзвичайних ситуацій необхідно проводити періодичну перевірку аварійних режимів. До таких перевірок належать тестування кнопки виходу, перевірка реакції системи на втрату живлення, контроль працездатності резервного джерела живлення, перевірка переходу в автономний режим при втраті зв’язку із сервером, а також перевірка коректності журналювання аварійних подій. Персонал, відповідальний за експлуатацію системи, повинен знати порядок дій при пожежі, відмові замка, втраті живлення, некоректній роботі контролера та необхідності аварійного розблокування дверей.

Отже, безпека в надзвичайних ситуаціях для автоматизованої системи керування доступом полягає у забезпеченні пріоритету евакуації людей, правильному виборі режимів fail-safe і fail-secure, наявності ручного аварійного відкривання, резервного живлення, автономної роботи контролера, журналювання критичних подій і регламентованих дій персоналу. Такий підхід дозволяє поєднати фізичну безпеку людей, контроль доступу до приміщень і надійність функціонування системи в умовах аварійних впливів.

ВИСНОВКИ

У бакалаврській кваліфікаційній роботі розглянуто задачу розроблення автоматизованої системи керування доступом до офісних приміщень на базі мікроконтролерів та засобів міжмережевої інтеграції. Визначено, що така система повинна забезпечувати не лише відкривання дверей за ідентифікатором, а й перевірку прав доступу, журналювання подій, блокування недійсних карток, автономну роботу при втраті зв’язку та підтримку аварійних режимів.

У першому розділі виконано аналіз сучасних систем контролю та керування доступом. Сформовано функціональні та нефункціональні вимоги до системи, зокрема вимоги до ідентифікації, авторизації, керування замком, журналювання, автономності, захисту мережевого обміну, масштабованості та експлуатаційної надійності.

У другому розділі розроблено проєктну структуру системи. Описано структуру бази даних, формат повідомлень про події доступу та принципи взаємодії між контролером і сервером.

Особливу увагу в роботі приділено засобам міжмережевої інтеграції. Така структура дозволяє поєднати автономність дверного вузла з централізованим контролем і можливістю подальшого масштабування системи.

У третьому розділі розглянуто спеціальні питання реалізації та експлуатації системи. Результати аналізу підтвердили, що система може забезпечувати доступ дозволеним користувачам, відмовляти невідомим або заблокованим ідентифікаторам, зберігати події в журналі, працювати в автономному режимі при втраті зв’язку та синхронізувати дані після відновлення мережі.

Також у роботі проаналізовано інформаційну та кібербезпеку системи. Для зменшення ризиків запропоновано автентифікацію адміністратора, розмежування ролей, API-ключі або токени контролерів, TLS-захист обміну, журналювання адміністративних дій, резервне копіювання бази даних і фізичний захист контролера.

Оцінювання надійності та експлуатаційної придатності показало, що система повинна мати передбачені реакції на відмову зчитувача, мікроконтролера, сервера, мережі, живлення, програмного забезпечення та бази даних. Техніко-економічне обґрунтування засвідчило, що мікроконтролерна система є доцільною для невеликих і середніх офісів, навчальних лабораторій та адміністративних об’єктів, де потрібне гнучке, масштабоване й відносно недороге рішення.

Отже, поставлена мета роботи досягнута. Запропоноване рішення може бути використане як основа для створення навчального або прикладного прототипу, а після доопрацювання апаратного захисту, кібербезпеки та монтажної частини — як основа для впровадження в реальних офісних умовах.

ПЕРЕЛІК ДЖЕРЕЛ

1 International Electrotechnical Commission. (2013). Alarm and electronic security systems — Part 11-1: Electronic access control systems — System and components requirements (IEC 60839-11-1:2013). IEC.

2 International Electrotechnical Commission. (2014). Alarm and electronic security systems — Part 11-2: Electronic access control systems — Application guidelines (IEC 60839-11-2:2014). IEC.

3 International Organization for Standardization, & International Electrotechnical Commission. (2018). Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics (ISO/IEC 14443-1:2018). ISO.

4 International Organization for Standardization, & International Electrotechnical Commission. (2018). Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision (ISO/IEC 14443-3:2018). ISO.

5 International Organization for Standardization, & International Electrotechnical Commission. (2023). Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol 1 (NFCIP-1) (ISO/IEC 18092:2023). ISO.

