НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет робототехніки та приладобудування

Кафедра автоматизації та систем неруйнівного контролю

До захисту допущено:

Завідувач кафедри

_____ Юрій КИРИЧУК

«___»_____20__ р.

Дипломний проєкт

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Комп'ютерно-інтегровані системи та технології в приладобудуванні»

спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології»

на тему: «Автоматизований пристрій контролю доступу до приміщень»

Виконав (-ла):
студент (-ка) IV курсу, групи ПК-21
Верешко Дмитро Михайлович _____

Керівник:
к.т.н. доцент кафедри АСНК
Баженов Віктор Григорович _____

Рецензент:
к.т.н. асистент кафедри КІТВП
Матвієнко Сергій Миколайович _____

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2026 року

ВІДОМІСТЬ ДИПЛОМНОГО ПРОЄКТУ

№ з/п	Формат	Позначення	Найменування	Кількість листів	Примітка
1	А4		Завдання на дипломний проєкт	2	
2	А4	ДПБ.ПК-21.03.1760.00.000 ПЗ	Пояснювальна записка	87	
3	А1	ДПБ.ПК-21.03.1760.00.000 СхЕ	Принципова схема	1	
4	А4	ДПБ.ПК-21.03.1760.00.000 СхС	Структурна схема	1	
5	А4	ДПБ.ПК-21.03.1760.00.000 СхФ	Функціональна схема	1	
6	А4	ДПБ.ПК-21.03.1760.00.000 ПЕ	Перелік елементів	2	
7	А1	ДПБ.ПК-21.03.1760.00.001 БС	Блок схема алгоритму webSocketEvent	1	
8	А1	ДПБ.ПК-21.03.1760.00.002 БС	Блок схема алгоритму loop	1	
9	А4	ДПБ.ПК-21.03.1760.01.000	Специфікація блока входу	1	
10	А1	ДПБ.ПК-21.03.1760.01.000 СК	Складальний кресленик блока входу	1	
11	А3, А4	ДПБ.ПК-21.03.1760.01.001	Корпус блока входу	2	
12	А4	ДПБ.ПК-21.03.1760.01.002	Кришка блока входу	1	
13	А4	ДПБ.ПК-21.03.1760.02.000	Специфікація блока виходу	1	
14	А1	ДПБ.ПК-21.03.1760.02.000 СК	Складальний кресленик блока виходу	1	
15	А3, А4	ДПБ.ПК-21.03.1760.02.001	Корпус блока виходу	2	
16	А4	ДПБ.ПК-21.03.1760.02.002	Кришка блока виходу	1	
17	А1	ДПБ.ПК-21.03.1760.00.000 ПЛ	Плакат	1	

				ДПБ.ПК-21.03.1760.00.000		
	ПІБ	Підп.	Дата			
Розробн.	Верешко Д.М			Відомість дипломного проєкту	Лист	Листів
Керівн.	Баженов В.Г.				1	1
Консульт.					КПІ ім. Ігоря Сікорського Каф. АСНК Гр. ПК-21	
Н/контр.						
Зав.каф.						

Пояснювальна записка
до дипломного проєкту
на тему: «Автоматизований пристрій контролю доступу до приміщень»

Київ – 2026 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет робототехніки та приладобудування
Кафедра автоматизації та систем неруйнівного контролю

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 151 «Автоматизація та комп'ютерно-інтегровані технології»

Освітньо-професійна програма «Комп'ютерно-інтегровані системи та технології в приладобудуванні»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Юрій КИРИЧУК
«___»_____20__ р.

ЗАВДАННЯ
на дипломний проєкт студенту
Верешкові Дмитру Михайловичу

1. Тема проєкту «Автоматизований пристрій контролю доступу до приміщень», керівник проєкту Баженов Віктор Григорович, к.т.н. доц. кафедри АСНК, затверджені наказом по університету від «26» травня 2026 р. №1905с

2. Термін подання студентом проєкту 09.06.2026

3. Вихідні дані до проєкту: напруга живлення системи 12 В, комутація струму замка до 10 А, робоча частота ідентифікації 13,56 МГц, бездротова передача даних по Wi-Fi, наявність веб-інтерфейсу з базою даних, проєктування конструкції корпусних деталей.
4. Зміст пояснювальної записки:

1. Аналіз предметної області та обґрунтування задачі
2. Розробка функціональної схеми та архітектури системи
3. Вибір компонентів та розробка принципової електричної схеми
4. Розробка програмного забезпечення

5. Розробка конструкції та корпусу пристрою
6. Висновки

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо): Складальні кресленики блоків входу та виходу, деталювання, принципова, структурна та функціональна схеми автоматизованого пристрою контролю доступу до приміщень, блок-схеми алгоритмів, плакат, презентація доповіді, 6 форматів А1.

6. Дата видачі завдання 13.03.2026

Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1.	Аналіз предметної області та обґрунтування задачі	З 13.03.26 р. По 27.03.26 р.	Виконано
2.	Розробка функціональної схеми та архітектури системи	З 28.03.26 р. По 10.04.26 р.	Виконано
3.	Вибір компонентів та розробка принципової електричної схеми	З 11.04.26 р. По 25.04.26 р.	Виконано
4.	Розробка програмного забезпечення	З 26.04.26 р. По 15.05.26 р.	Виконано
5.	Розробка конструкції та корпусу пристрою	З 16.05.26 р. По 25.05.26 р.	Виконано
6.	Оформлення пояснювальної записки та написання висновків	З 26.05.26 р. По 03.06.26 р.	Виконано
7.	Перевірка на плагіат, отримання відгуку та рецензії	З 04.06.26 р. По 08.06.26 р.	Виконано
8.	Створення презентації та плакату	З 09.06.26 р. По 12.06.26 р.	Виконано
9.	Захист дипломного проєкту	З 15.06.26 р. По 19.06.26 р.	Заплановано

Студент Дмитро ВЕРЕШКО

Керівник Віктор БАЖЕНОВ

АНОТАЦІЯ

У дипломному проєкті розроблено автоматизований пристрій контролю доступу до приміщень. Основною метою проєкту є підвищення ефективності контролю доступу в офісних і подібних приміщеннях та забезпечення моніторингу статистики відвідувань персоналу. У проєкті обґрунтовано вибір зчитувачів ідентифікаційних карток, датчиків положення дверей, сигналізації та механізмів їхньої взаємодії з мікроконтролером ESP32. Розроблено алгоритми керування запірною системою та збору аналітичних даних. Проведено порівняльний аналіз існуючих ринкових рішень. Результати проєкту мають прикладне значення для впровадження на підприємствах малого та середнього бізнесу.

Ключові слова: система керування та управління доступу (СКУД), автентифікація, мікроконтролер, веб-інтерфейс, веб-застосунок, моніторинг відвідуваності, ESP32, React. Nextjs, Nodejs, SQL.

ABSTRACT

In the thesis project, an automated room access control device was developed. The main goal of the project is to increase the efficiency of access control in office and similar premises and to provide monitoring of staff attendance statistics. The project justifies the choice of ID card readers, door position sensors, alarms, and mechanisms of their interaction with the ESP32 microcontroller. Algorithms for managing the locking system and collecting analytical data were developed. A comparative analysis of existing market solutions was conducted. The results of the project have practical value for implementation in small and medium-sized enterprises.

Keywords: access control system (ACS), authentication, microcontroller, web interface, web application, attendance monitoring, ESP32, React, Next.js, Node.js, SQL. Translated with DeepL.com (free version)

ВСТУП

Впевненість у безпеці підприємства чи офісного приміщення неможлива без сучасних систем контролю доступу. Наразі такі системи перестають бути лише механічними, перетворюючись на інтелектуальні екосистеми, що поєднують у собі складні апаратні рішення, мережеві протоколи та засоби глибокої аналітики даних. Високі вимоги до надійності, масштабованості та оперативності моніторингу стимулюють перехід від закритих систем до гнучких рішень, побудованих на базі відкритих веб-технологій та енергоефективних мікроконтролерів.

Ефективне управління доступом у сучасному корпоративному чи промисловому середовищі вимагає не просто фіксації подій, а створення єдиного інформаційного простору. Це передбачає можливість відстеження переміщень персоналу у реальному часі, автоматизацію процесів авторизації та впровадження інтелектуальних алгоритмів захисту, таких як запобігання повторному проходу або виявлення фізичного втручання. Використання мікроконтролерів у поєднанні з технологією RFID дозволяє створювати розподілені мережі точок доступу, які зберігають працездатність навіть за умов нестабільного мережевого з'єднання, що є критично важливим для систем безпеки.

Актуальність проєкту зумовлена потребою в централізованих системах із високим рівнем захисту даних і фізичного периметра за мінімальних витрат на розгортання та обслуговування. Метою є дослідження принципів функціонування сучасних СКУД, а також проєктування й практична реалізація автоматизованого комплексу на базі мікроконтролера та веб-технологій. У проєкті розглядаються архітектурні рішення для двостороннього зв’язку між пристроями та сервером, алгоритми ідентифікації, логіка безпеки, створення інтерфейсу для моніторингу подій, а також питання відмовостійкості та захисту від несанкціонованого проникнення.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ ЗАДАЧІ

Розширення можливостей інформаційних технологій вимагає модернізації існуючих методів контролю фізичного доступу. Це пов’язано з тим, що інтелектуальні комплекси безпеки інтегруються в інфраструктуру об’єктів різного призначення. Для того щоб спроєктувати по-справжньому ефективну, надійну та конкурентоспроможну систему, яка буде повністю відповідати актуальним запитам користувачів та сучасним стандартам безпеки, необхідно максимально детально розглянути історичні передумови виникнення таких рішень, глибоко проаналізувати наявну апаратну базу, детально розглянути існуючі комерційні рішення, а також визначити ключові програмні та апаратні чинники, які безпосередньо впливають на формування архітектури сучасних засобів безпеки [1].

1.1. Еволюція систем контролю та управління доступом

Система контролю та управління доступом (СКУД) на сучасному етапі розвитку технічних засобів безпеки є третім рубежем захисту об'єкта після систем відеоспостереження та охоронно-пожежної сигналізації. Еволюція цих систем відображає перехід від пасивного фізичного обмеження до активного інтелектуального керування потоками людей та ресурсів [2].

Розвиток систем контролю доступу нерозривно пов’язаний з еволюцією замків та методів ідентифікації, які поступово трансформувалися від примітивних механічних конструкцій до біометричних комплексів. На ранніх етапах безпека трималася виключно на фізичних замках і присутності охорони, що створювало суттєві незручності для роботи підприємства. З розвитком електроніки галузь перейшла на цифрові ідентифікатори, а це вже зовсім інший рівень безпеки й контролю персоналу [3].

Коли в 1970-х з’явилися доступні мікроелектронні компоненти, зокрема TMS1000 від Texas Instruments у 1971 році, процесор і пам’ять вдалося розмістити на одному чипі [4]. Це дало поштовх для активного впровадження кодових панелей і

локальних систем на картках з магнітною смугою, які хоча б частково автоматизували допуск персоналу та дозволили вести базовий облік відвідуваності. Однак магнітні картки мали серйозну вразливість і їх легко копіювали та підробляли за допомогою спеціального обладнання [2].

Справжнім проривом стала технологія радіочастотної ідентифікації RFID, яка забезпечила безконтактне зчитування унікальних ідентифікаторів через електромагнітне поле й відкрила широкі можливості для інтеграції з комп'ютерними мережами [5]. Згідно зі стандартом ISO/IEC 14443 [6], сучасні смарт-картки працюють на частоті 13,56 МГц і використовують складні алгоритми ініціалізації, що дає системі змогу миттєво розпізнавати ключ навіть за наявності кількох карток у полі зчитування. Сьогодні галузь рухається до повної цифровізації, тож ізольовані пристрої минулого масово замінюються комплексами, здатними в реальному часі синхронізувати бази даних, взаємодіяти з хмарними серверами та керуватися віддалено через застосунки з будь якої точки світу. Графічну схему еволюції засобів ідентифікації зображено на рисунку 1.1.

Рисунок 1.1 – Графічна схема еволюції засобів ідентифікації

1.2. Класифікація систем контролю доступу

Відповідно до загальноприйнятих галузевих стандартів, системи контролю та управління доступом прийнято класифікувати за кількома ключовими критеріями, серед яких базовими виступають спосіб управління виконавчими пристроями та загальний масштаб розгорнутої інфраструктури [7]. Залежно від способу управління точками проходу системи поділяються на три основні категорії:

1. Автономні або локальні системи керують одним чи кількома запірними пристроями без передачі даних на центральний пульт і без постійного контролю оператора. Зазвичай це контролер із вбудованою базою ідентифікаторів, що обслуговує зчитувач на вхід та кнопку або датчик руху на вихід. Сучасні моделі можуть накопичувати події у власній пам’яті, що дає змогу періодично знімати ці дані через спеціалізоване програмне забезпечення [7].
2. Централізовані або мережеві системи призначені для комплексного контролю на великих об’єктах і підтримують постійний двосторонній обмін даними з головним сервером, що дає оператору змогу дистанційно керувати всіма пристроями в реальному часі. Такий підхід легко інтегрується з охоронною та пожежною сигналізацією, а також дозволяє налаштувати багаторівневу ідентифікацію для приміщень із підвищеними вимогами безпеки [7].
3. Універсальні системи поєднують можливості обох попередніх типів. У штатному режимі вони працюють під керуванням центрального сервера, а в разі апаратних відмов мережевого обладнання миттєво переходять в автономний режим, зберігаючи цілісність даних і накопичуючи журнали подій до відновлення зв’язку [7].

За кількістю точок проходу та ємністю бази даних користувачів системи поділяють на малі (одиночні двері в невеликих офісах), середні (десятки точок і тисячі співробітників у банках чи готелях) та великі масштабовані платформи для сотень прохідних точок і десятків тисяч користувачів на промислових підприємствах або в

аеропортах [7]. Загальну структурну класифікацію та поділ систем контролю та управління доступом наведено на рисунку 1.2.

Рисунок 1.2 – Структурна класифікація СКУД

1.3. Апаратні рішення та платформи для автоматизації контролю доступу

СКУД це єдиний апаратно-програмний комплекс, де всі компоненти працюють на забезпечення максимальної безпеки [8]. Архітектура такої системи складається з ідентифікаторів, зчитувачів, контролера, виконавчих механізмів так комунікаційних технологій [9]. Розгляньмо кожен із цих елементів окремо.

1.3.1. Контролер системи

Контролер це мозок системи, саме він ухвалює рішення про надання доступу [8]. Автономні контролери зберігають базу локально й підходять для поодиноких дверей [9]. Мережеві дають змогу керувати системою дистанційно та об’єднувати пристрої в єдину сітку [8]. Для веб-орієнтованих комплексів найефективнішими є мікроконтролери з підтримкою бездротових мереж, які беруть на себе керування периферією, тоді як логіка авторизації виноситься на центральний сервер [9].

1.3.2. Зчитувачі та ідентифікатори

Процес надання доступу починається з ідентифікації користувача. Найпоширенішою технологією залишаються безконтактні смарт-картки та брелки стандарту RFID, а для об’єктів із підвищеними вимогами застосовують захищені формати з криптографічним шифруванням [8]. Активно впроваджуються біометричні рішення, такі як сканування відбитків пальців чи обличчя [9]. Популярним є й використання смартфона як електронного ключа через бездротові технології або веб-інтерфейс. Усі зчитувачі встановлюються безпосередньо на точках проходу, зчитують ідентифікатори й передають дані контролеру для обробки [8]. Порівняння усіх типів ідентифікації наведено у табл. 1.1.

1.3.3. Виконавчі пристрої та сенсори

Фізичний рівень безпеки забезпечують виконавчі пристрої, які безпосередньо блокують вхід [8]. До них належать електромагнітні та електромеханічні замки й подібні механізми [9]. Контролер, отримавши дані від зчитувачів, ухвалює рішення про надання дозволу. Важливою складовою є також сенсорна периферія, зокрема датчики положення дверей, які фіксують стан проходу та виявляють несанкціоноване відкриття або утримання дверей у відкритому стані [9].

1.3.4. Комунікаційні технології

Комунікаційні технології забезпечують зв’язок між компонентами, контролером та сервером [8]. У великих корпоративних системах застосовують OSDP та Wiegand [9]. Проте в компактних рішеннях, де зчитувач розташований безпосередньо біля контролера, обмін даними відбувається через локальні послідовні шини SPI, I2C або UART, що гарантує високу швидкість на коротких відстанях. Взаємодія контролера з сервером здійснюється через Ethernet або Wi-Fi, що дає змогу віддалено керувати системою через єдиний веб-інтерфейс.

Таблиця 1.1 – Порівняльний аналіз типів ідентифікації у СКУД

Критерій оцінки	Безконтактні картки (RFID)	NFC-технології	Bluetooth (BLE)	Біометричні системи
Дальність зчитування	Дуже мала (до 5–10 см)	Вкрай мала (до 2–4 см, впритул)	Налаштовувана (від 10 см до 10–15 м)	Контактна або безконтактна (до 1–2 м для обличчя)
Рівень безпеки та захисту	Від низького (EM-Marine) до високого (Mifare з шифруванням)	Високий (динамічне шифрування, захист копіювання)	Високий (шифровані канали зв'язку)	Найвищий (унікальні біометричні ознаки людини)
Зручність для користувача	Середня (потрібно постійно носити окрему картку/брелок)	Висока (використовується смартфон, який завжди під рукою)	Найвища (можливий "вільні руки" доступ без виймання телефону)	Максимальна (не потрібні жодні фізичні носії чи гаджети)
Ризик компрометації	Високий (картку можна загубити, передати або скопіювати)	Низький (смартфон захищений паролем чи біометрією)	Низький (ідентифікатор прив'язаний до додатка на телефоні)	Мінімальний (неможливо передати іншому, захист від муляжів)
Швидкість спрацьовування	Миттєво (до 0.1 сек)	Дуже швидко (до 0.2 сек)	Швидко (0.5–1 сек, залежно від налаштування дистанції)	Залежить від бази (від 0.2 сек до 1.5 сек на розпізнавання)
Вартість ідентифікаторів	Мінімальна (низька ціна карток та брелоків)	Нульова (використовуються особисті смартфони)	Нульова (використовуються особисті смартфони та мобільний додаток)	Відсутня (ідентифікатором виступає сам користувач)
Вартість зчитувачів та обладнання	Низька / Середня	Середня	Середня / Висока	Висока / Дуже висока
Чутливість до зовнішніх умов	Мінімальна (працюють у бруді, воді, через одяг)	Мінімальна	Середня (залежить від радіоперешкод та екранування корпусом)	Висока (забруднення пальців, погане освітлення, наявність масок)

1.4. Порівняльна оцінка підходів до побудови архітектури

Вибір архітектури є визначальним етапом проєктування. Щоб обґрунтувати технології для нашого проєкту, порівняймо три базові концепції, що були визначені раніше. Цими концепціями є повністю автономна, класична локальна та сучасна

розподілена архітектури. Оцінка проводиться за вартістю обладнання, складністю встановлення, гнучкістю управління та здатністю до масштабування.

Автономні системи працюють ізольовано й зберігають картки користувачів у внутрішній пам’яті контролера. Це найдешевший варіант, він майже не потребує налаштування мережі, але геть позбавлений гнучкості. Адміністратор не може дистанційно керувати доступом або переглядати історію подій у реальному часі.

Класична локальна архітектура вирішує проблему централізації. Усі зчитувачі підключаються до локального сервера, що дає повний контроль над даними. Однак це тягне за собою значні витрати на серверне обладнання, складне прокладання кабелів і потребу в спеціалістах для обслуговування.