6 NXP Semiconductors. (2016). MFRC522: Standard performance MIFARE and NTAG frontend (Rev. 3.9) [Data sheet]. NXP Semiconductors.

7 Espressif Systems. (2026). ESP32 Series Datasheet (Version 5.2) [Data sheet]. Espressif Systems.

8 Espressif Systems. (2026). ESP-IDF Programming Guide: Get Started — ESP32, stable version 6.0.1. Espressif Systems.

9 Espressif Systems. (2026). ESP-IDF Programming Guide: Security Guides — ESP32, stable version 6.0.1. Espressif Systems.

10 STMicroelectronics. (2026). STM32F405xx and STM32F407xx datasheet: Arm Cortex-M4 32-bit MCU with FPU [Data sheet]. STMicroelectronics.

11 Arduino. (2026). UNO R3: Technical specifications. Arduino Documentation.

12 OASIS. (2019). MQTT Version 5.0: OASIS Standard. OASIS Open.

13 Eddy, W. (2022). Transmission Control Protocol (TCP) (RFC 9293). RFC Editor. https://doi.org/10.17487/RFC9293

14 Fielding, R., Nottingham, M., & Reschke, J. (2022). HTTP Semantics (RFC 9110). RFC Editor. https://doi.org/10.17487/RFC9110

15 Fielding, R. T. (2000). Architectural styles and the design of network-based software architectures [Doctoral dissertation, University of California, Irvine].

16 Fette, I., & Melnikov, A. (2011). The WebSocket Protocol (RFC 6455). RFC Editor. https://doi.org/10.17487/RFC6455

17 Bray, T. (2017). The JavaScript Object Notation (JSON) Data Interchange Format (RFC 8259). RFC Editor. https://doi.org/10.17487/RFC8259

18 Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). RFC Editor. https://doi.org/10.17487/RFC8446

19 Jones, M., Bradley, J., & Sakimura, N. (2015). JSON Web Token (JWT) (RFC 7519). RFC Editor. https://doi.org/10.17487/RFC7519

20 [20] OWASP Foundation. (2023). OWASP API Security Top 10 — 2023. OWASP Foundation.

21 OWASP Foundation. (2026). OWASP Application Security Verification Standard (ASVS), Version 5.0.0. OWASP Foundation.

22 Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259A

23 Fagan, M., Marron, J., Brady, K., Cuthill, B., Megas, K. N., Herold, R., Lemire, D., & Hoehn, B. (2021). IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (NIST SP 800-213). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-213

24 International Organization for Standardization, & International Electrotechnical Commission. (2022). Information security, cybersecurity and

privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). ISO.

25 PostgreSQL Global Development Group. (2026). PostgreSQL 18.4 Documentation. PostgreSQL Global Development Group.

26 International Electrotechnical Commission. (2023). Audio/video, information and communication technology equipment — Part 1: Safety requirements (IEC 62368-1:2023). IEC.

27 International Electrotechnical Commission. (2017). Low-voltage electrical installations — Part 4-41: Protection for safety — Protection against electric shock (IEC 60364-4-41:2005+A1:2017). IEC.

28 International Organization for Standardization. (2018). Risk management — Guidelines (ISO 31000:2018). ISO.

29 Микитишин А.Г., Митник М.М., Стухляк П.Д. Телекомунікаційні системи та мережі: навчальний посібник для студентів спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» – Тернопіль: ТНТУ ім.Івана Пулюя, 2017 – 384 с

30 Stanko, A., Palka, O., Matiichuk, L., Martsenko, N., & Matsiuk, O. (2021, September). Smart City: A Review of Model Architecture and Technology. In 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT) (Vol. 2, pp. 273–277). IEEE.

31 Duda, O., Mykytyshyn, A., Mytnyk, M., & Stanko, A. Information technology sets formation and" TNTU Smart Campus" services network support. Proceedings of the 3rd International Workshop on ITTAP 2023,Ternopil, Ukraine, Opole, Poland, November 22–24, 2023.

32 Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання / укл.: Стручок В. С. Тернопіль: ФОП Паляниця В. А., 2022. 156 с.

ДОДАТКИ

Додаток А

Фрагмент програмного коду мікроконтролера

```
#include <WiFi.h>
#include <SPI.h>
#include <MFRC522.h>

#define SS_PIN 5
#define RST_PIN 22
#define LOCK_PIN 26
#define DOOR_SENSOR_PIN 34
#define EXIT_BUTTON_PIN 27
#define LED_GREEN 14
#define LED_RED 12
#define BUZZER_PIN 13

MFRC522 rfid(SS_PIN, RST_PIN);

const char* ssid = "office_wifi";
const char* password = "office_password";

String controllerId = "ctrl-door-01";
String doorId = "office-main";

void setup() {
  Serial.begin(115200);

  pinMode(LOCK_PIN, OUTPUT);
  pinMode(DOOR_SENSOR_PIN, INPUT);
  pinMode(EXIT_BUTTON_PIN, INPUT_PULLUP);
  pinMode(LED_GREEN, OUTPUT);
  pinMode(LED_RED, OUTPUT);
  pinMode(BUZZER_PIN, OUTPUT);

  digitalWrite(LOCK_PIN, LOW);
  digitalWrite(LED_GREEN, LOW);
  digitalWrite(LED_RED, LOW);
  digitalWrite(BUZZER_PIN, LOW);

  SPI.begin();
  rfid.PCD_Init();

  WiFi.begin(ssid, password);
}

void loop() {
  if (digitalRead(EXIT_BUTTON_PIN) == LOW) {
    openDoor("exit_button");
    createAccessEvent("button", "granted", "exit_button");
    delay(1000);
  }

  if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial()) {
    return;
  }

  String uid = readCardUid();
```

```
  if (checkAccess(uid)) {
    openDoor(uid);
    createAccessEvent(uid, "granted", "valid_rule");
  } else {
    denyAccess(uid);
    createAccessEvent(uid, "denied", "unknown_or_blocked_card");
  }

  rfid.PICC_HaltA();
}

String readCardUid() {
  String uid = "";
  for (byte i = 0; i < rfid.uid.size; i++) {
    uid += String(rfid.uid.uidByte[i], HEX);
  }
  uid.toUpperCase();
  return uid;
}

bool checkAccess(String uid) {
  // У реальній системі тут виконується запит до сервера
  // або перевірка локального кешу дозволених ідентифікаторів.
  if (uid == "A1B2C3D4") {
    return true;
  }
  return false;
}

void openDoor(String source) {
  digitalWrite(LOCK_PIN, HIGH);
  digitalWrite(LED_GREEN, HIGH);
  tone(BUZZER_PIN, 2000, 150);
  delay(3000);
  digitalWrite(LOCK_PIN, LOW);
  digitalWrite(LED_GREEN, LOW);
}

void denyAccess(String uid) {
  digitalWrite(LED_RED, HIGH);
  tone(BUZZER_PIN, 700, 300);
  delay(1000);
  digitalWrite(LED_RED, LOW);
}

void createAccessEvent(String uid, String result, String reason) {
  Serial.println("{");
  Serial.println("\"controller_id\":\"" + controllerId + "\",");
  Serial.println("\"door_id\":\"" + doorId + "\",");
  Serial.println("\"card_uid\":\"" + uid + "\",");
  Serial.println("\"result\":\"" + result + "\",");
  Serial.println("\"reason\":\"" + reason + "\"");
  Serial.println("}");
}
```

Додаток Б

Приклад JSON- або MQTT-повідомлення про спробу доступу

```
{
  "event_id": "ev-2026-000145",
  "controller_id": "ctrl-door-01",
  "door_id": "office-main",
  "card_uid_hash": "9f2a4c7b91d0a43e8b2f",
  "timestamp": "2026-06-07T10:25:18Z",
  "event_type": "access_request",
  "result": "granted",
  "reason": "valid_rule",
  "network_mode": "online",
  "access_list_version": "v12",
  "signature": "hmac_sha256_value"
}
```

Приклад MQTT-тем для обміну між контролером і сервером:

```
access/controllers/ctrl-door-01/events
access/controllers/ctrl-door-01/status
access/controllers/ctrl-door-01/commands
access/controllers/ctrl-door-01/config
```

Призначення основних тем:

MQTT-тема	**Призначення**
access/controllers/ctrl-door-01/events	Передавання подій доступу від контролера до сервера
access/controllers/ctrl-door-01/status	Передавання стану контролера, версії прошивки та доступності
access/controllers/ctrl-door-01/commands	Отримання команд від сервера
access/controllers/ctrl-door-01/config	Отримання оновлених правил доступу