Розподілена архітектура пропонує інший підхід. Апаратний вузол лише зчитує картки й передає сигнал виконавчому пристрою, тоді як уся логіка перевірки лежить на віддаленому сервері. Безпровідні модулі дозволяють відмовитися від більшості кабелів, що робить систему гнучкою, легко масштабованою та придатною для дистанційного керування.

Для наочності результату аналізу було створено порівняльну табл. 1.2.

Таблиця 1.2 – Порівняльний аналіз архітектур побудови

Критерій оцінки	Автономна архітектура	Локальна серверна система	Розподілена архітектура
Вартість розгортання	Низька	Висока	Середня
Складність встановлення	Низька	Дуже висока (кабелі)	Низька (бездротовий зв'язок)
Дистанційне управління	Відсутнє	Наявне (лише локально)	Наявне (через інтернет)
Здатність до масштабування	Низька	Обмежена сервером	Висока

З наведеного порівняння у табл. 1.2 видно, що для розробки сучасної системи контролю доступу найкращим вибором є розподілена архітектура. Використання новітніх мікроконтролерів у парі зі зчитувачами карток забезпечує надійну роботу при

мінімальному енергоспоживанні. Водночас перенесення логіки з контролера на сервер дозволяє зручно контролювати та використовувати систему, що робить її гнучкою до подальшого розширення.

1.5. Роль сучасних веб-технологій в управлінні системами безпеки

Історично системи безпеки потребували присутності оператора, однак автоматизація дозволила прибрати людину з ланцюга керування. Сучасні веб-технології дають змогу створювати системи, управління якими більше не прив'язане до робочого місця чи локального комп'ютера [10].

Головна перевага веб-технологій це кросплатформеність і гнучкість. Замість важкого програмного забезпечення прив’язаного до комп’ютера, користувач заходить у систему зі смартфона чи будь-якого іншого пристрою незалежно від операційної системи й бачить усі дані про пункти пропуску та стан обладнання в реальному часі [10]. Адміністратор може оперативно змінювати права доступу для груп або окремих осіб і автоматично генерувати аналітичні звіти щодо порушень трудової дисципліни. Такий підхід спрощує щоденне адміністрування й суттєво зменшує навантаження на локальні обчислювальні ресурси.

1.6. Огляд існуючих комерційних рішень на ринку безпеки

Для об’єктивної технічної оцінки ринку та формування максимально правильних і обґрунтованих вимог до власної апаратної розробки необхідно детально розглянути існуючі комерційні системи контролю доступу, які сьогодні масово представлені продукцією таких відомих світових брендів як Ajax Systems та Hikvision [11].

Першим об’єктом дослідження є комплекс на базі централізованого хмарного пристрою Ajax Hub 2 Plus [11], безконтактної кодової панелі Ajax KeyPad Plus [12] та виконавчого модуля Ajax Relay [13]. Центральний хаб підтримує одночасну роботу через чотири незалежні канали зв’язку, включаючи Ethernet, Wi-Fi та дві SIM-картки

з підтримкою мереж високої швидкості. Кодова панель Ajax KeyPad Plus має інтегрований зчитувач на частоті 13,56 МГц і працює із захищеними від копіювання картками та брелками на основі технології Mifare DESFire. Керування електромагнітним замком реалізується через бездротовий протокол Jeweller, а саме хаб подає логічний сигнал на силове реле Ajax Relay, яке комутує лінію живлення замка. Перевагами системи є висока швидкість монтажу та надійне бездротове шифрування, однак повна закритість операційної системи OS Malevich унеможливлює додавання нестандартних датчиків або зміну алгоритмів взаємодії апаратної частини з користувацькими застосунками. Систему зображено на рисунку 1.3 [11]-[13].

Рисунок 1.3 – Візуальний вигляд Ajax Hub 2 Plus, Ajax KeyPad Plus та Ajax Relay

Другим комерційним аналогом є мережевий контролер доступу Hikvision DS-K2602, який розроблений для керування двома точками проходу. Це класичний IP-контролер на 32-розрядному процесорі з енергонезалежною пам’яттю, яка здатна зберігати дані про 100000 карток користувачів і понад 300000 подій проходу [14]. Пристрій підтримує підключення до чотирьох зовнішніх зчитувачів через інтерфейси Wiegand або RS-485, а також має велику кількість входів для підключення датчиків стану дверей та кнопок виходу. Керування замками здійснюється через релейні виходи із гальванічною розв’язкою. Адміністрування потребує розгортання локального сервера зі спеціалізованим програмним забезпеченням iVMS-4200. Загальний вигляд приладу наведено на рисунку 1.4 [14].

Рисунок 1.4 – Візуальний вигляд Hikvision DS-K2602

Щоб остаточно зрозуміти спільні та відмінні характеристики розглянутих систем, варто розглянути табл. 1.3 [11]-[14].

Таблиця 1.3 – Порівняльний аналіз технічних характеристик комерційних рішень Ajax Systems та Hikvision

Критерій порівняння	Комплекс Ajax (Hub 2 Plus + KeyPad Plus)	Контролер Hikvision DS-K2602
Тип підключення компонентів	Бездротовий (радіопротокол Jeweller)	Дротовий (інтерфейси RS-485, Wiegand)
Основні мережеві інтерфейси	Wi-Fi, Ethernet, 2G/3G/4G (LTE)	Ethernet (TCP/IP)
Підтримувані стандарти ідентифікаторів	Mifare DESFire, Mifare Plus (13.56 МГц)	Спадкові та сучасні формати (Mifare, EM-Marine)
Об'єм локальної пам'яті подій	Залежить від хмарного сховища	300 000 подій автономно
Керування виконавчим пристроєм	Через зовнішній бездротовий модуль реле	Через інтегровані реле на платі контролера
Спосіб адміністрування бази даних	Мобільні та десктопні закриті додатки Ajax	Локальне програмне забезпечення iVMS-4200

Проведений аналіз комерційних приладів показує, що наявні рішення або прив’язані до закритих хмарних платформ, або потребують розгортання складних та дорогих локальних серверів, що ще раз підтверджує високу актуальність проєктування власної відкритої системи з веб-додатком.

1.7. Протоколи та моделі обміну даними в архітектурі

Робота системи контролю доступу неможлива без надійного та швидкого обміну даними між мікроконтролером та сервером. Класична архітектура REST API на базі протоколу HTTP дозволяє мікроконтролеру надсилати на сервер запити про валідацію щойно зчитаного ідентифікатора й отримувати у відповідь чіткі інструкції у форматі JSON щодо дозволу або відхилення доступу [15].

Однак для повноцінного моніторингу подій у реальному часі без постійного, ресурсоємного опитування сервера доцільно застосувати технологію WebSocket. Згідно зі специфікацією RFC 6455, протокол WebSocket встановлює постійне двостороннє мережеве з'єднання поверх одного TCP-сокета, завдяки чому адміністратор у браузері миттєво отримує сповіщення про зміну стану дверей або спроби несанкціонованого проходу [16].

1.8. Керування виконавчими пристроями блокування

Ми вже з'ясували, що роль виконавчих механізмів у СКУД відіграють електрозамки. Саме вони є кінцевою ланкою і фізично виконують команду контролера, або обмежуючи прохід, або надаючи його. Тепер варто розглянути їх детальніше, адже від їхнього типу залежить логіка роботи всієї системи безпеки.

У сучасних СКУД виконавчим пристроєм найчастіше виступає електромагнітний або електромеханічний замок. Електромагнітний замок працює за рахунок взаємодії електромагніту з металевою пластиною й підходить для систем із частою роботою, однак він потребує постійного живлення, тому при вимкненні електроенергії відчиняється. В свою чергу, електромеханічний замок не потребує постійної подачі, адже в момент закриття зводиться пружина, яка утримує замок зачиненим до моменту подачі живлення, тож при знеструмленні він залишається заблокованим [17].

Керування виконавчими пристроями здійснюється через мікроконтролер, однак пряме підключення до його логічних виходів неможливе через високий струм

споживання замків. Для вирішення цієї задачі існують комутаційні елементи, зокрема електромагнітні реле, які за сигналом від мікроконтролера подають або знімають напругу з виконавчого пристрою [18]. Критично важливо при проектуванні СКУД передбачити відмикання замка при повному знеструмленні, оскільки за правилами пожежної безпеки електрозамок має бути нормально відкритим, щоб не перешкоджати евакуації людей у надзвичайних ситуаціях [19].

1.9. Постановка завдання

1.9.1. Мета проєкту

Головною метою є проєктування та розробка пристрою контролю доступу для захисту приміщень із безконтактною ідентифікацією користувачів, керуванням запірним механізмом дверей та зручним дистанційним адмініструванням. Цільовий сценарій експлуатації передбачає зчитування безконтактного ідентифікатора, автоматичну валідацію прав доступу, подачу сигналу на відкриття виконавчого механізму та обов’язкову фіксацію події в електронному журналі на сервері.

1.9.2. Вимоги до системи

Апаратна частина системи повинна будуватися на основі мікроконтролера з модулем бездротового зв’язку для обміну даними з сервером. Для авторизації користувачів необхідний модуль радіочастотної ідентифікації, який забезпечить швидке зчитування безконтактних карток. Разом з тим, пристрій має постійно відстежувати положення дверей за допомогою магнітоконтактного датчика і надійно керувати живленням електрозамка.

1.10. Побудова загальної структурної схеми системи

Для реалізації поставлених завдань необхідно визначити базові вузли системи та зв'язки між ними. Апаратна архітектура пристрою має включати обчислювальний модуль, систему збору даних із датчиків, елементи індикації та виконавчий механізм. Графічне представлення розробленої структурної схеми наведено на рисунку 1.5.

Рисунок 1.5 – Структурна схема автоматизованого пристрою контролю доступу до приміщень

Робота комплексу базується на безперервній взаємодії апаратних та програмних компонентів, де керуючим ядром виступає мікроконтролер. Принцип дії починається з моменту, коли користувач підносить ідентифікатор до зчитувача на вході або на виході. Отриманий унікальний код миттєво передається до мікроконтролера, який обробляє його та відправляє запит на сервер через бездротову мережу.

Програмна частина системи, яка включає сервер та веб-інтерфейс, отримує запит, перевіряє права доступу користувача в базі даних і повертає мікроконтролеру відповідь. Якщо доступ дозволено, мікроконтролер активує виконавчий механізм, надсилаючи керуючий сигнал на блок реле, яке замикає або розмикає силове коло живлення електрозамка. Паралельно вмикається блок індикації, який повідомляє користувачеві про результат.

Для забезпечення повного контролю за ситуацією система використовує зворотний зв’язок, за який відповідає магнітний датчик геркона. Він постійно відстежує фактичне положення дверей і передає дані мікроконтролеру. Це дає системі

змогу підтвердити, що двері дійсно відчинилися після дозволу, або зафіксувати тривогу, якщо прохід залишився відкритим занадто довго.

Висновки до розділу 1

У цьому розділі було проведено комплексний аналіз предметної області систем контролю фізичного доступу, який переконливо довів необхідність використання мікропроцесорної архітектури у поєднанні з сучасними веб-технологіями. Огляд існуючих класифікацій дозволив визначити, що найбільш надійним інженерним підходом виступає побудова універсальних систем, які вдало поєднують переваги централізованого мережевого моніторингу.

Детальний аналіз комерційних рішень підтвердив доцільність розробки власного апаратного-програмного комплексу, оскільки наявні на ринку аналоги мають повністю закрите програмне забезпечення або потребують розгортання дорогих локальних серверів. Разом з тим дослідження мережевих стандартів дозволило обґрунтувати вибір технологій HTTP та WebSocket для забезпечення стабільного двостороннього обміну даними у реальному часі. На основі зібраної аналітичної інформації було сформульовану голову мету кваліфікаційної роботи, визначено технічні вимоги та розроблено структурну схему системи, яка описує принцип роботи.

РОЗДІЛ 2. РОЗРОБКА ФУНКЦІОНАЛЬНОЇ СХЕМИ ТА АРХІТЕКТУРИ СИТЕМИ

2.1. Розробка функціонально схеми системи

Функціональна схема розроблюваної системи детально відображає внутрішню архітектуру логічних вузлів та напрямки потоків даних між апаратними і програмними компонентами. На рисунку 2.1 представлено схему, яка повністю описує процеси обробки інформації на рівні окремих апаратних блоків.

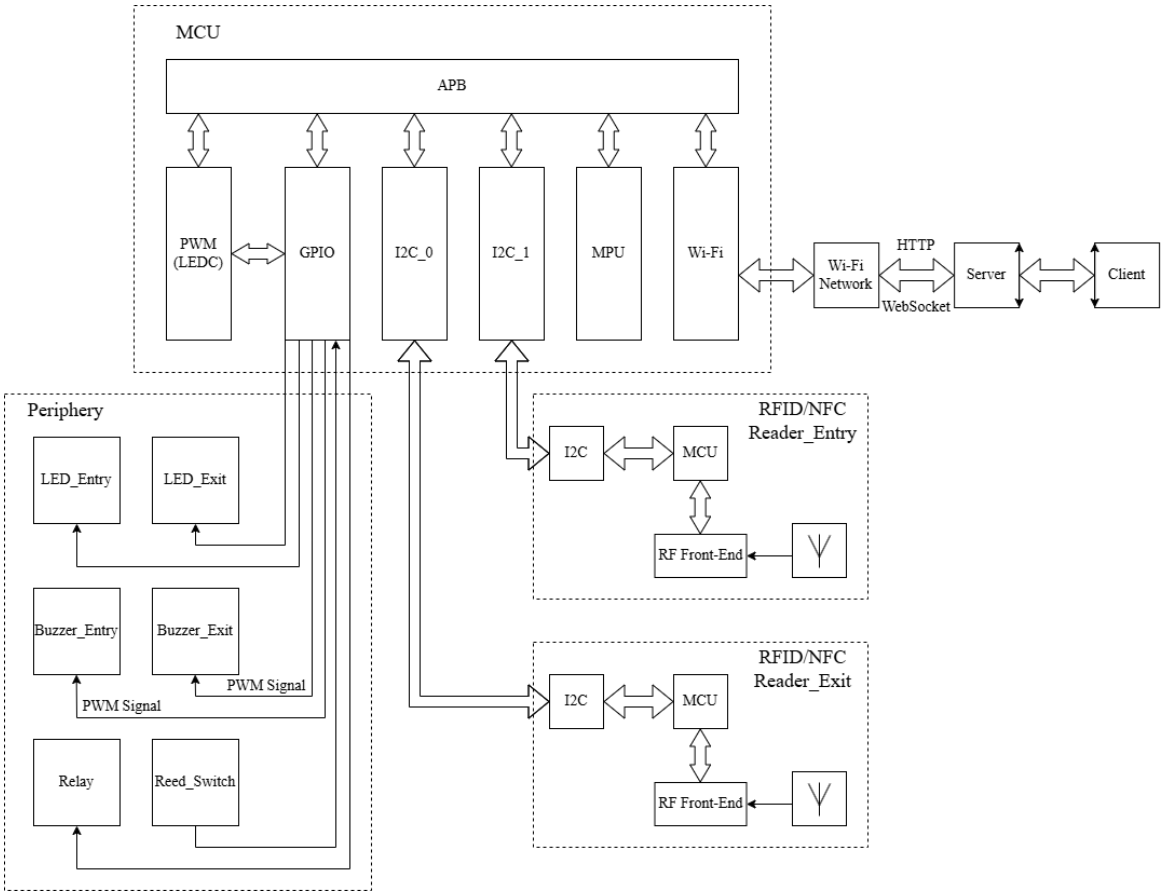

Рисунок 2.1 – Функціональна схема автоматизованого пристрою контролю доступу до приміщень

Основою схеми є мікроконтролер MCU, внутрішня архітектура якого побудована навколо мікропроцесорного ядра MPU. Для забезпечення швидкого та синхронного обміну даними між ядром і всіма периферійними блоками використовується внутрішня шина APB, до якої підключені контролери інтерфейсів

вводу та виводу, що дозволяє центральному процесору ефективно розподіляти ресурси при обробці сигналів.

Підсистема збору вхідних даних формується з двох джерел. Першим джерелом виступають модулі безконтактного зчитування ідентифікаторів для входу Reader_Entry та виходу Reader_Exit. Кожен такий пристрій має власну антену та спеціалізований інтерфейс RF Front-End. Після первинної обробки локальним мікроконтролером зчитувача цифровий код передається до головного процесора через шину I2C. Другим джерелом вхідних даних є датчик стану дверей Reed_Switch, який передає цифровий стан безпосередньо на порт введення загального призначення GPIO.

Керування виконавчою та індикаційною периферією реалізується через контролер портів загального призначення GPIO. Цифрові виходи мікроконтролера подають логічні рівні на світлодіодні індикатори LED_Entry, LED_Exit та комутаційне реле Relay, яке замикає або розмикає силове кола живлення електрозамка. Для генерації звукових сповіщень використовується блок широтно-імпульсної модуляції PWM, який формує імпульси заданої частоти для динаміків Buzzer_Entry та Buzzer_Exit.

Мережевий рівень системи реалізується за допомогою інтегрованого блоку Wi-Fi, який відповідає за встановлення стабільного зв’язку та забезпечує передачу інформації про всі події на сервер.

2.2. Розробка архітектури та загального алгоритму роботи системи

2.2.1. Розробка архітектури системи

Проєктована нами система контролю доступом побудована за класичною багаторівневою архітектурою, що дозволяє чітко розмежувати апаратні та програмні процеси. Тому загальну структуру комплексу доцільно розділити на чотири основні взаємопов’язані рівні, кожен з яких виконує суворо визначений спектр завдань.

Першим рівнем нашої архітектури виступає фізичний рівень периферійних пристроїв, який безпосередньо взаємодіє з навколишнім середовищем та кінцевими користувачами. Головним обчислювальним ядром на цьому етапі є мікроконтролер, який виконує первинну обробку даних та керує периферією. До складу цього рівня входить сенсорна підсистема із зчитувачами для входу та виходу, а також датчиком для контролю положення дверей. Виконавча підсистема тут реалізована через модуль реле, який комутує лінію живлення електрозамка, тоді як здійснюється звукова та світлова індикація.

Зібрана на фізичну рівні інформація потребує надійного каналу зв’язку, за що відповідає мережевий та транспортний рівень. Його головним завданням є безпечна та швидка передача пакетів даних між локальним контролером і віддаленим сервером. У розробленій системі ця взаємодія реалізується за допомогою гібридної моделі обміну інформацією через бездротовий інтерфейс Wi-Fi. Протокол HTTP архітектури REST API використовується мікроконтролером одноразово під час завантаження для отримання базових налаштувань системи. Водночас WebSocket забезпечує постійне двостороннє з'єднання у режимі реального часу для оперативної передачі унікальних ідентифікаторів карток, отримання дозволів на прохід та надсилання сповіщень у форматі JSON.

Усі дані, які проходять через транспортний рівень, потрапляють до серверного рівня та бази даних, що виконує роль центрального вузла прийняття рішень. Цей програмний контур реалізований за допомогою серверної платформи із використанням бази даних. Серверна частина безперервно приймає запити від мікроконтролера, класифікує типи подій та за перевіряє отримані ідентифікатори. Звіривши дані з базою, сервер генерує відповідний статус доступу, а також веде журнал подій, фіксуючи точний час проходу персоналу або моменти спрацювання тривоги.

Завершальною ладною архітектури, яка дозволяє адміністратору взаємодіяти із зібраною та обробленою інформацією, є клієнтський рівень веб-інтерфейсу. Він реалізований у вигляді веб-застосунку, який слугує повноцінною панеллю керування. Цей застосунок забезпечує візуальний моніторинг статусу підключених пристроїв,

дозволяючи оперативно змінювати їхні налаштування та здійснювати віддалене примусове відкриття дверей. Крім того, саме на цьому рівні відбувається адміністрування бази користувачів, включаючи реєстрацію нових карток та генерацію аналітичних звітів на основі журналу подій.