Додаток В

Структура бази даних системи керування доступом

```
CREATE TABLE users (
    id SERIAL PRIMARY KEY,
    full_name VARCHAR(120) NOT NULL,
    department VARCHAR(80),
    position VARCHAR(80),
    status VARCHAR(20) NOT NULL DEFAULT 'active'
);

CREATE TABLE cards (
    id SERIAL PRIMARY KEY,
    user_id INTEGER REFERENCES users(id),
    uid_hash VARCHAR(128) NOT NULL UNIQUE,
    status VARCHAR(20) NOT NULL DEFAULT 'active',
    issued_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE TABLE doors (
    id SERIAL PRIMARY KEY,
    name VARCHAR(100) NOT NULL,
    location VARCHAR(120),
    mode VARCHAR(30) NOT NULL DEFAULT 'standard'
);

CREATE TABLE controllers (
    id SERIAL PRIMARY KEY,
    controller_uid VARCHAR(80) NOT NULL UNIQUE,
    door_id INTEGER REFERENCES doors(id),
    ip_address VARCHAR(45),
    firmware_version VARCHAR(40),
    status VARCHAR(20) NOT NULL DEFAULT 'offline',
    last_seen TIMESTAMP
);

CREATE TABLE access_rules (
    id SERIAL PRIMARY KEY,
    user_id INTEGER REFERENCES users(id),
    door_id INTEGER REFERENCES doors(id),
    permission VARCHAR(20) NOT NULL DEFAULT 'allow',
    schedule VARCHAR(120),
    valid_from TIMESTAMP,
    valid_to TIMESTAMP
);

CREATE TABLE events (
    id SERIAL PRIMARY KEY,
    event_uid VARCHAR(80) NOT NULL UNIQUE,
    controller_id INTEGER REFERENCES controllers(id),
    door_id INTEGER REFERENCES doors(id),
    card_id INTEGER REFERENCES cards(id),
    event_time TIMESTAMP NOT NULL,
    event_type VARCHAR(40) NOT NULL,
    result VARCHAR(20) NOT NULL,
    reason VARCHAR(120)
);

CREATE TABLE admins (
    id SERIAL PRIMARY KEY,
    login VARCHAR(80) NOT NULL UNIQUE,
    password_hash VARCHAR(255) NOT NULL,
    role VARCHAR(40) NOT NULL DEFAULT 'operator',
    status VARCHAR(20) NOT NULL DEFAULT 'active'
);
```