2.2.2. Розробка загального алгоритму системи

Описані раніше процеси, найдоцільніше представити у вигляді загальних алгоритмів, які визначають чітку логічну послідовність дій апаратної та програмної частини під час експлуатації.

Ініціалізація пристрою

Після подачі живлення мікроконтролер автоматично підключається до бездротової мережі. Одразу після отримання мережевої адреси пристрій формує й одразу надсилає HTTP GET запит із унікальною фізичною адресою контролера. Сервер знаходить цю адресу в базі даних і повертає у відповідь JSON пакет із прив’язаними налаштуваннями системи. Мікроконтролер застосовує отримані параметри, подає сигнал на блокування дверей, після чого встановлює безперервний WebSocket зв’язок і надсилає команди реєстрації. Далі система переходить у штатний режим очікування подій. Блок-схема алгоритму ініціалізації системи наведена на рисунку 2.2.

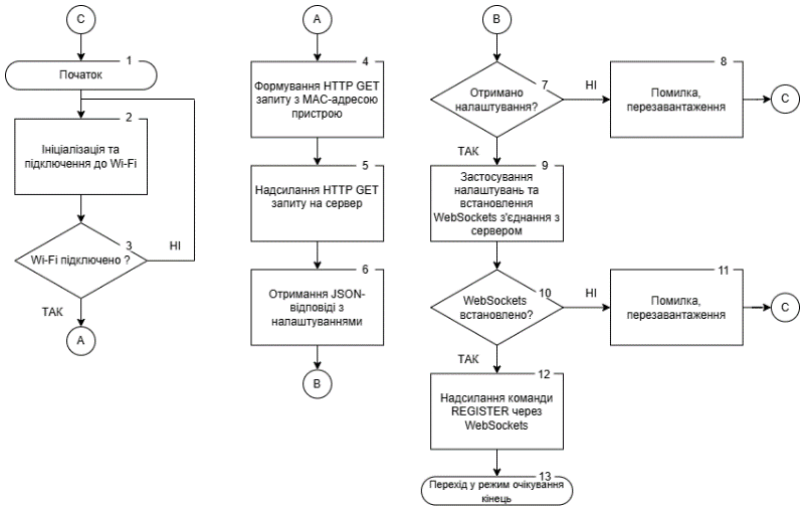

Рисунок 2.2 – Блок-схема алгоритму ініціалізації системи

Прохід за ідентифікаційною карткою

У минулому абзаці ми визначили, як проходить ініціалізація системи та перехід до режиму очікування. Тому варто розглянути алгоритм контролю доступу, адже він активується у момент, коли користувач підносить свою картку до зчитувача. Мікроконтролер миттєво зчитує унікальний номер картки та відправляє запит на перевірку через активний канал WebSocket на сервер. Серверна логіка перевіряє наявність отриманого коду в базі даних та, у разі успішної авторизації, відправляє на мікроконтролер команду підтвердження доступу, який в свою чергу активує звукову та світлову індикацію і розблоковує двері, при цьому запустивши таймер очікування проходу, щоб точно зафіксувати факт проходження. Тому, якщо датчик стану дверей зафіксував фізичне відкриття дверей до спливання таймеру, мікроконтролер підтверджує факт успішного проходу, відправляючи інформаційний пакет на сервер, в іншому разі транзакція проходу скасовується і двері блокуються. Блок-схема алгоритму ідентифікації картки наведена на рисунку 2.3.

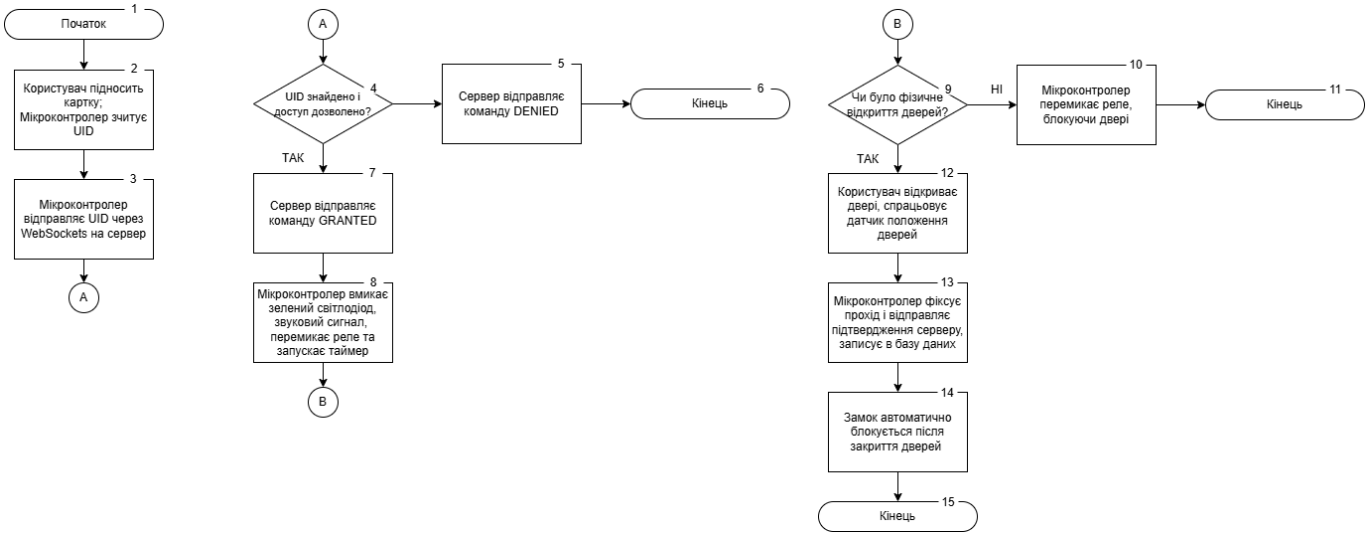

Рисунок 2.3 – Блок-схема алгоритму ідентифікації картки

Обробка несанкціонованого доступу

Алгоритм фіксації тривоги розпочинає свою роботу у випадку, якщо датчик положення дверей фіксує фізичне відкриття дверей без попередньої авторизації. Отримавши такий сигнал, мікроконтролер перевіряє логічну умову наявності

недавнього успішного зчитування картки або отримання команди віддаленого відкриття. Якщо жодна з цих умов не виконується, мікроконтролер класифікує подію як несанкціоноване проникнення, після чого негайно вмикає локальну світлову та звукову сигналізацію для привернення уваги. Одночасно з цим пристрій формує та відправляє пакет даних, який повідомляє про тривогу через WebSocket на сервер, який автоматично записує критичну подію в базу даних і миттєво оновлює статус безпеки у панелі керування. Блок-схема алгоритму обробки несанкціонованого доступу наведена на рисунку 2.4.

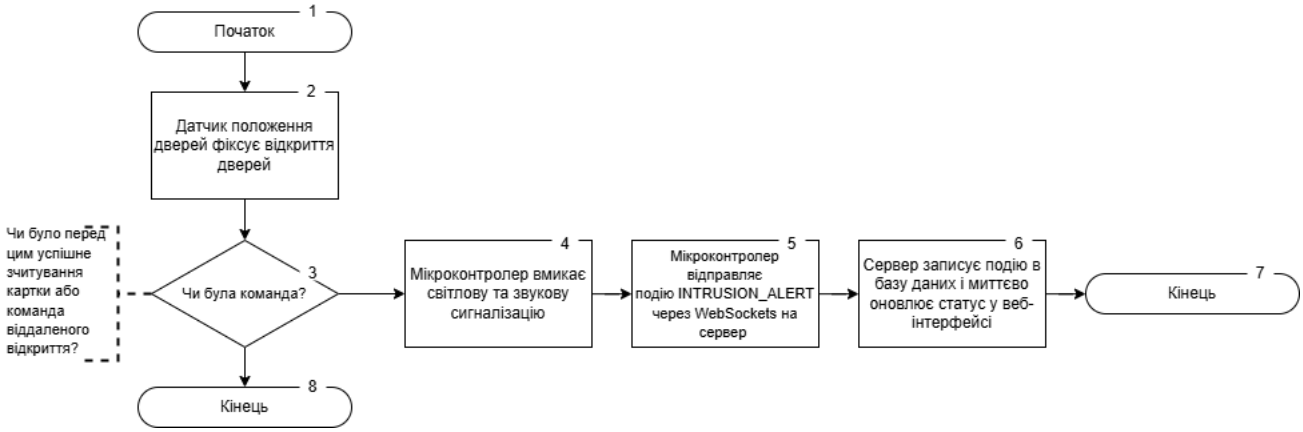

Рисунок 2.4 – Блок-схема алгоритму обробки несанкціонованого доступу

Висновки до розділу 2

У другому розділі було розроблено багаторівневу архітектуру системи та побудовано функціональну схему, яка наочно відображає маршрутизацію інформаційних потоків між логічним ядром мікроконтролера та периферією. Також чітко визначено базові алгоритми роботи, що описують процеси початкової ініціалізації, авторизації користувачів із перевіркою фактичного відкриття дверей та реагування на несанкціонований доступ. Розроблена архітектура і алгоритмічна база повністю описує логіку взаємодії вузлів системи та відповідає поставленій меті.

РОЗДІЛ 3. ВИБІР КОМПОНЕНТІВ ТА РОЗРОБКА ПРИНЦИПОВОЇ ЕЛЕКТРИЧНОЇ СХЕМИ

3.1. Вибір компонентів

3.1.1. Вибір мікроконтролера

Центральним обчислювальним компонентом нашого пристрою є мікроконтролер, до якого висуваються високі вимоги щодо обчислювальної потужності, об’єму внутрішньої пам’яті ті наявності інтегрованих бездротових інтерфейсів. Для проведення об’єктивного аналізу було розглянуто три популярні мікропроцесорні платформи, які найчастіше використовуються при розробці систем автоматизації, а саме ATmega328P [20], STM32F103C8T6 [21] та ESP32 [22]. Результати порівняльного аналізу архітектур та технічних можливостей цих мікроконтролерів наведені у табл. 3.1 [20]-[22].

Таблиця 3.1 – Порівняльний аналіз технічних характеристик мікроконтролерів

Критерій порівняння	ATmega328P	STM32F103C8T6	ESP32
Архітектура та розрядність	AVR (8-біт)	ARM Cortex-M3 (32-біт)	Xtensa LX6 (32-біт)
Тактова частота ядра	До 16 МГц	До 72 МГц	До 240 МГц
Кількість ядер	1	1	2
Об'єм оперативної пам'яті (RAM)	2 КБ	20 КБ	520 КБ
Об'єм постійної пам'яті (Flash)	32 КБ	64 КБ	4 МБ
Інтегровані мережеві модулі	Відсутні	Відсутні	Wi-Fi (802.11 b/g/n), Bluetooth
Апаратне шифрування даних	Відсутнє	Відсутнє	AES, SHA, RSA, ECC

Аналіз табл. 3.1 показує, що ATmega328P не підходить через критично малий об’єм оперативної пам’яті та низьку тактову частоту. STM32F103C8T6 має високу швидкодію, проте позбавлений вбудованого бездротового інтерфейсу, що вимагає

зовнішніх мережевих компонентів. Тому головним керуючим пристроєм системи обрано плату ESP32 NODEMCU-32S на чипі ESP32, зображену на рисунку 3.1. Вибір зумовлений підтримкою бездротового зв’язку для з’єднання з сервером, високим рівнем безпеки передачі даних та швидкою обробкою сигналів від периферії.

Рисунок 3.1 – Загальний вигляд плати розробника ESP32 NODEMCU-32S

Базовий чип ESP32 від компанії Espressif Systems [23] це система на кристалі SoC, виготовлена за 40-нанометровою технологією TSMC, що забезпечує низьке енергоспоживання та якісну інтеграцію компонентів [22]. Основним обчислювальним вузлом системи є двоядерний 32-бітний мікропроцесор Xtensa LX6, архітектура якого дозволяє розділяти критичні завдання: одне ядро відповідає за бездротовий зв’язок, інше виконує код розробника, що мінімізує ризик розриву мережевого з’єднання через складні обчислення [24]. Вбудована пам’ять включає 448 КБ ROM для завантаження системи, 520 КБ статичної оперативної пам’яті SRAM, а також 16 КБ пам’яті в області RTC, яка в свою чергу розділена на 8 КБ швидкої та 8 КБ повільної пам’яті, для тривалого збереження даних в енергозберігаючих режимах [25]. Основні технічні характеристики цієї плати наведені у табл. 3.2 [22], [24], [25].

Таблиця 3.2 – Технічні характеристики ESP32 NODEMCU-32S

Параметр	Значення
Процесор	Xtensa LX6 (два ядра)
Максимальна частота	240 МГц
Обсяг SRAM	520 КБ
Бездротовий зв'язок	Wi-Fi + Bluetooth (Classic & BLE)
Канали АЦП (ADC)	18 (12-біт)
Канали ЦАП (DAC)	2 (8-біт)
Сенсори дотику	10 каналів
Апаратне шифрування	AES, SHA-2, RSA, ECC, RNG

Продовження таблиці 3.2

Параметр	Значення
USB-UART конвертер	CP2102
Напруга живлення	5 В
Температурний режим	-40 ~ +85 °C
Розміри плати	25 x 50 мм

Окремої уваги заслуговує багатий набір інтерфейсів введення-виведення. ESP32 має два 12-бітні модулі АЦП, а саме ADC1 та ADC2. ADC1 обслуговує 8 каналів на пінах GPIO 32-39, і залишається доступним під час роботи Wi-Fi. ADC2 обслуговує піни GPIO 0, 2, 4, 12-15 та 25-27, однак не може використовуватись одночасно з активним Wi-Fi передавачем. Також мікроконтролер має два 8-бітних каналів ЦАП на GPIO 25 та 26 для генерації аналогових сигналів. На додаток модуль підтримує 3 порти UART, 3 інтерфейси SPI (SPI, HSPI, VSPI) та 2 інтерфейси I2C [26]. Усі наявні інтерфейси наведено у табл. 3.3 [26].

Таблиця 3.3 – Інтерфейси введення-виведення плати NODEMCU-32S

Назва інтерфейсу	К-сть	Функціональне призначення
UART	3	Послідовний зв'язок (RS232, RS485, IrDA)
SPI	3	Високошвидкісний зв'язок із дисплеями, пам'яттю, сенсорами
I2C	2	Шина для підключення датчиків та периферії
I2S	2	Передача цифрового звуку
PWM	16	Керування яскравістю LED та швидкістю двигунів
CAN (TWAI)	1	Зв'язок із автомобільними та промисловими шинами

Однією з найсильніших сторін ESP32 є система керування живленням, яка робить NODEMCU-32S придатним для пристроїв з батарейним живленням, адже чип підтримує складну ієрархію режимів сну, а саме:

1. Active Mode: Всі компоненти активні, споживання струму складає від 160 мА до 260 мА. Це режим інтенсивних обчислень або активного обміну даними [27].

2. Modem-sleep: Процесор працює, але Wi-Fi та Bluetooth вимкнені, при цьому споживання знижується до 20-68 мА [27].
3. Light-sleep: Стан процесора зберігається в оперативній пам’яті, цифрова периферія призупинена, а споживання становить близько 0,8 мА [27].
4. Deep-sleep: Живлення подається лише на область RTC та копроцесор ULP, що дозволяє знизити споживання струму до неймовірних 10 мкА. Це основний режим для автономних датчиків, які прокидаються лише раз на годину для передачі даних [27].
5. Hibernation: Цей рижим вимикає майже все, окрім одного таймера RTC, що робить споживання близько 5 мкА [27].

Для реалізації цих режимів можна використовувати таймери або зовнішні події на GPIO.

Ще одним фактором вибору саме цієї плати стало надійність захищення даних, адже NODEMCU-32S пропонує апартну підтримку криптографії, що значно швидше та енергоефективніше за програму реалізацію. У нашому розпорядженні є аж три системи захисту:

1. Flash Encryption: Шифрування вмісту зовнішньої флеш-пам’яті за допомогою ключа, що зберігається в захищеній області eFuse чипа, що дозволяє запобігти копіювання прошивки та крадіжці інтелектуальної власності [28].
2. Secure Boot: Це механізм перевірки цифрового підпису прошивки перед запуском, саме це гарантує, що пристрій виконує лише довірений код і не був скомпрометований зловмисниками [28].
3. Cryptographic Acceleration: Це спеціальні блоки для обробки алгоритмів AES, SHA-2, RSA та ECC дозволяють працювати з протоколами TLS та SSL (https, mqtts) без значного впливу на продуктивність системи [28].

Саме ці механізми дозволяються безпечно передавати дані користувачів мережею не переживаючи за їх цілісність, чого і потребує наша система.

Не менш важливим є розподіл пінів GPIO за функціями, оскільки не всі 38 виведених контактів рівноцінні. Піни GPIO 34, 35, 36 та 39 працюють лише на ввід, не мають внутрішніх підтягувальних резисторів і найкраще підходять для аналогових сигналів через АЦП. Strapping-піни GPIO 0, 2, 5, 12 та 15 відповідають за режим запуску, і зміна їхнього стану під час подачі живлення може перешкодити завантаженню програми. Піни GPIO 6, 7, 8, 9, 19 та 11 з'єднанні з чипом SPI Flash, тому їх використання для периферії призведе до негайної зупинки системи. Найнадійнішими для підключення будь-якої периферії є безпечні піни GPIO 18, 19, 21, 22, 23, 25, 26, 27, 32 та 33, оскільки вони не впливають на процес старту й мають повну функціональність вводу-виводу [29]. Такий розподіл дозволяє уникнути проблем під час запуску чи перезавантаження плати. Схему розташування та функціонал кожного піна зображено на рисунку 3.2 [30].

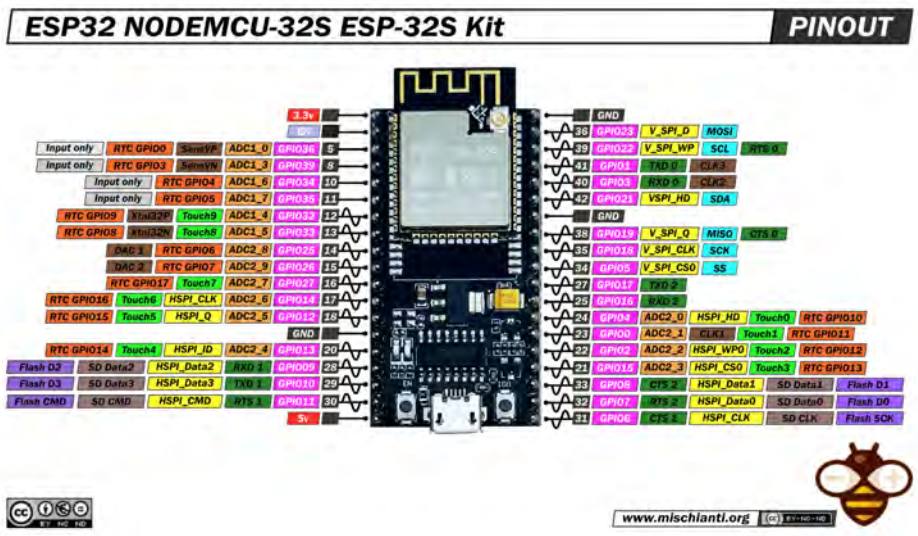

Рисунок 3.2 – Схема пінів плати ESP32 LuaNode32 NODEMCU-32S

3.1.2. Вибір зчитувачів ідентифікаторів

Вибір зчитувача ідентифікаторів є одним із найважливіших етапів розробки. Раніше ми з'ясували, що одним з найкращих варіантів є RFID зчитувач, тому спочатку потрібно порівняти дві найпопулярніші моделі на базі мікросхем MFRC522 [31] та PN532 [32]. Порівняльні характеристики зчитувачів наведені у табл. 3.4 [31], [32].

Таблиця 3.4 – Порівняльний аналіз модулів радіочастотної ідентифікації

Критерій порівняння	Модуль MFRC522	Модуль PN532
Підтримувані інтерфейси зв'язку	SPI, I2C, UART	I2C, SPI, HSU (High Speed UART)
Робочі режими пристрою	Тільки читання та запис міток	Читання/запис, емуляція картки, Peer-to-Peer
Підтримка технології NFC	Відсутня	Повна апаратна підтримка
Сумісність із захищеними картами	Обмежена (лише Mifare Classic)	Повна (Mifare Classic, Mifare DESFire)
Стабільність радіочастотного поля	Середня	Висока (завдяки вбудованому драйверу антени)

Спираючись на результати порівняння, для розробки обрано зчитувач Elechouse PN532 NFC Module V3, зображений на рисунку 3.3. Контролер PN532 від компанії NXP Semiconductors це надійне рішення для безконтактного зв’язку на частоті 13,56 МГц, що стало фактичним стандартом у галузі. Сам пристрій базується на архітектурі мікроконтролера 80C51, яка дозволяє виконувати складні операції з протоколами NFC безпосередньо на кристалі, звільняючи ресурси центрального процесора системи для інших завдань [32].

Рисунок 3.3 – Загальний вигляд модуля Elechouse PN532 NFC Module V3

Однією з найважливіших особливостей модуля RN532 V3 є його здатність працювати в чотирьох основних режимах, детальний опис яких наведено у табл. 3.5 [33].

Таблиця 3.5 – Режими роботи модуля RN532 V3

Режим роботи	Характеристики та стандарти	Особливості та застосування
Зчитувач та записувач	Підтримує ISO/IEC 14443A/MIFARE, ISO/IEC 14443B та FeliCa	Масштабні системи, де потрібне шифрування та швидка передача біометричних або банківських даних всередині картки.
Емуляція картки	Модуль працює як пасивний ідентифікатор (фізична картка)	Обмеження безпеки: перший байт UID примусово встановлюється у 0x08, що вказує на випадковий або згенерований програмно ідентифікатор.
NFCIP-1	Обмін даними між двома пристроями NFC на швидкості до 424 кбіт/с	Ідеально для швидкої передачі конфігурацій, обміну картками або налаштування з'єднання. Пристрої почергово створюють радіочастотне поле.
Робота з модулем SAM	Інтерфейс для з'єднання зчитувача з криптографічним чипом SAM	Критично для банківських систем. Модуль SAM виконує обчислення, зберігає ключі та перевіряє автентичність без передачі даних у відкритий доступ.

Також модуль PN532 V3 вирізняється високою енергоефективністю завдяки вбудованим режимам споживання. У режимі Hard Power Down струм становить близько 1 мкА, у режимі Soft Power Down цей показник зростає до 10-22 мкА, що забезпечує швидке пробудження при виявленні радіочастотного поля або команди від контролера [33]. Окрім гнучкого керування живленням, модуль пропонує три варіанти підключення, а саме I2C, SPI та High-Speed UART (HSU) [34]. Усі інші важливі технічні характеристики модуля наведені у табл. 3.6. [34].

Таблиця 3.6 – Технічні характеристики модуля Elechouse PN532 NFC Module V3

Параметр	Значення
Напруга живлення (VBAT)	2.7 В – 5.5 В
Логічні рівні інтерфейсів	5V TTL (I2C/UART), 3.3V TTL (SPI)
Струм у режимі читання/запису	120 мА
Струм у режимі очікування	100 мА
Максимальний струм передавача	до 150 мА

Продовження таблиці 3.6

Параметр	Значення
Робоча частота	13.56 МГц
Типова дистанція зчитування	5 – 7 см (залежно від антени)
Об’єм пам’яті	40 KB ROM, 1 KB RAM
Робочий температурний діапазон	-30°C до +85°C
Розміри модуля	51 x 25.5 мм

Розглянувши технічні характеристики та режими живлення модуля, переходимо до аналізу безпеки та вразливостей ідентифікаторів, адже саме це впливає на кінцеву безпеку даних користувачів. Найбільш розповсюджені картки MIFARE Classic, що працюють за протоколом ISO/IEC 14443A [6], використовують алгоритм шифрування Crypto-1. Цей алгоритм складається з 48-бітного ключа та регістру зсуву з лінійним зворотним зв’язком LFSR [35]. У табл. 3.7 наведено усі типи атак, які потенційно можуть бути направлені на картки MIFARE Classic [35].

Таблиця 3.7 – Основні вразливості та типи атак да ідетифікатори

Тип атаки	Принцип реалізації	Особливості та наслідки
Darkside	Базується на експлуатації слабкості генератора псевдовипадкових чисел (PRNG). Стан LFSR відновлюється шляхом аналізу відповідей картки на неправильні запити автентифікації.	Дозволяє здійснити злам системи та отримати доступ без знання жодного ключа.
Nested та Hardnested	Реалізується через аналіз кореляції між зашифрованими відповідями різних секторів пам'яті картки.	Вимагає знання хоча б одного ключа від будь-якого сектора. Дозволяє обчислити всі інші ключі та отримати повний доступ до даних.
Клонування UID	Використовуються спеціальні картки, де можна перезаписувати нульовий блок пам'яті (який за стандартом є незмінним). Модуль PN532 надсилає команди розблокування.	Дозволяє записати довільний UID та створити ідеальний клон оригінального ідентифікатора.

Щоб уникнути вразливостей стандарту Classic, необхідно застосувати комплексний підхід. Першим кроком є перехід на захищені ідентифікатори MIFARE стандарту DESFire версії EV3 [36]. Такі картки використовують апаратну реалізацію алгоритмів AES-128 та 3DES для надійного шифрування й взаємної автентифікації

між карткою та зчитувачем [36]. Вони підтримують гнучку файлову систему, де кожен додаток може мати власні ключі та права доступу. Для захисту від атак типу Relay, коли сигнал перехоплюється й передається в реальному часі, створюючи ілюзію фізичної присутності картки поруч із ним, версія EV3 має механізм Transaction Timer, який обмежує час виконання операції [36]. Другим і одним із найефективніших методів захисту є диверсифікація ключів. Замість єдиного статичного ключа для всіх карток системи генерується унікальний ключ на основі UID кожної картки та системного ключа [37]. Процес зазвичай базується на алгоритмі AES-128 у режимі Cipher Block Chaining [37].

Проаналізувавши всі типи атак і способи їх вирішення, ми переконалися, що PN532 у поєднанні з MIFARE DESFire EV3 та диверсифікацією ключів дозволяє створювати системи, стійкі до більшості відомих типів атак, включаючи клонування UID та злам ключів методом перебору.

3.1.3. Вибір комутаційного елемента

Для керування виконавчим механізмом було обрано модуль одноканального реле з номінальною напругою 12 В. Реле виконує функцію силового ключа, який замикає або розмикає коло живлення виконавчого механізму, в ролі якого може виступати електромагнітний або електромеханічний замок із напругою живлення 12 В. Зображення модуля реле зображено на рисунку 3.4 [38].

Рисунок 3.4 – Загальний вигляд модуля одноканального реле

Фундаментом модулю є класичне електромагнітне реле, робота якого базується на силі Лоренца та законах електромагнітної індукції. Коли через обмотку котушки проходить електричний струм, виникає магнітне поле, яке притягує металевий якір, механічно замикаючи або розмикаючи групу контактів.

Модуль являє собою завершений пристрій на друкованій платі з усією необхідною обв’язкою для безпечного керування. Основу складає електромеханічне реле, здатне комутувати струм до 10 А. Оптопара забезпечує гальванічну ізоляцію керуючого кола від силового, а транзисторний драйвер підсилює слабкий сигнал з оптопари до рівня, достатнього для активації котушки. Захист реалізовано через зворотний діод для гасіння імпульсів самоіндукції котушки та резистори для обмеження струму. Детальні технічні характеристики модуля наведені у табл. 3.8. [38]

Таблиця 3.8 – Технічні характеристики модуля одноканального реле

Параметр	Опис та значення
Робоча напруга котушки (VCC)	12 В постійного струму (DC)
Струм споживання (активний стан)	67-68 мА на канал
Напруга керуючого сигналу (IN)	3.3 В - 5 В (сумісність з TTL)
Струм керування (активація)	2 - 10 мА
Логіка спрацювання	Низький рівень
Макс. напруга комутації (AC)	250 В
Макс. напруга комутації (DC)	30 В
Максимальний струм комутації	10 А
Час спрацювання / відпускання	~15 мс / ~10 мс
Розміри	4.5 х 1.8 х 1.8 см або 50 х 26 х 18.5 мм

3.1.4. Вибір засобів індикації та звукового сповіщення

Для відображення поточного стану систему та інформування користувача про результати авторизації використовується комплекс засобів світлової та звукової індикації. Візуальне сповіщення реалізовано за допомогою групи світлодіодів, які встановлюються на кожному пристрої, а саме для входу та виходу по три світлодіоди: червоний, жовтий та зелений. Використання саме цих світлодіодів забезпечує відмінну видимість навіть при інтенсивному зовнішньому освітленні [39]. Основні технічні характеристики обраних світлодіодів наведено у табл. 3.9 [39].

Таблиця 3.9 – Технічні характеристики світлодіодів індикації

Параметр	Значення
Колір світіння	Зелений, червоний, жовтий
Діаметр	5 мм
Тип лінзи	Прозора
Робоча напруга	від 3.0 до 3.4 В
Робочий струм	20 мА
Кут огляду	30 градусів
Сила світла	від 8000 до 10000 мкд

Для звукової індикації було обрано модуль KY-006, що представляє собою пасивний п'єзодинамік, здатний генерувати сигнали різної частоти через ШІМ від мікроконтролера, зображення якого наведено на рисунку 3.5. Це дозволяє відтворювати різні тональності для різних подій, роблячи експлуатацію системи інтуїтивно зрозумілішою [40]. Технічні характеристики звукового модуля KY-006 наведено у табл. 3.10 [40].

Рисунок 3.5 – Загальний вигляд модуля динаміка KY-006

Таблиця 3.10 – Технічні характеристики звукового модуля KY-006

Параметр	Значення
Тип випромінювача	Пасивний п'єзодинамік
Робоча напруга	від 1.5 до 15 В
Струм споживання	25 мА
Діапазон відтворюваних частот	від 1.5 до 2.5 кГц
Звуковий тиск	85 дБ
Робоча температура	від -20 до +70 °C
Кількість контактів	3
Розміри	19 x 16 мм
Вага	3 г

3.1.5. Вибір датчика положення дверей

Для моніторингу фізичного стану дверного полотна було вибрано магнітоконтактний датчик геркона моделі MC-38 [41]. Принцип роботи дуже простий і полягає у взаємодії двох феромагнітних лопатей, які виготовляються зі сплаву нікелю та заліза. Ці лопаті розміщуються всередині скляної колби, заповненої інертним газом під тиском або вакуумом, що повністю виключає можливість окислення контактів або виникнення електричної дуги при комутації низьковольтних сигналів. При піднесенні постійного магніту до корпусу датчика, магнітне поле пронизує лопаті, перетворюючи їх на магнітні диполі, в результаті чого, сили магнітного притягання переборюють механічну пружність лопатей, що призводить до їхнього розмикання [42]. Основні технічні характеристики датчика наведені у табл. 3.11 [41].

Таблиця 3.11 – Технічні характеристики датчика геркона MC-38

Характеристика	Значення
Номінальна робоча напруга	100 — 200 В DC
Тип контакту	Нормально відкритий (NO)
Максимальний струм комутації	100 мА — 500 мА
Максимальна потужність	3 — 10 Вт
Робоча відстань (зазор)	15 — 25 мм
Час спрацьовування	0.45 мс
Час відпускання	0.35 мс
Матеріал корпусу	ABS-пластик
Розмір (датчик та магніт)	27 x 9 x 13 мм
Робочий ресурс	> 1,000,000 циклів

3.1.6. Вибір виконавчого механізму

Останнім повноцінним компонентом розроблюваної системи є виконавчий механізм, який буде обмежувати фізичний доступ, на основі отриманого сигналу від мікроконтролера . Проаналізувавши велику кількість доступних типів замків, було обрано електромагнітний замок моделі ML-180, його вигляд зображено на рисунку 3.6 [43].

Рисунок 3.6 – Загальний вигляд електромагнітного замка ML-180

Вибір моделі ML-180 обґрунтовується вдалим балансом між помірним енергоспоживання та силою утримання у 180 кг, якої цілком достатньо для надійного захисту типових офісних чи навчальних приміщень. Крім того, використання саме такого типу замка є пріоритетним з погляду пожежної безпеки. Завдяки відсутності рухомих механічних елементів, такий пристрій практично не піддається ризику заклинювання, що є критично важливим у надзвичайних ситуаціях. Принцип роботи за схемою fail-safe гарантує, що за будь-якого аварійного знеструмлення будівлі магнітне поле зникне, і замок автоматично звільнить двері для безперешкодної евакуації людей [44]. Технічні характеристики електромагнітного замка ML-180 наведено у табл. 3.12 [43].

Таблиця 3.12 – Технічні характеристики електромагнітного замка ML-180

Характеристика	Значення
Тип пристрою	електромагнітний замок
Сила утримання	180 кг
Напруга живлення	12 В постійного струму
Споживаний струм	350 мА
Матеріал корпусу	анодований алюміній
Робоча температура	від -10 до +55 °C
Габарити	170 x 35 x 20 мм

Варто зауважити, що розроблена система є універсальною, її схемотехніка та алгоритми керування дозволяються використовувати й інші типі запірних механізмів, зокрема електромагнітні або електромеханічні замки за умови їх відповідності параметрам живлення 12 В постійного струму та характеристикам комутаційного елементу, що описані у розділі 3.1.3, табл. 3.8.

3.2. Розробка принципової електричної схеми

Розробка принципової електричної схеми є одним із найвідповідальніших етапів, оскільки від її якості залежить стабільність роботи усієї платформи. У попередньому розділі було обрано основні компоненти, а саме мікроконтролер ESP32 NODEMCU-32S, зчитувачі PN532 RFID/NFC V3, модуль реле, засоби звукової та візуальної індикації, а також датчик положення дверей MC-38. Спершу розглянемо принципові електричні схеми окремих готових компонентів, після чого перейдемо до загальної схеми всієї системи контролю доступу.

3.2.1. Принципова електрична схема модуля ESP32 NODEMCU-32S

Основою системи є модуль ESP32 NODEMCU-32S, який виконує усі обчислення, зчитує дані з датчиків та керує підключеними виконавчими механізмами. Його внутрішня будова складається з кількох логічних блоків, які забезпечують стабільне живлення, зв’язок з персональним комп’ютером чи сервером та зручне виведення контактів для підключення зовнішньою периферії. Принципова електрична схема модуля наведена на рисунку 3.7 [45].

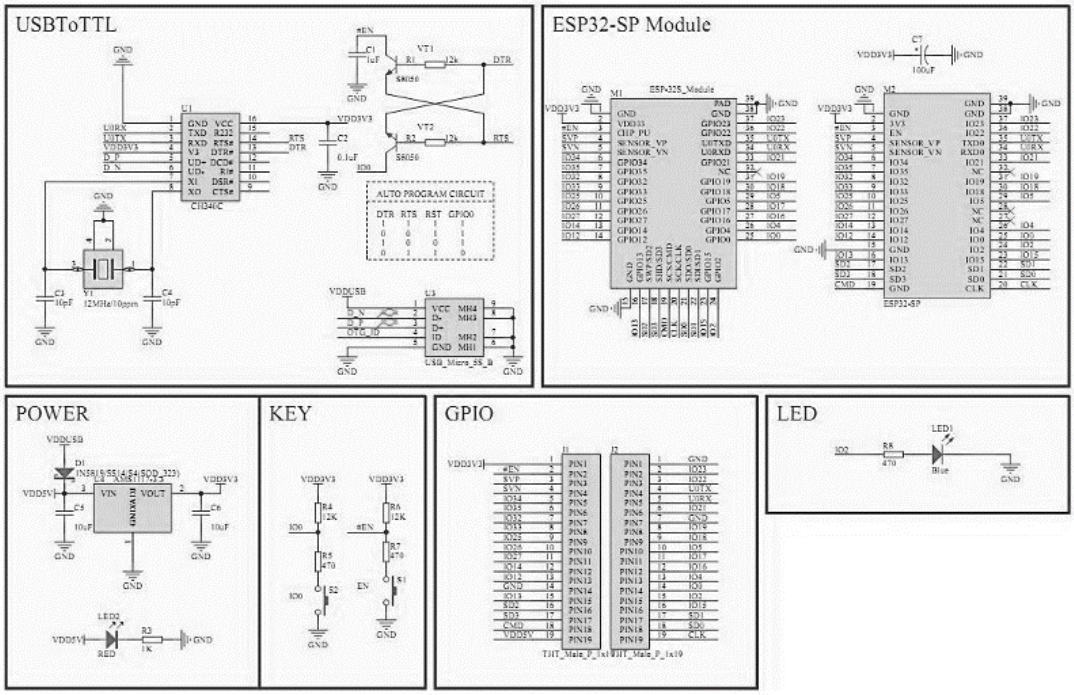

Рисунок 3.7 – Принципова електрична схема ESP32 NODEMCU-32S

На рисунку 3.7 можна побачити функціональні блоки, які відповідають за живлення, зв’язок, керування платою, індикація та центральне ядро, кожен з яких варто розглянути детально.

Блок живлення POWER перетворює вхідну напругу 5 В від порту USB або піну VIN у стабільні 3.3 В за допомогою лінійного стабілізатора AMS1117-3.3. Також для захисту від зворотної полярності на вході схеми встановлено захисний діод D1, а конденсатори C5 та C6 ємністю по 10 мкФ згладжують пульсації струму на вході та виході.

Блок зв’язку USBToTTL реалізовано на базі конвертера CH340C, який перетворює сигнали USB у послідовний інтерфейс UART для програмування та налагодження мікроконтролера. Вбудована транзисторна схема на двох біполярних NPN транзисторах, використовуючи сигнали DTR та RTS, автоматично керує виводами EN та IO0, що дозволяє прошивати мікроконтролер без ручного натискання кнопок на платі.

Центральне ядро плати ESP32-SP Module інтегрує екранований мікроконтролер із двоядерним процесором, енергонезалежною пам’яттю та радіочастотним трактом для забезпечення бездротового зв’язку. На схемі показано маршрутизацію внутрішніх контактів чипа до ліній на платі, зокрема порти загального призначення, контакти АЦП, лінії для роботи з SD-картками та апаратні інтерфейси UART, I2C та SPI. Електролітичний конденсатор C7 ємністю 100 мкФ, встановлений паралельно ланцюгу живлення біля контактів модуля, компенсує різкі стрибки споживання струму та просадки напруги під час активної роботи передавача Wi-Fi.

3.2.2. Принципова електрична схема зчитувача PN532 RFID/NFC V3

Модуль PN532 RFID/NFC V3 використовується для безконтактного зчитування ідентифікаторів, та передавання інформації мікроконтролеру. Його схема побудована на базі мікросхеми PM532, яка відображає підключення вбудованої антени, перемикачів вибору інтерфейсу, перетворювачів логічних рівнів та виводів живлення. Принципова електрична схема модуля наведена на рисунку 3.8 [46].