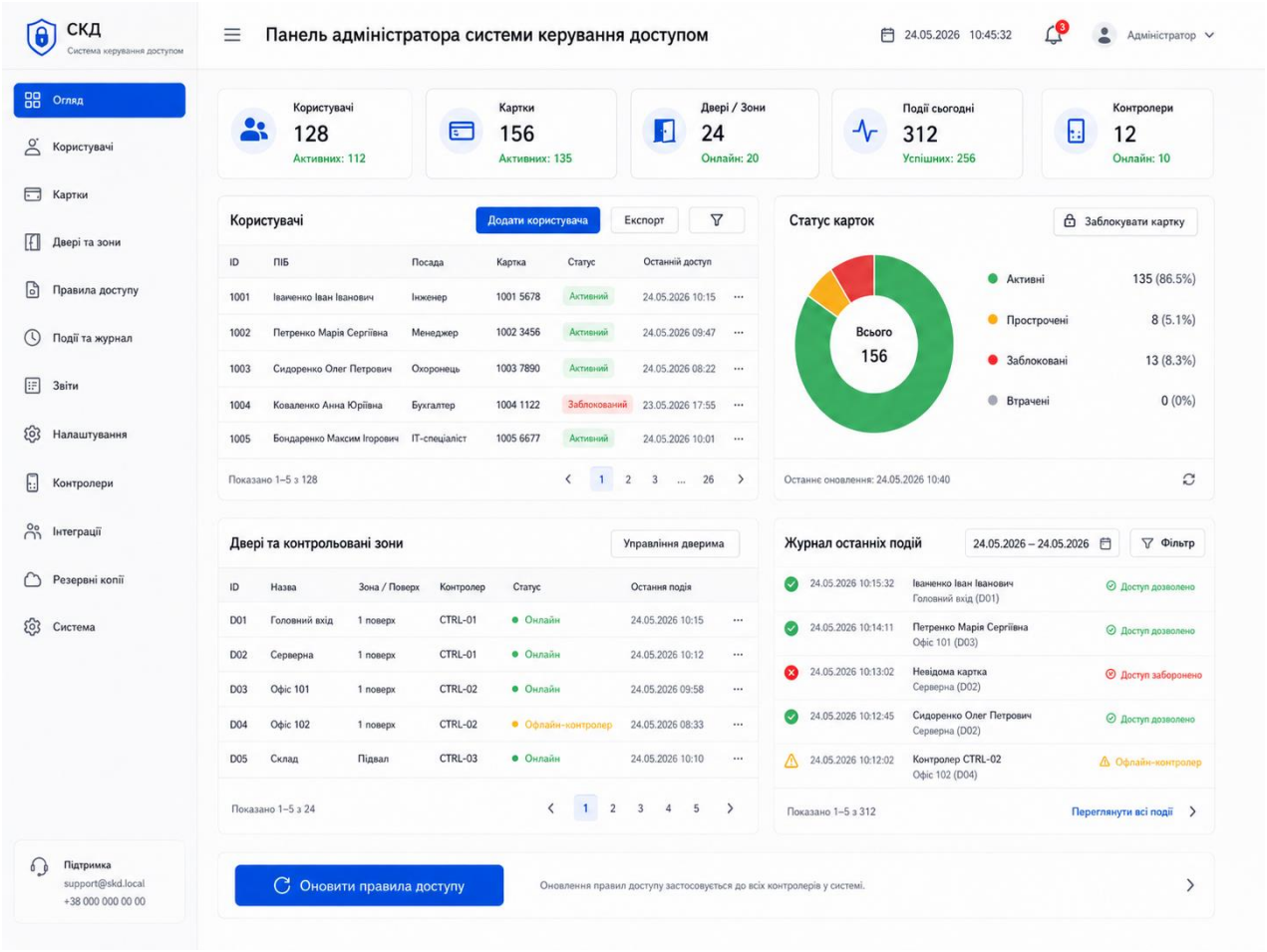
Додаток Г

Перелік тестових сценаріїв системи

№	Сценарій	Початкова умова	Очікуваний результат
1	Доступ дозволеному користувачу	Картка активна, правило доступу чинне	Замок активується, подія записується
2	Доступ невідомій картці	UID відсутній у базі	Доступ заборонено, подія записується
3	Доступ заблокованій картці	Картка має статус blocked	Доступ заборонено
4	Відкривання кнопкою виходу	Натиснуто EXIT_BUTTON	Замок активується з внутрішнього боку
5	Втрата мережі	Сервер недоступний	Контролер переходить до локального кешу
6	Відновлення мережі	У буфері є події	Події синхронізуються із сервером
7	Тривале відчинення дверей	Геркон фіксує відкритий стан	Формується попередження
8	Втрата живлення	Основне живлення відсутнє	Перехід до резервного або fail-режиму
9	Зміна прав користувача	Адміністратор змінює правило	Контролер отримує оновлений список
10	Спроба replay-атаки	Повторено старе повідомлення	Сервер відхиляє дубль події

Додаток Д

Макет вебінтерфейсу адміністратора системи керування доступом



Додаток Е

Схема життєвого циклу події доступу в системі

Додаток Ж

Матриця ролей і прав доступу користувачів

Роль користувача	Вхідна зона	Кабінети	Серверна	Архів	Журнал подій	Керування користувачами
Адміністратор	✓	✓	✓	✓	✓	✓
Працівник	✓	✓	−	−	−	−
Охорона	✓	✓	−	✓	✓	−
Технічний персонал	✓	✓	✓	−	−	−
Відвідувач	✓	−	−	−	−	−

Умовні позначення

✓ **Повний доступ** — Користувач має повні права доступу до ресурсу.

− **Обмежений доступ** — Користувач має обмежені або умовні права доступу.

− **Доступ заборонено** — Користувач не має прав доступу до ресурсу.

Примітка: Матриця відображає типовий розподіл прав доступу в системі контролю доступу. Конкретні налаштування можуть змінюватися відповідно до політик безпеки організації.