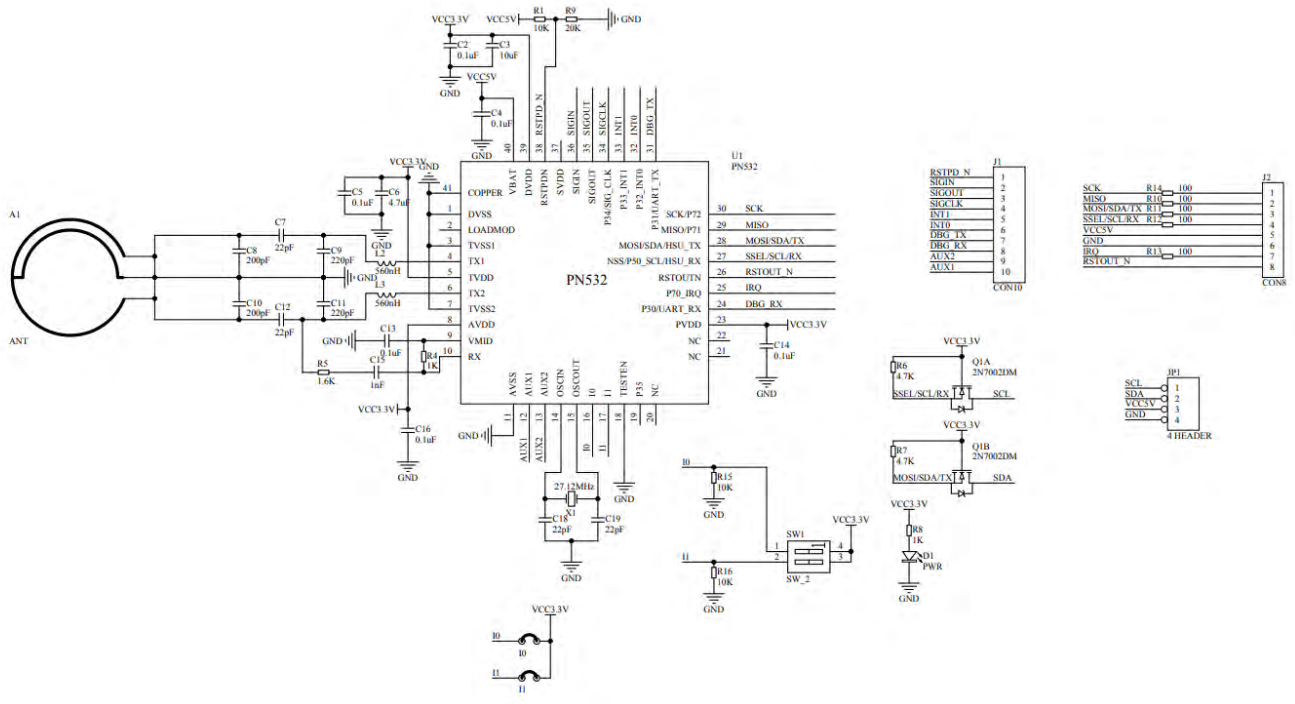

Рисунок 3.8 – Принципова електрична схема модуля PN532 RFID/NFC V3

Центральним елементом схеми є мікросхема PN532, яка відповідає за обробку радіочастотних сигналів та комунікацію з нашим мікроконтролером. Її тактування забезпечує зовнішній кварцовий резонатор X1 на 27.12 МГц, а радіочастотний тракт містить друковану антену A1 та узгоджувальний LC-фільтр для стабільної генерації електромагнітного поля на частоті 13.56 МГц. Вибір робочого інтерфейсу реалізовується через DIP-перемикач, який задає необхідні логічні рівні на конфігураційних виводах мікросхеми. Для сумісності з контролерами різної напруги схема містить двонаправлений перетворювач рівнів на польових транзисторах QA1 та Q1B.

3.2.3. Принципова електрична схема модуля перетворювача Mini-360 MP2307

Живлення логічної частини системи забезпечує модуль понижуючого DC-DC перетворювача Mini-360 MP2307. У системі він відповідає за ефективне перетворення вхідної напруги 12 В у стабільну 5 В для живлення плати мікроконтролера ESP32. Принципова електрична схема модуля наведена на рисунку 3.9 [47].

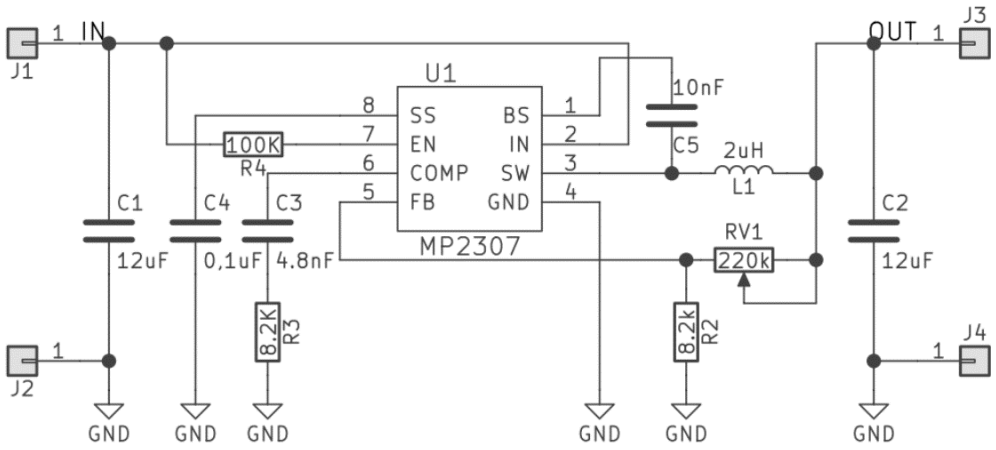

Рисунок 3.9 – Принципова електрична схема модуля Mini-360 MP2307

Схема побудована на синхронному понижуючому перетворювачі MP2307. На його вхід подається нестабілізована напруга, згладжена конденсатором C1. Автоматичний запуск при подачі живлення забезпечує з’єднання виводу EN із вхідною лінією через підтягуючий резистор R4. Стабілізована вихідна напруга з мінімальними завадами формується згладжувальним LC-контуром із дроселя L1 та керамічного конденсатора C2. При чому точне налаштування вихідної напруги на необхідний рівень 5 В здійснюється за допомогою дільника у ланцюзі зворотного зв’язку на виводі FB, який містить постійний резистор R2 та підлаштовуваний резистор RV1.

3.2.4. Принципова електрична схема модуля динаміка KY-006

Звукова індикація реалізується через модуль пасивного п’єзодинаміка KY-006, який підключається до мікроконтролера напряму, без додаткових підсилювачів. Оскільки п’єзоелемент не має вбудованого генератора частоти, мікроконтролер формує звукові сигнали будь-якої тональності за допомогою ШІМ. Сигнальний вивід модуля підключається до цифрового порту мікроконтролера, а інший до загальної шини заземлення. Робочого струму цифрового порту цілком достатньо для розгойдування мембрани, що робить схему технічно виправданою без зайвих компонентів [40].

3.2.5. Принципові електрична схема комутаційного елемента

Керування електромагнітним замок здійснює комутаційний елемент, в ролі якого виступає модуль одноканального реле, який забезпечує надійну комутацію струмів до 10 А та повну гальванічну розв’язку між чутливою логічною частиною мікроконтролера і силовим ланцюгом 12 В. Принципова електрична схема модуля наведена на рисунку 3.10 [38].

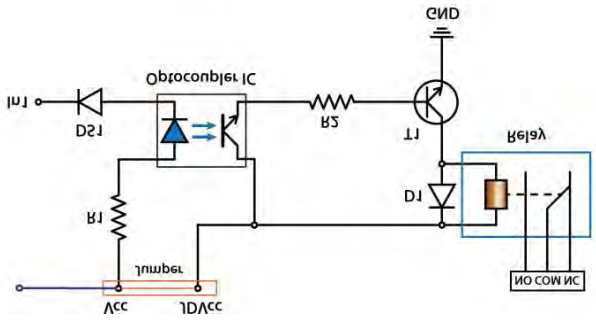

Рисунок 3.10 – Принципова електрична схема модуля реле

Безпеку модуля забезпечує оптопара, яка фізично розділяє керуючий сигнал та ланцюг живлення котушки реле, передаючи команду через світловий потік. Модуль працює за інверсивною логікою активного низького рівня, тобто для активації реле мікроконтролер має подати на вхід ln1 логічний нуль. Захисний діод D1, встановлений паралельно котушці у зворотному напрямку, захищає керуючий транзистор T1 від пробою струмами самоіндукції, які неминуче виникають під час відключення індуктивного навантаження. Комутація електромагнітного замка здійснюється через вихідні контакти реле, де задіяні загальний вивід COM та нормально закритий контакт NC, що відповідає вимогам пожежної безпеки та гарантує розблокування дверей при аварійному знеструмлені.

3.2.6. Побудова загальної принципової електричної схеми

Загальна принципова електрична схема об’єднує всі розглянуті модулі та додаткові електронні компоненти в єдину функціональну систему контролю доступу. Вхідна напруга живлення 12 В подається від зовнішнього джерела через роз’єм

живлення XS1. Для стабільної роботи системи, надійного утримання електромагнітного замка та запобігання просідання напруги, зовнішній блок живлення повинен забезпечувати номінальний струм не менше 2 А. Для згладжування пульсацій струму та забезпечення стабільної роботи електромагнітного замка на вході встановлено електролітичний конденсатор C1 ємністю 1000 мкФ (25 В), від якого силова лінія 12 В розгалужується на вхід модуля понижуючого перетворювача mini-360 MP2307 (A1) та комутаційні контакти модуля KV1. На виході перетворювача A1 формується стабілізована напруга 5 В, яка додатково фільтрується конденсатором C2 ємністю 470 мкФ (16 В) і подається безпосередньо на вхід живлення мікроконтролера, що має позиційне позначення DD1, який в свою чергу живить модуль реле.

Центральний мікроконтролер DD1 керує всією периферією, живлячи її логічною напругою 3.3 В зі свого внутрішнього лінійного стабілізатора. До цієї шини живлення підключені два модулі зчитування PN532 (A2 та A3), які обмінюються даними з мікроконтролером по інтерфейсу I2C через різні апаратні порти, щоб уникнути програмного конфлікту адрес.

Система візуальної індикації складається з шести світлодіодів діаметром 5мм. Червоні D1 та D4 підключені через струмообмежувальні резистори R1 та R4 номіналом 1000 Ом для оптимальної яскравості. Жовті D2, D5 та зелені D3, D6 підключені через резистори R2, R5 та R3, R6 номіналом 220 Ом. Звукове сповіщення забезпечують два модулі динаміків KY-006 із позначенням BF1 та BF2.

Моніторинг фізичного стану дверей виконується за допомогою мігнітоконтактного датчика геркона SF1, який підключається між входом мікроконтролера та спільною шиною заземлення. Керування електромагнітним замком YA1 здійснюється через гвинтовий клемний XT1 та нормально закритий контакт реле KV1, що апаратно гарантує пожежну безпеку об’єкта. Для захисту ланцюгів від струму самоіндукції котушки замка паралельно клемам XT1 у зворотному включенні встановлено випрямний діод VD1.

Усі описані з’єднання, логічні зв’язки та позиційні позначення застосованих компонентів детально відображені на рисунку 3.11 та у ДОДАТКУ А. Разом з тим

відповідна специфікація з повним переліком використаних елементів міститься окремо у ДОДАТКУ Б.

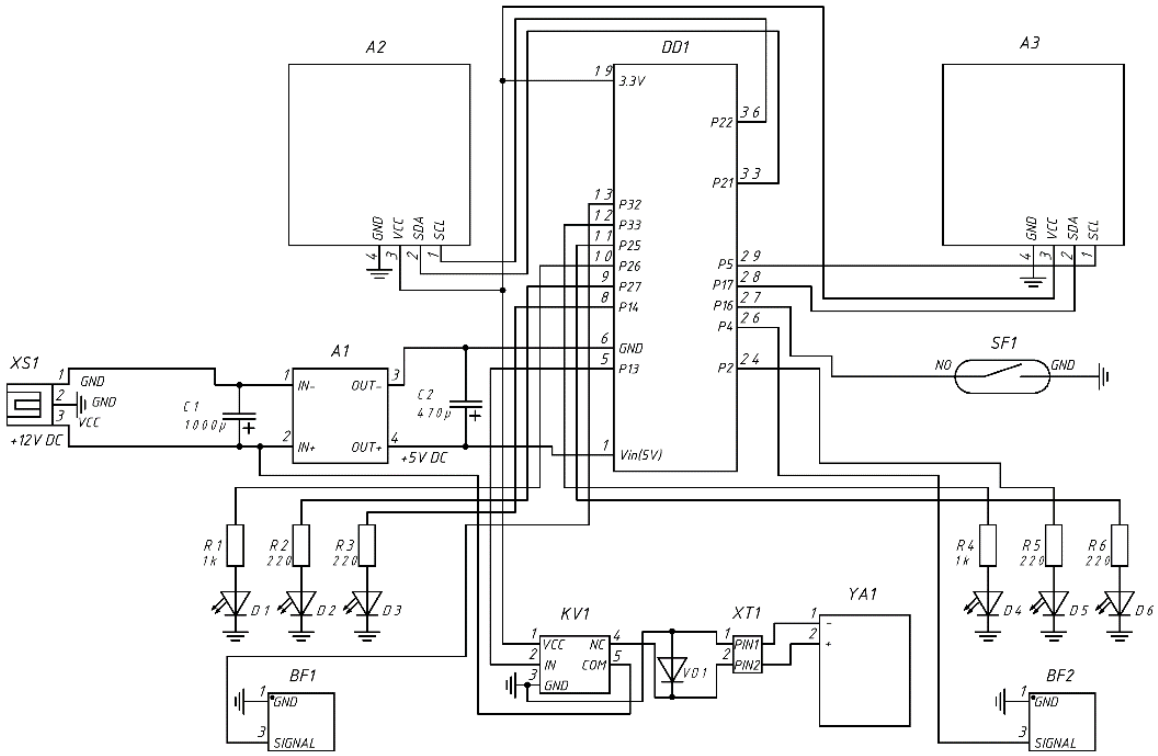

Рисунок 3.11 – Принципова електрична схема автоматизованого пристрою контролю доступу до приміщень

Висновки до розділу 3

У цьому розділі було сформовано апаратну частину системи контролю доступу та розроблено її принципову електричну схему. Центральним контролером обрано ESP32 NODEMCU-32S, який відповідає вимогам щодо збору інформації та мережевої взаємодії з сервером. Поєднання зчитувачів типу PN532 V3 разом із датчиком стану дверей МС-38 сформувало надійний контур ідентифікації та фізичного моніторингу об’єкта. Електромагнітний замок та модуль реле з опторозв’язкою гарантують безпечну комутацію силових ланцюгів.

Аналіз схем окремих модулів дозволив обґрунтувати їхнє застосування на апаратному рівні, а загальна принципова схема об’єднала всі вузли в єдиний комплекс зі стабілізацією живлення. У підсумку отримано надійну архітектуру, яка вирізняється модульністю, захищеністю та легкістю у подальшій модернізації.

РОЗДІЛ 4. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Створення програмного забезпечення є ключовим та найвідповідальнішим етапом розробки системи контролю доступу, адже від його якості залежить стабільність роботи та зручність використання для кінцевого користувача. Відповідно до розробленої архітектури у минулих розділах, програмна частина системи розділена на два автономні блоки, які функціонують разом. Головна задача створити програмне забезпечення мікроконтролера, розробити серверну частину з базою даних та користувацький веб-інтерфейс.

4.1. Вибір та обґрунтування стека технологій

Перед написанням будь-якого коду, перш за все потрібно визначитись зі стеком технологій, адже від цього залежить швидкість, зручність та можливість розширення нашої системи. Для програмування мікроконтролера ESP32 було обрано мову C++, розробка на якій здійснюється в інтегрованому середовищі Arduino IDE [48]. Вибір мови зумовлений тим, що вона є стандартною для програмування мікроконтролерів типу ESP32, а середовище розробки Arduino IDE забезпечує її повну підтримку. Це дозволяє суттєво прискорити процес написання внутрішньої прошивки, завдяки наявності великої кількості готових і перевірених бібліотек для взаємодії з периферійними модулями та мережами.

Для створення серверної частини та інтерфейсу користувача було обрано сучасний фреймворк Next.js [49], який функціонує разом із бібліотекою React [50]. Розробка всього проєкту ведеться з використанням мови TypeScript [51], яка додає строгу типізацію даних, що дозволяє виявити помилки прямо під час написання коду. Також мова TypeScript додає можливість створення типів, інтерфейсів та дженериків, що дозволяє використовувати функції з різними типами вхідних даних, що значно економить ресурси. Варто додати, що вибір Next.js є стратегічним інженерним рішенням, оскільки дана платформа дозволяє реалізувати концепцію

монорепозиторія, де серверна бізнес-логіка та клієнтська частина розробляється в межах одного проєкту, спрощуючи підтримку, тестування та розгортання системи.

Важливим етапом проєктування архітектури є вибір типу бази даних для надійного збереження інформації. Наразі в інженерній практиці основними підходами є використання реляційних SQL та нереляційних NoSQL систем управління базами даних. Нереляційні рішення мають такі переваги, як гнучка структура документів та висока швидкість горизонтального масштабування, проте їхніми недоліками виступають відсутність суворої типізації зв'язків та складність забезпечення цілісності даних при паралельних запитах [52]. Реляційні бази даних в свою чергу характеризуються наявністю чіткої схеми та повною відповідністю вимогами ACID [52], [53] (атомарність, узгодженість, ізольованість, довговічність), що гарантує високу точність фіксації подій. Оскільки система контролю доступу вимагає суворого логічного зв'язку між профілями користувачів, апаратними пристроями та журналом транзакцій без ризику втрати чи викривлення інформації, для реалізації проєкту було обрано саме реляційну модель бази даних [52], [53].

Взаємодія з обраною базою даних організована за допомогою сучасного інструменту об'єктно-реляційного відображення Prisma ORM [54]. Використання Prisma дозволяє повністю відмовитися від ручного написання складних SQL-запитів, замінюючи їх об'єктно-орієнтованими методами. Основною системою для написання та відлагодження всього коду нашого додатку було обрано інтегроване середовище розробки WebStorm [55], яке має потужні інструменти автоматичного рефакторингу та статичного аналізу TypeScript.

4.2. Розробка програмного забезпечення мікроконтролера

Внутрішня прошивка мікроконтролера розробляється з урахуванням того, що пристрій повинен працювати безперервно та стабільно, забезпечуючи виконання алгоритмів автентифікації, координацію роботи виконавчих механізмів, обробку сигналів від периферійних пристроїв та підтримання стабільного мережевого зв'язку із сервером у режимі реального часу.

4.2.1. Алгоритм звукової індикації

Функція startBeep запускає апаратну генерацію ШІМ-сигналу через метод ledcAttach і одразу фіксує в глобальній змінній розрахований час, коли звучання має припинитись. Сама зупинка сигналу відбувається асинхронно в головному циклі програми через регулярний виклик функції handleBuzzer. Щойно поточний час збігається зі збереженим лічильником мілісекунд, генерація вимикається. Такий підхід дозволяє процесору не блокуватися на час звучання і спокійно утримувати мережеве з’єднання навіть під час довгих сигналів тривоги. Послідовність усіх дій зображена на рисунку 4.1.

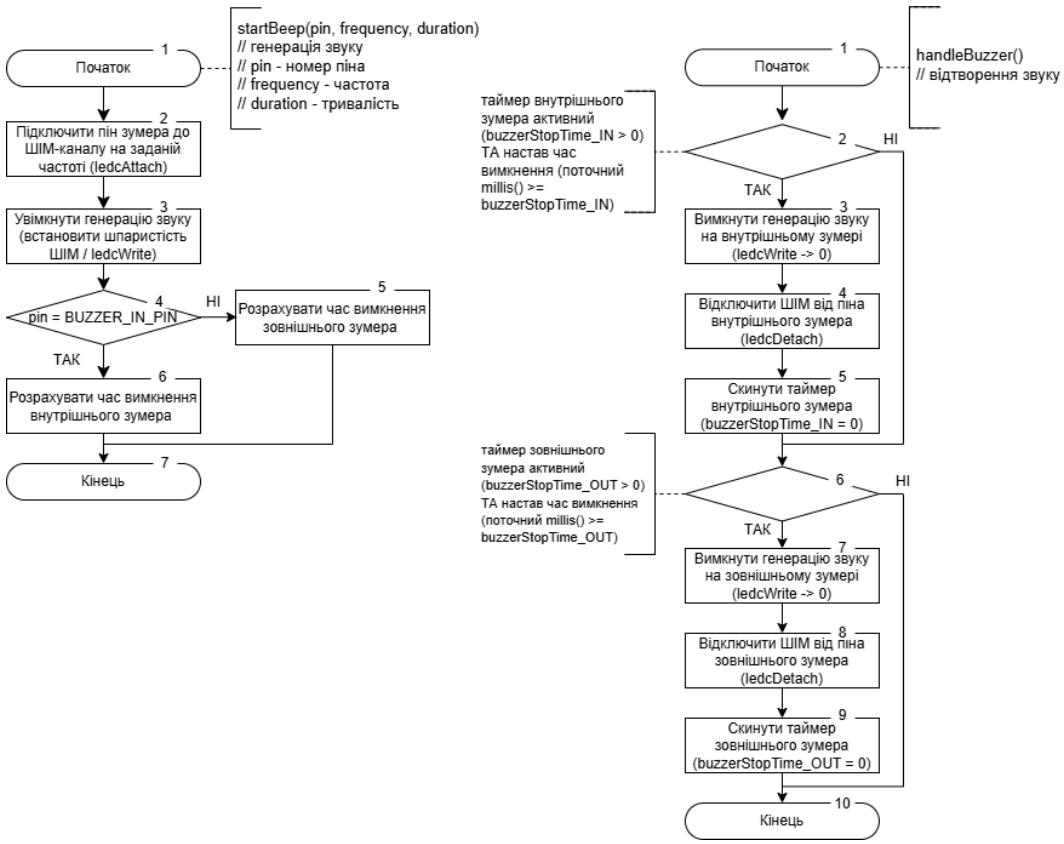

Рисунок 4.1 – Блок-схема алгоритму функції startBeep

4.2.2. Алгоритм скидання стану світлової індикації

Службова функція ledsOff призначена для повного очищення поточного стану світлодіодних індикаторів перед зміною експлуатаційних режимів системи. Робота

алгоритму полягає у послідовному переведенні всіх шести цифрових пінів, відповідальних за світлодіоди, у низький логічний рівень. Це забезпечує одночасне їх вимкнення, що дозволяє уникнути накладання сигналів при зміні режимів. Блок-схема алгоритму наведена на рисунку 4.2.

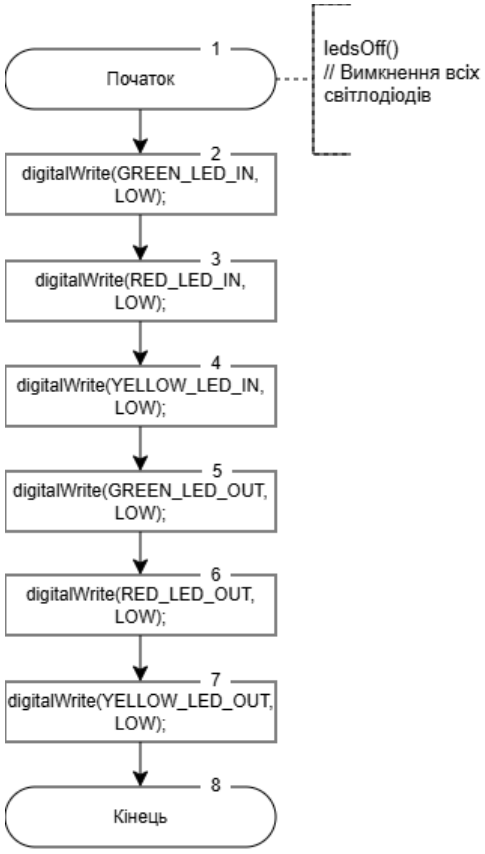

Рисунок 4.2 – Блок-схема алгоритму функції ledsOff

4.2.3. Алгоритм фізичного керування замком

Точка доступу переводиться у безпечний зачинений стан функцією lockDoor. Спершу вона перевіряє глобальну змінну currentRelayType, щоб визначити тип виконавчого механізму. Якщо замок працює за схемою NC нормально-зачинений, на керуючий вивід реле йде низький логічний рівень, що знеструмлює котушку. Якщо ж замок налаштовано як нормально-відкритий NO, на вивід подається високий логічний рівень. Далі функція скидає прапорець розблокування дверей, а саме змінну isDoorUnlocked, яка тепер має значення false, вимикає світлову індикацію та фіксує подію в журналі подій. Блок-схема алгоритму наведена на рисунку 4.3.

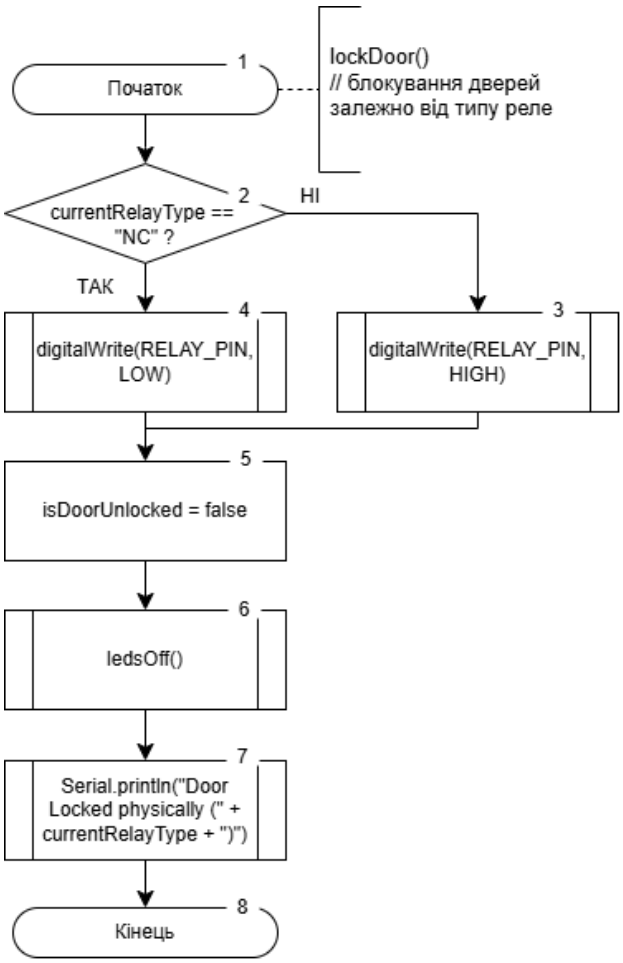

Рисунок 4.3 – Блок-схема алгоритму функції lockDoor

4.2.4. Алгоритм ініціалізації та конфігурації

Функція fetchConfiguration виконує HTTPS GET-запити до сервера, щоб отримати базові налаштування. Завдяки бібліотеці HTTPClient [56] потік не зависає навіть за відсутності відповіді. JSON, що повертається, десеріалізується через JsonDocument з ArduinoJson [57], який сам розподіляє пам’ять під структуру даних. Отримані параметри часу затримки й типу реле застосовуються фізично через виклик функції lockDoor, але лише за умови, що двері не повинні бути легально розблокованими. Це вберігає користувача від випадкового блокування саме в той момент, коли оновлюються налаштування. Блок-схема алгоритму наведена на рисунку 4.4.

Рисунок 4.4 – Блок-схема алгоритму функції fetchConfiguration

4.2.5. Алгоритм надання доступу

Після успішної авторизації функція accessGranted активує виконавчий механізм замка разом із світловою індикацією. Алгоритм спочатку визначає напрямок проходу, ENTRY чи EXIT, і вмикає відповідні зелені світлодіоди. Далі спрацьовує адаптивне керування реле, воно зчитує конфігураційний тип замка, NO або NC, і подає на керуючий пін логічну одиницю чи нуль залежно від цього. Коли замок розблоковано, система переводить прапорець очікування проходу в активний стан, запускає таймер

й генерує короткий звуковий сигнал підтвердження. Блок-схема алгоритму наведена на рисунку 4.5.

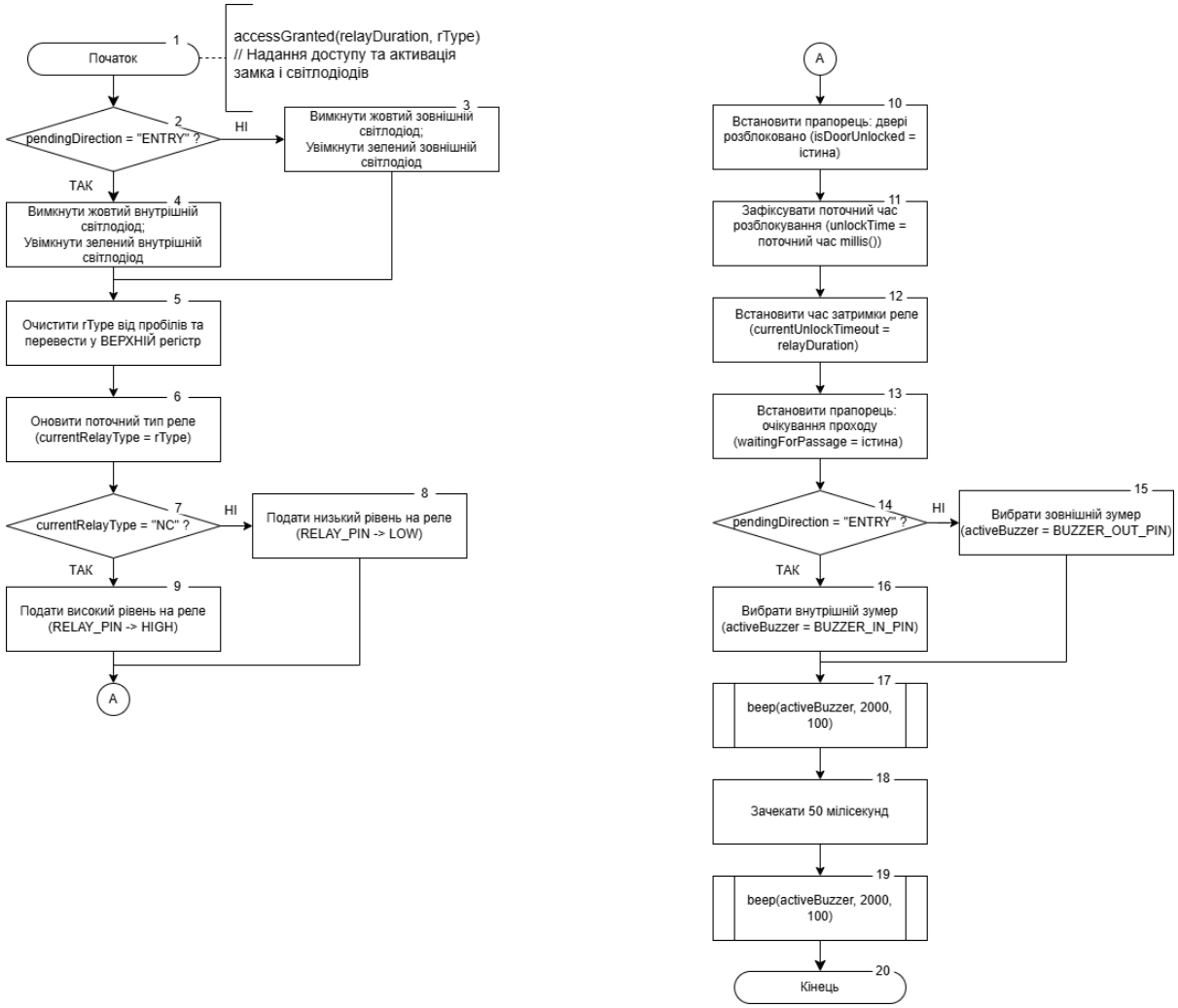

Рисунок 4.5 – Блок-схема алгоритму функції accessGranted

4.2.6. Алгоритм відмови у доступі

Створена функція реалізує алгоритм реагування на піднесення неавторизованої або заблокованої картки. Система вмикає червону індикацію на відповідній стороні точки доступу й одразу генерує низькочастотний сигнал помилки. Щоб уникнути зависання процесора при швидкому циклічному прикладанні невідомої мітки до зчитувача, функція працює асинхронно, вона лише встановлює прапорець стану і фіксує поточний час, а вся подальша обробка триває у фоновому режимі. Блок-схема алгоритму наведена на рисунку 4.6.

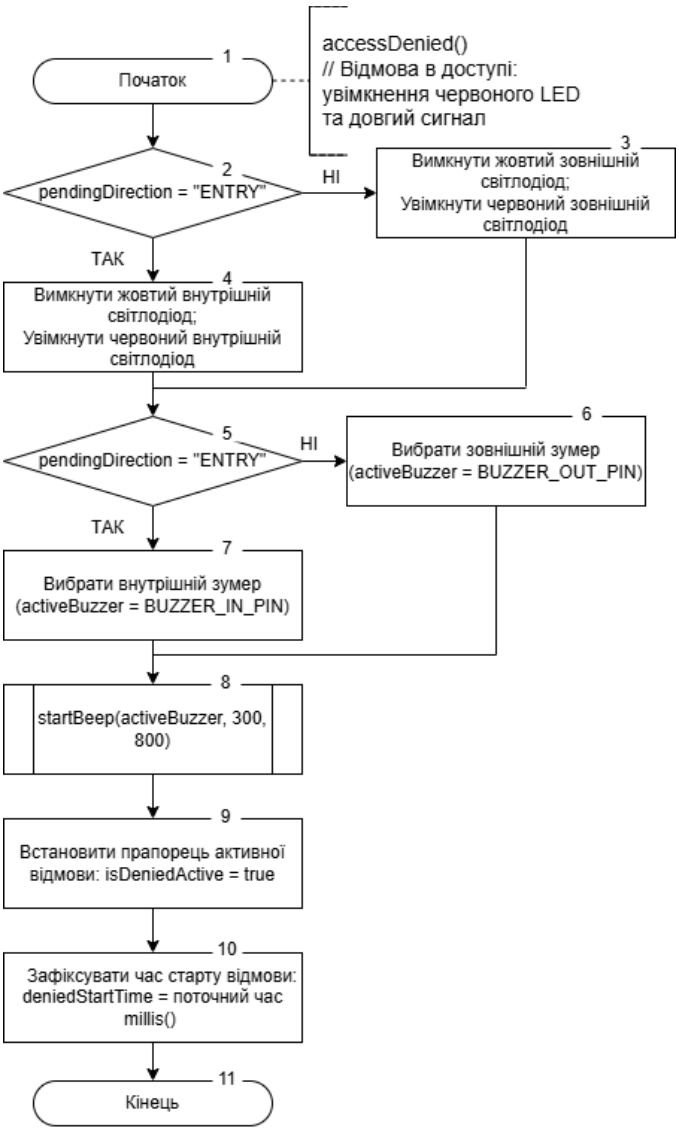

Рисунок 4.6 – Блок-схема алгоритму функції accessDenied

4.2.7. Алгоритм обробки мережевих подій

Функція забезпечує асинхронний двосторонній обмін пакетами між мікроконтролером і сервером, побудований за моделлю кінцевого автомата [58]. Для захисту від DoS-атак [59] вхідні текстові пакети, що перевищують 1024 байти, відкидаються ще до етапу десеріалізації. Далі обробник класифікує серверні команди. ACCESS_RESPONSE відповідає за верифікацію карток, UNLOCK виконує віддалене відкриття замка, а START_SCAN ініціалізує режим реєстрації міток. Окремо стоїть IPDATE_CONFIG, яка просто встановлює прапорець очікування налаштувань, а сам HTTP-запит делегується головному циклу loop, щоб уникнути взаємоблокування

мережевих потоків. Блок-схема алгоритму обробки мережевих подій наведена у ДОДАТКУ В.

4.2.8. Ініціалізація апаратної частини

Початкове налаштування мікроконтролера, периферії та мережевих з’єднань виконується одразу після подачі живлення. Щоб апаратно захистити силове реле від небажаного імпульсу в момент завантаження, спершу на керуючий пін подається сигнал блокування, і лише потім він переводиться в режим pinMode(OUTPUT). Робота з двома зчитувачами PN532 організована через дві незалежні шини, після чого для обох активується режим SAMConfig. Далі контролер підключається до мережі через WIFIManager [60], проводить HTTP-синхронізацію налаштувань і відкриває WebSocket-сесію для подальшого обміну даними. Блок-схема алгоритму наведена на рисунку 4.7.

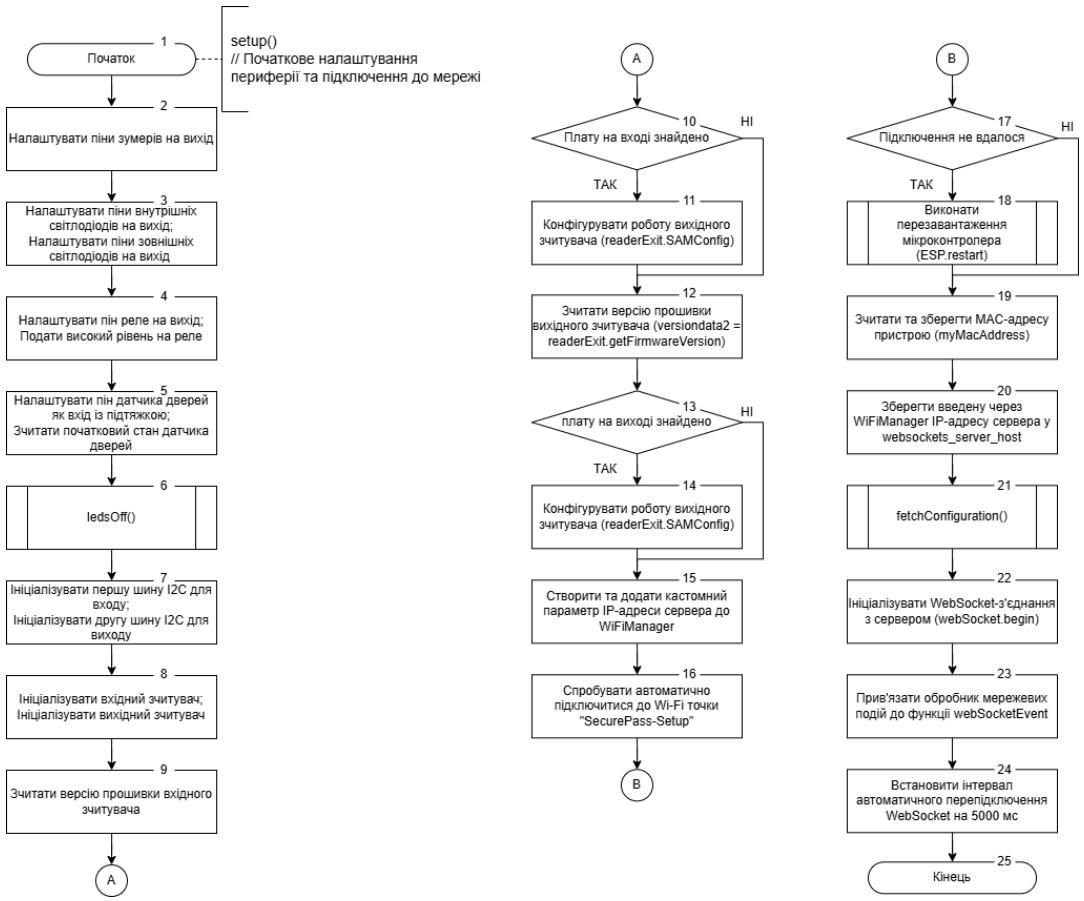

Рисунок 4.7 – Блок-схема алгоритму функції setup

4.2.9. Алгоритм головного циклу контролю периферії

Цей блок працює як диспетчер завдань, безперервно опитуючи датчик й не блокуючи процесор. Щойно змінюється стан датчика стану дверей, системи генерує пакет DOOR_EVENT. Безпечна фіксація легального проходу формує пакет PASSAGE_CONFIRMED разом із UID картки, причому з пам’яті цей UID видаляється лише після того, як пакет успішно доставлено мережею. Якщо ж двері відкриваються без авторизації, негайно ініціюється пакет INTRUSION_ALERT і вмикається режим світлової та звукової сирени. Опитування шини I2C для модулів PN532 виконується методом readPassiveTargetID із жорстким тайм-аутом у 20 мілісекунд, що дозволяє звести затримки циклу до мінімуму, коли карток поблизу немає. Блок-схема алгоритму наведена у ДОДАТКУ Д.

4.3. Розробка серверної частини та бази даних

Серверна частина системи координує роботу всіх апаратних точок доступу, обробляє клієнтські запити з веб-інтерфейсу та веде централізований облік подій. Усе це побудовано на базі Node.js [61]. Це середовище добре справляється з великою кількістю одночасних підключень від пристроїв завдяки своїй асинхронній природі.

Для надійного зберігання даних і чіткого дотримання транзакцій використовується база даних PostgreSQL [62]. Взаємодія з нею на рівні коду відбувається через інструмент Prisma ORM [54], який дає змогу писати строго типізовані запити й загалом підвищує надійність роботи з даними. Логічну структуру бази, типи полів і реляційні зв’язки між таблицями наочно показано на рисунку 4.8.

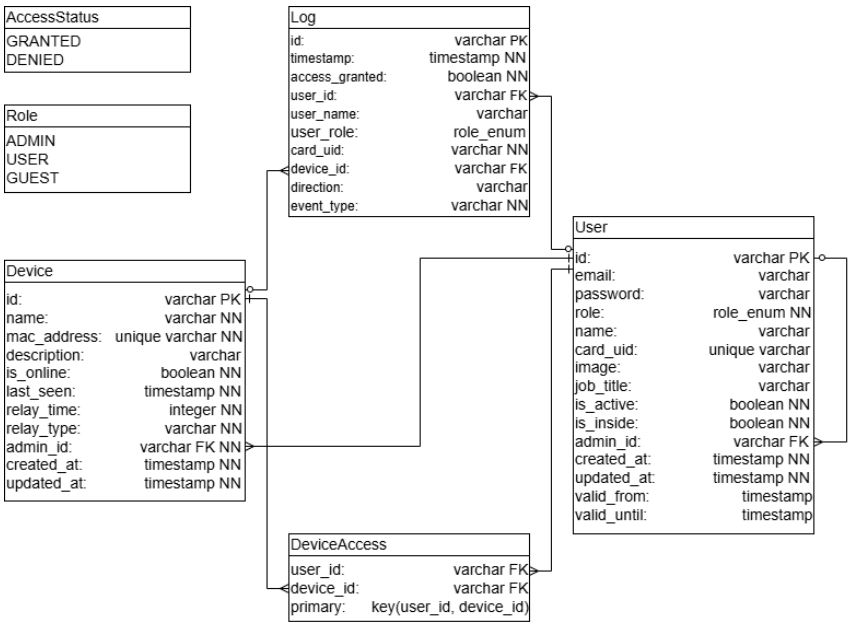

Рисунок 4.8 – ER-діаграма розробленої бази даних

Рисунок 4.8 показує, що архітектура бази даних спирається на три основні сутності. Таблиця пристроїв зберігає MAC-адреси мікроконтролерів, назви локацій, статуси підключення та апаратні налаштування реле. Таблиця користувачів об’єднує облікові записи персоналу й гостей із прив’язкою UID карток, статусом поточного місцеперебування та часовими лімітами. Журнал доступу реляційно пов’язує ці дані, фіксуючи кожну операцію. Щоб забезпечити цілісність обліку безпеки, в цій таблиці реалізовано архітектурний патерн знімка даних, тому ім’я та роль особи автоматично копіюються в момент проходу, завдяки чому історія зберігається навіть після повного видалення профілю з системи.

Для взаємодії в реальному часі в систему інтегровано окремий WebSocket-сервер, який ми обрали в минулих розділах. Написаний він мовою TypeScript із використанням бібліотеки ws [63]. Після запуску він переходить у режим прослуховування й постійно утримує список активних з’єднання з точками доступу. Завдяки цьому сервер може миттєво надсилати команди на мікроконтролери, не чекаючи запиту з їхнього боку. Щоб мережа залишалася стабільною, додатково працює механізм перевірки активності, тому кожні 10 секунд він автоматично опитує пристрої й оновлює їхні мережеві статуси у базі даних.

Головним обчислювальним процесом серверної частини є логіка перевірки доступу, яка запускається, щойно від мікроконтролера надходить код ідентифікатора. Сервер послідовно проходить такі кроки.

1. Спочатку виконується ідентифікація: WebSocket-пакет парситься, з нього дістаються UID картки, MAC-адреса пристрою та напрямок руху.
2. Далі йде валідація по базі даних: Через PRISMA ORM надсилається запит на пошук користувача за вказаним UID і перевіряється, чи прив'язаний він до цього пристрою, тобто чи дозволені йому ці двері.
3. Після цього перевіряються часові ліміти. Для ролі GUEST система звіряє поточний час сервера із заданими межами validFrom та validUntil.
4. Наступним кроком є anti-passback контроль. Система перевіряє наявність всередині, щоб запобігти повторному входу за однією карткою без попереднього виходу. Це захищає від ситуації, коли перепустку передають іншій особі.
5. Нарешті виконуються логування та отримання відповіді. Якщо всі перевірки пройдені успішно, сервер записує подію в журнал як дозволену, оновлює локацію користувача й відправляє на мікроконтролер команду відкриття. Якщо ж порушується будь-яка з умов, формується запис про відмову в доступі.

Окрім фізичного доступу за картками, сервер обробляє команди віддаленого відкриття дверей з персонального кабінету співробітника. Також WebSocket-сервер виконує роль інформаційного мосту для веб-інтерфейсу, здійснюючи розсилку подій підключеним клієнтам, завдяки чому графіки й статус дверей оновлюються миттєво.

4.4. Розробка веб-інтерфейсу

Клієнтський рівень системи представлений інтерактивним веб-інтерфейсом, який побудований на компонентному підході бібліотеки React [50] у поєднанні з архітектурою Next.js App Router [49]. Інтерфейс чітко розділено на клієнтські

компоненти, які обробляють інтерактивні стани, анімації та модальні вікна, і серверні компоненти, що відповідають за безпечну вибірку даних на стороні бекенду. Навігація між основними функціональними модулями реалізована через адаптивне бокове меню, яке динамічно змінює свій вміст і доступність розділів залежно від ролі автентифікованого користувача. Застосунок доступний за доменом diploma-vereshko.vercel.app.

Публічна стартова сторінка

Точкою входу для неавторизованих користувачів слугує публічна стартова сторінка. На ній розміщено загальний опис можливостей системи, його архітектурні переваги та інструкції з інтеграції. Головне завдання цього екрану полягає в тому, щоб дати користувачеві вибір. Він може перейти до форми авторизації, якщо вже є співробітником або адміністратором, або зареєструвати нову компанію. Весь внутрішній функціонал системи закритий захищеними маршрутами на рівні проміжного програмного забезпечення middleware [64], допоки не буде успішно перевірено криптографічно підписаний JWT-токен сесії [65], а якщо користувач реєструється, його створений пароль хешується за допомогою бібліотеки bcryptjs [66], щоб зберегти надійність його зберігання. Після авторизації цей токен безпечно зберігається в браузері клієнта через механізм HTTP-only cookies. Інтерфейс публічної сторінки зображено на рисунку 4.9, а форми реєстрації та логіну на рисунку 4.10.

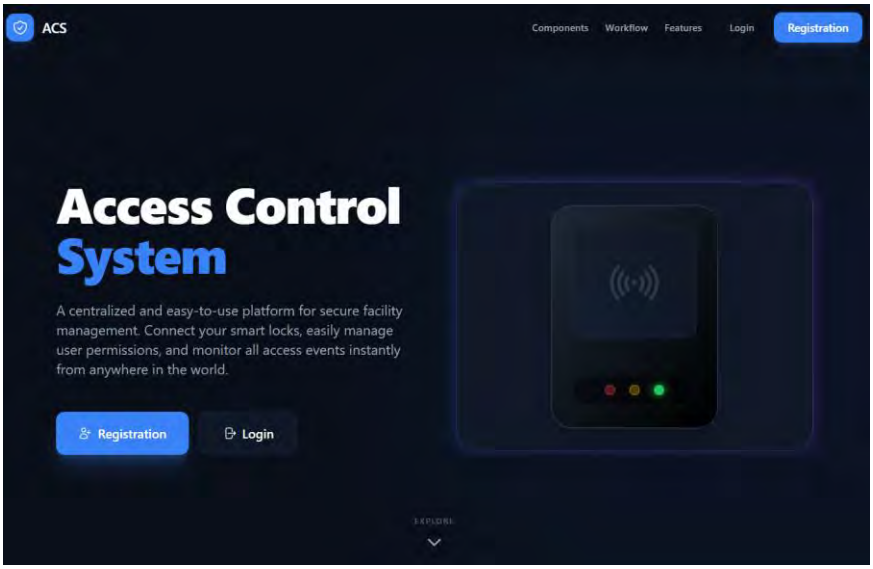

Рисунок 4.9 – Інтерфейс публічної сторінки застосунку

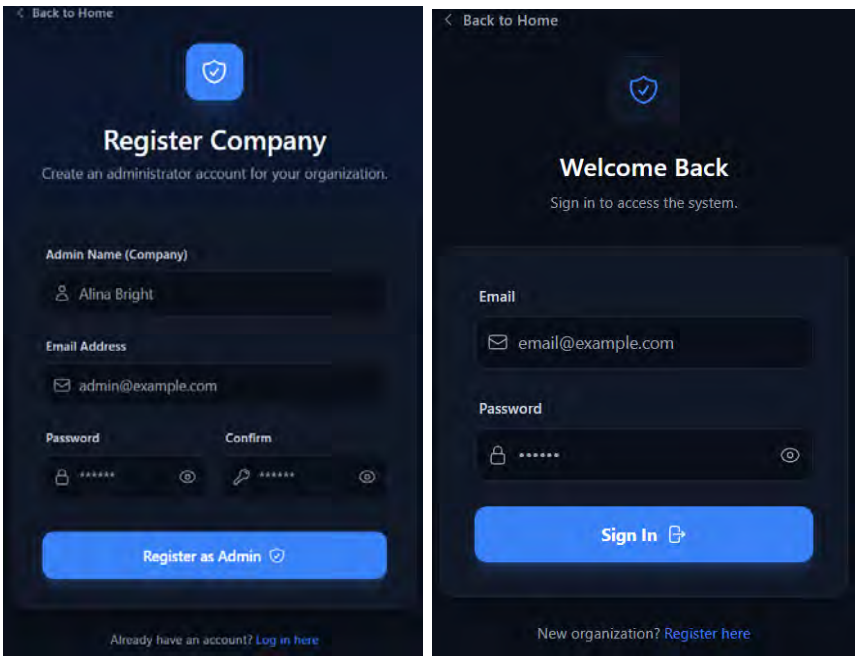

Рисунок 4.10 – Інтерфейс форм реєстрації та логіну

Головна панель

Цей розділ є внутрішньою стартовою сторінкою, яка відкривається одразу після успішної перевірки JWT-токена. Інтерфейс панелі кардинально відрізняється залежно від ролі особи. Для адміністратора тут реалізовано блок глобальної аналітики, а саме інформаційні картки із сумарною статистикою та інтерактивні графіки, які візуалізують пікові години активності й безпекові інциденти. Окремим віджетом виведено статус підключених пристроїв, що показує роботу мікроконтролерів і фізичний стан дверей. Також присутня стрічка останніх подій, яка завдяки WebSocket оновлюється в реальному часі. Для швидкого завантаження сторінки застосовано динамічний імпорт даних та скелетне завантаження.

Якщо ж у систему входить звичайний співробітник, він бачить персоналізовану версію панелі. Глобальна аналітика приховується, натомість відображається його цифровий профіль із поточним статусом локації та список дозволених точок доступу. Працівник бачить лише ті двері, до яких йому надано права, і може віддалено розблокувати їх за допомогою віртуальної кнопки. Вигляд сторінки dashboard для адміністратора та працівника наведено на рисунках 4.11, 4.12 та 4.13 відповідно.

Рисунок 4.11 – Інтерфейс головної панелі адміністратора

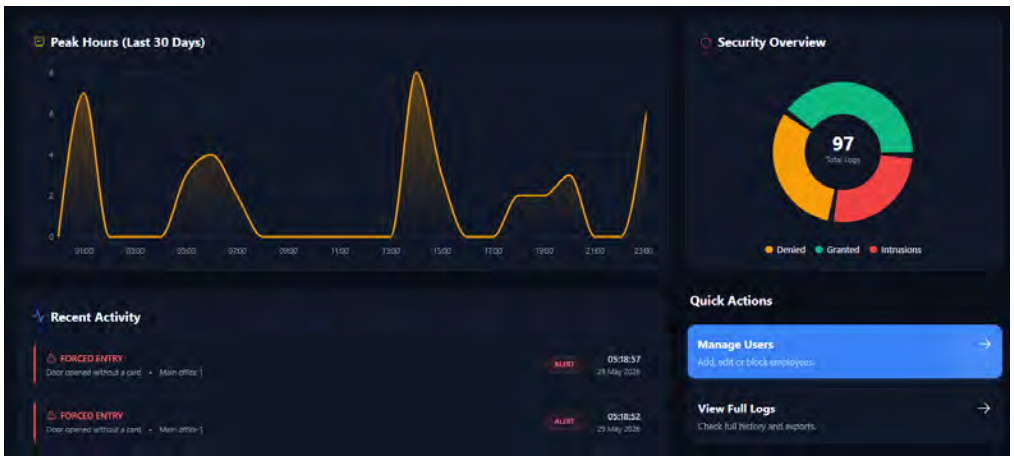

Рисунок 4.12 – Продовження інтерфейсу головної панелі адміністратора

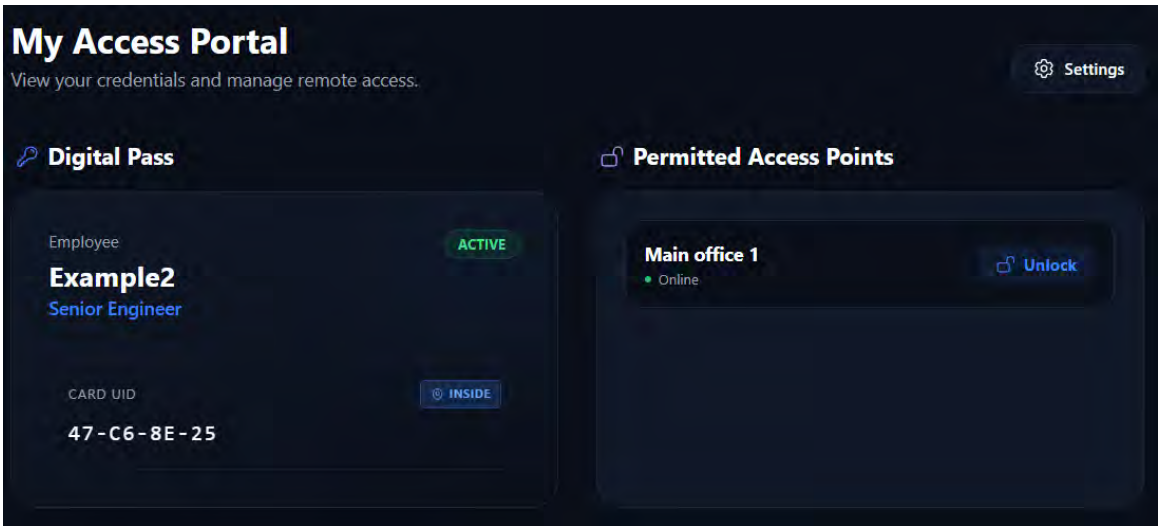

Рисунок 4.13 – Інтерфейс головної панелі працівника

Керування пристроями

Цей розділ доступний виключно адміністраторам, а для звичайних працівників пункт меню автоматично приховується. У робочій області виводиться список усіх підключених пристроїв з індикатором мережевого статусу. Функціонал охоплює реєстрацію нового обладнання за MAC-адресою, присвоєння назви локації та гнучке налаштування реле, де можна обрати тип контактів і вказати точний час затримки в секундах. Також адміністратор може миттєво розблокувати будь-які двері безпосередньо з браузера. Вигляд сторінки керування пристроями та формою додавання нового пристрою наведено на рисунках 4.14 та 4.15 відповідно.

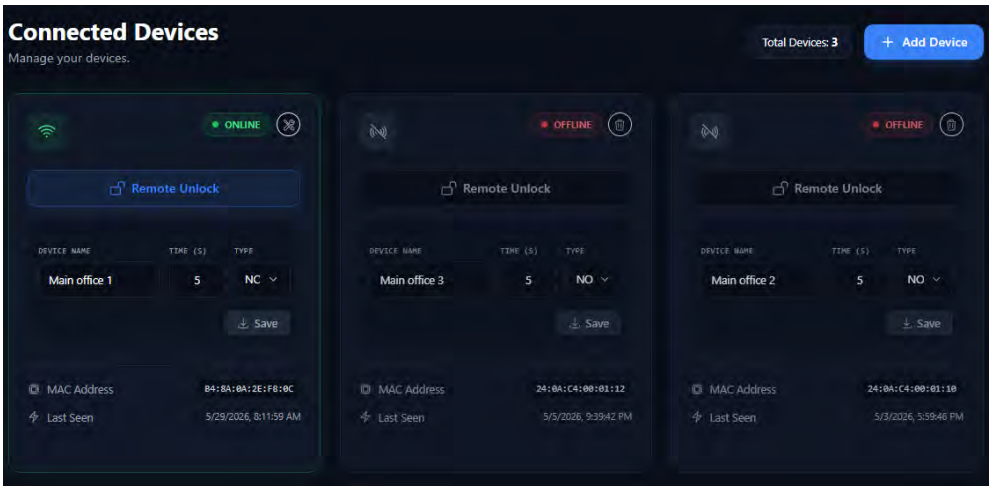

Рисунок 4.14 – Інтерфейс сторінки керування пристроями

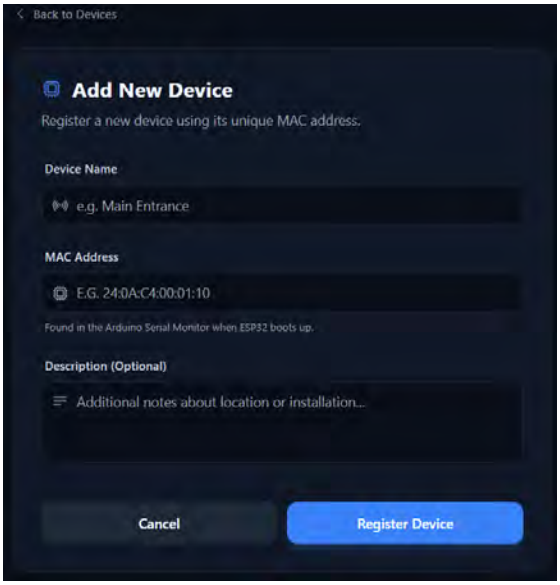

Рисунок 4.15 – Інтерфейс форми додавання нового пристрою

Модуль користувачів

Це спеціалізований розділ для керування персоналом та ідентифікаторами доступу. Для зручної роботи з великим об'ємом даних впроваджено систему фільтрації, яка дозволяє миттєво відфільтрувати загальний список осіб за конкретною точкою доступу. Вигляд сторінки керування користувачами на рисунку 4.16.

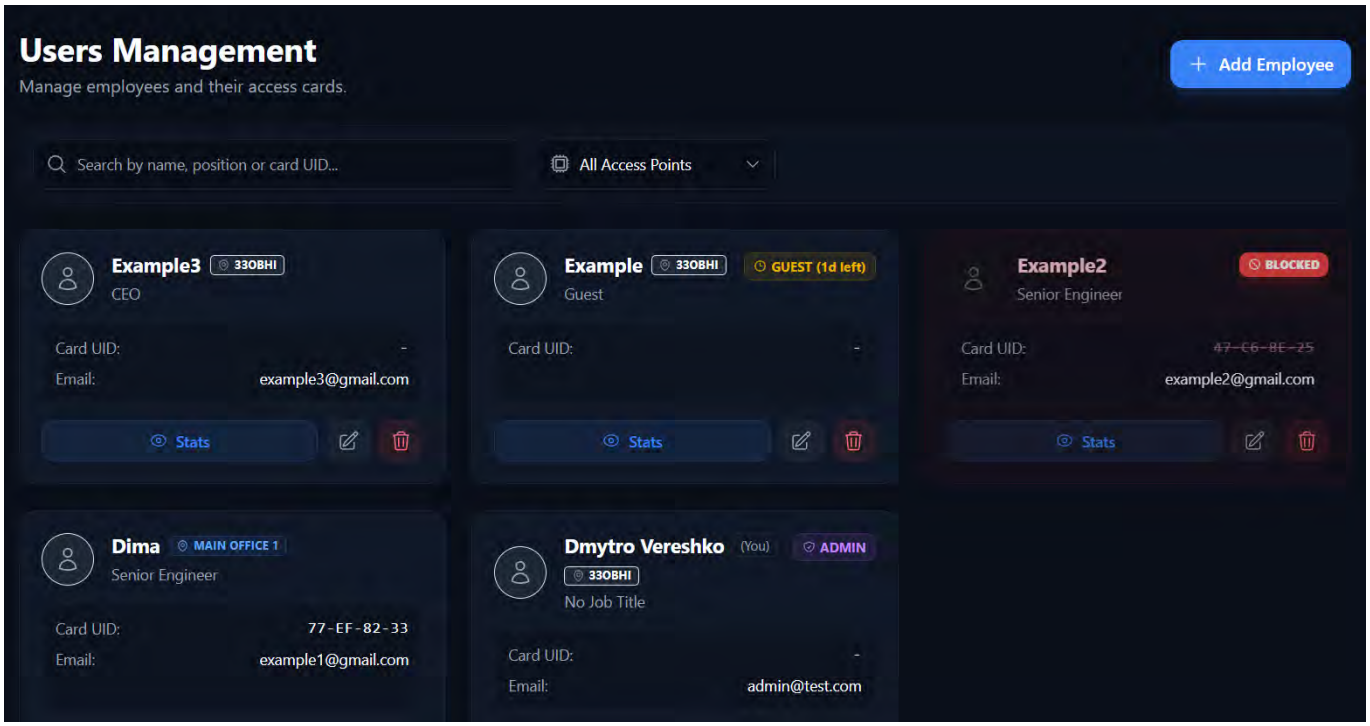

Рисунок 4.16 – Інтерфейс сторінки керування користувачами

Процес реєстрації розділено на дві окремі форми залежно від ролі. Форма додавання нового співробітника, показана на рисунку 4.17, містить поля для введення базових персональних даних, пошти, посади та постійного ідентифікатора доступу. Після успішної реєстрації, система автоматично формує пароль для входу в особистий аккаунт працівника, який адміністратор передає йому. Вигляд створеного логіну та паролю показано на рисунку 4.18. Форма реєстрації тимчасового гостя, зображена на рисунку 4.19, додатково включає точне налаштування дозволених часових рамок роботи картки. Для зручного прив'язування RFID-ключів реалізовано функцію сканування. Адміністратор надсилає команду зчитувачу, підносить картку, і її ідентифікатор автоматично заповнює поле на формі.

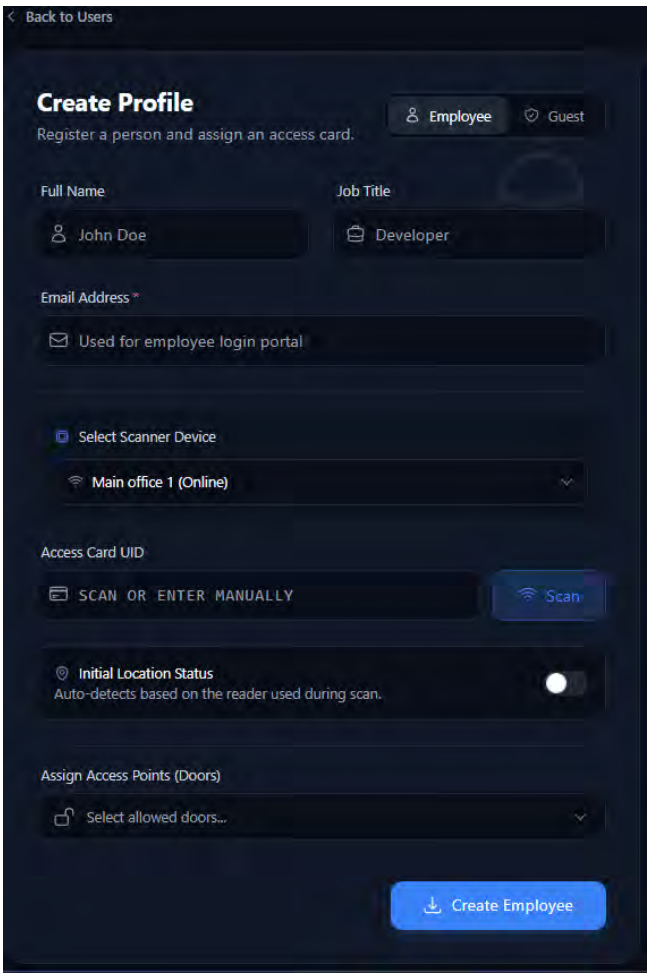

Рисунок 4.17 – Інтерфейс форми створення нового користувача

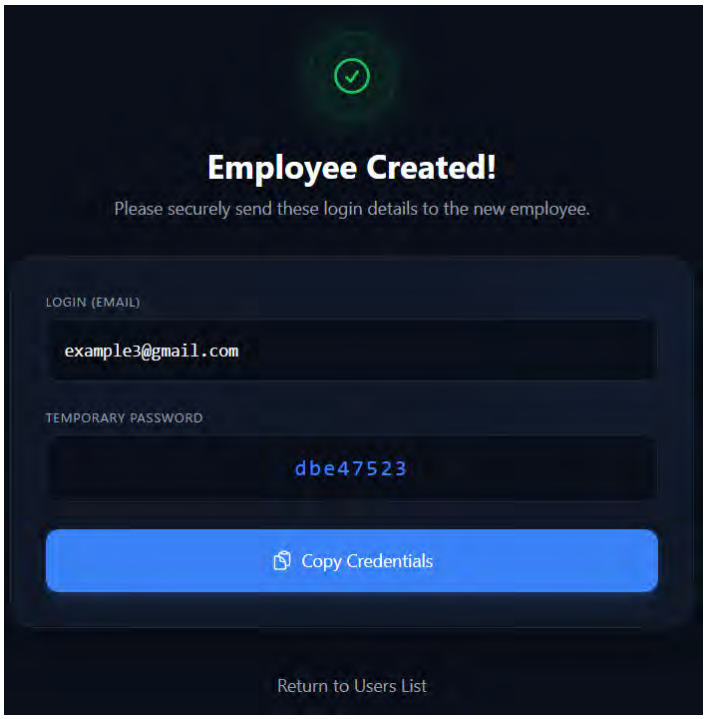

Рисунок 4.18 – Інтерфейс логіну та згенерованого паролю користувача

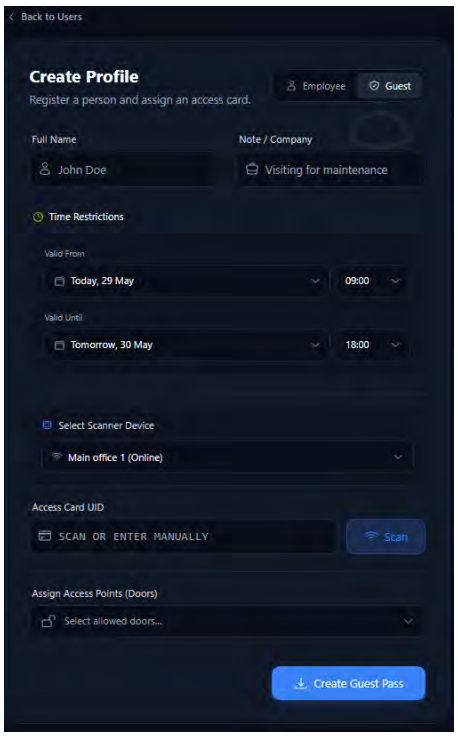

Рисунок 4.19 – Інтерфейс форми створення тимчасового гостя

У модулі також передбачено швидке блокування профілів і ручне керування статусом локації для коригування системи контролю переміщень.

Перегляд індивідуальної статистики винесено в окрему інформаційну панель, яку показано на рисунку 4.20. Перейшовши до картки конкретної особи, адміністратор отримує доступ до деталізованого зрізу її активності. Тут відображається персональна історія переміщень об’єктом і графіки відвідуваності.

Рисунок 4.20 – Інтерфейс вікна редагування користувача

Процес редагування існуючих записів адаптовано під тип профілю, що відображено в інтерфейсі відповідної форми на рисунку 4.21 та 4.22. Для штатних працівників передбачено можливість оперативно змінити посаду, оновити код картки в разі її втрати та розширити список дозволених дверей. Для гостьових облікових записів інтерфейс дозволяє змінити дозволені часові рамки.

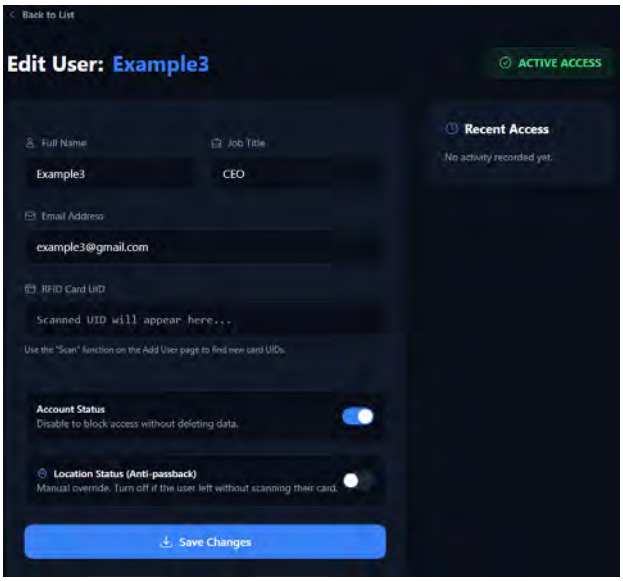

Рисунок 4.21 – Інтерфейс вікна редагування користувацького аккаунта

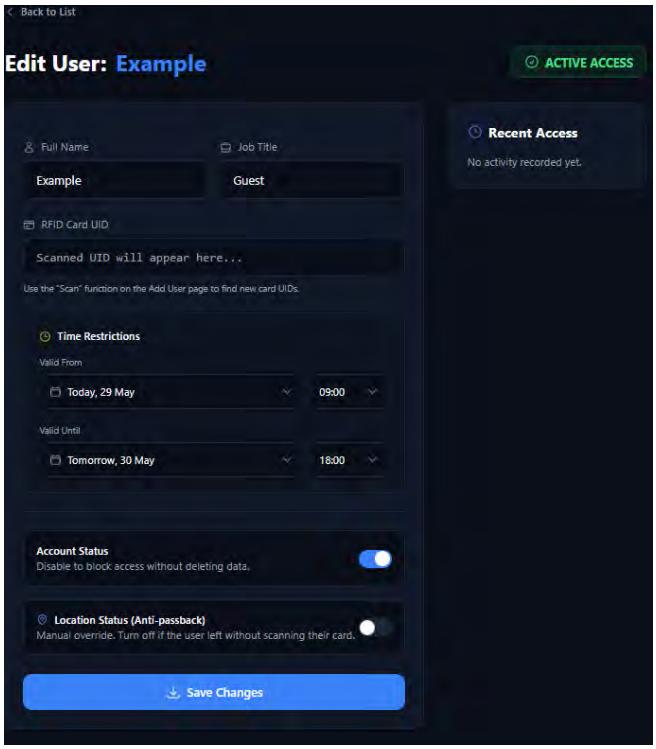

Рисунок 4.22 – Інтерфейс вікна редагування гостьового аккаунта

Журнал подій

Цей розділ призначений для комплексного аудиту безпеки й так само адаптується під роль користувача. Адміністратор бачить структуровану таблицю всіх подій системи, де зафіксовано час, ім’я, точку доступу, напрямок руху та результат проходу. Щоб гарантувати цілісність, інтерфейс використовує архітектуру знімків даних. Якщо профіль порушника або колишнього працівника було видалено, журнал усе одно відображає його ім’я, супроводжуючи запис маркером про видалення. Для адміністратора доступні серверна пагінація, фільтри та можливість експорту журналу. Вигляд сторінки журналу подій наведено на рисунку 4.23.

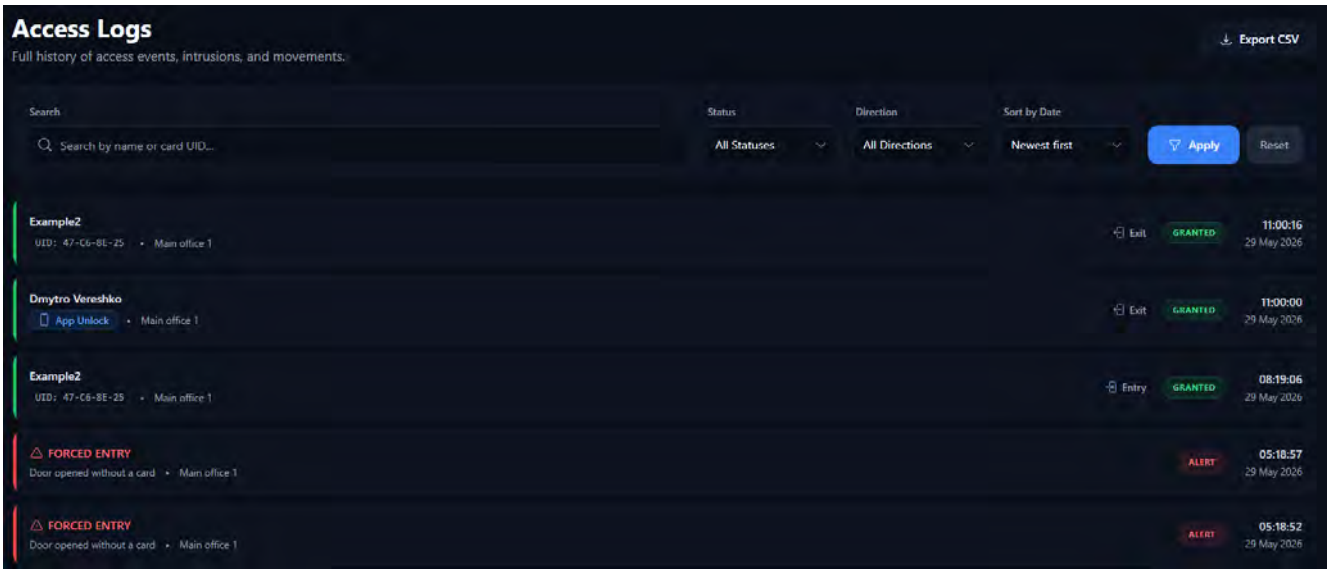

Рисунок 4.23 – Інтерфейс сторінки журналу подій

Системні налаштування

Вкладка для конфігурації профілю та управління безпекою доступна всім користувачам незалежно від їхніх прав. Тут реалізовано форми для зміни логіна й електронної адреси. Зміна пароля вимагає обов’язкової верифікації старого ключа. Вигляд сторінки налаштувань для адміністратора та користувача наведено на рисунку 4.24.

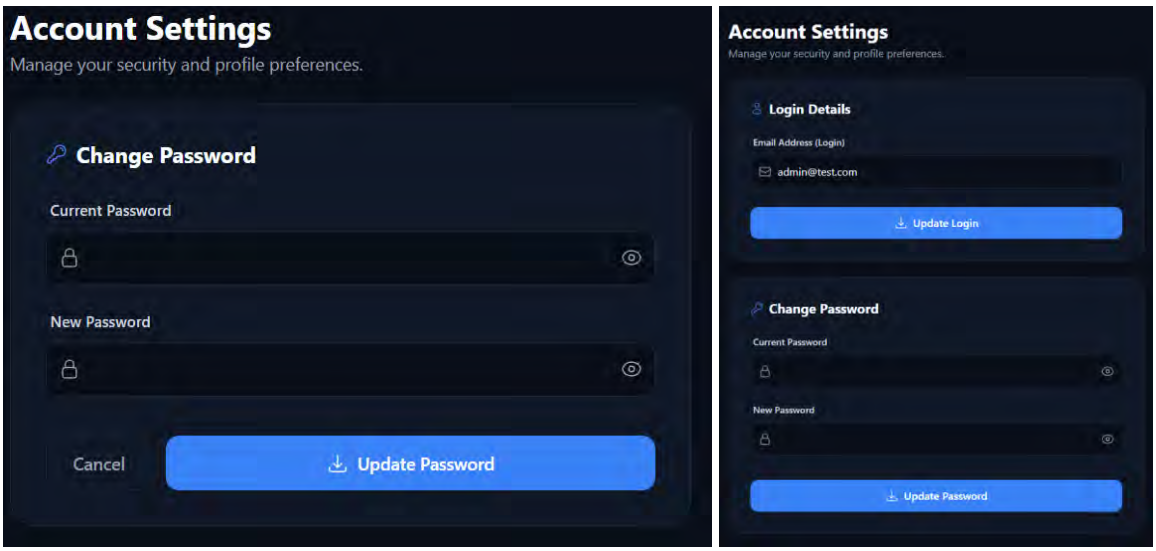

Рисунок 4.24 – Інтерфейс сторінки налаштувань для адміністратора та користувача

На останок варто зазначити, що усю візуальну частину веб-застосунку розроблено з використанням CSS-фреймворку Tailwind CSS [67] та бібліотеки іконок Heroicons [68]. Дизайн повністю адаптивний, тому для зручної роботи з мобільних пристроїв основна бокова навігаційна панель автоматично трансформується в компактне виїзне меню. Це забезпечує комфортне використання системи зі смартфонів.

4.5. Налаштування системи та тестування програмного забезпечення

4.5.1. Підключення до мережі

При першому запуску або за відсутності збережених мереж мікроконтролер розгортає власну точку доступу. Користувач підключається до неї, після чого автоматично відкривається сторінка конфігурації, де вводяться назва Wi-Fi мережі та пароль. Після цього система готова до роботи. Вигляд процесу підключення наведено на рисунку 4.25.

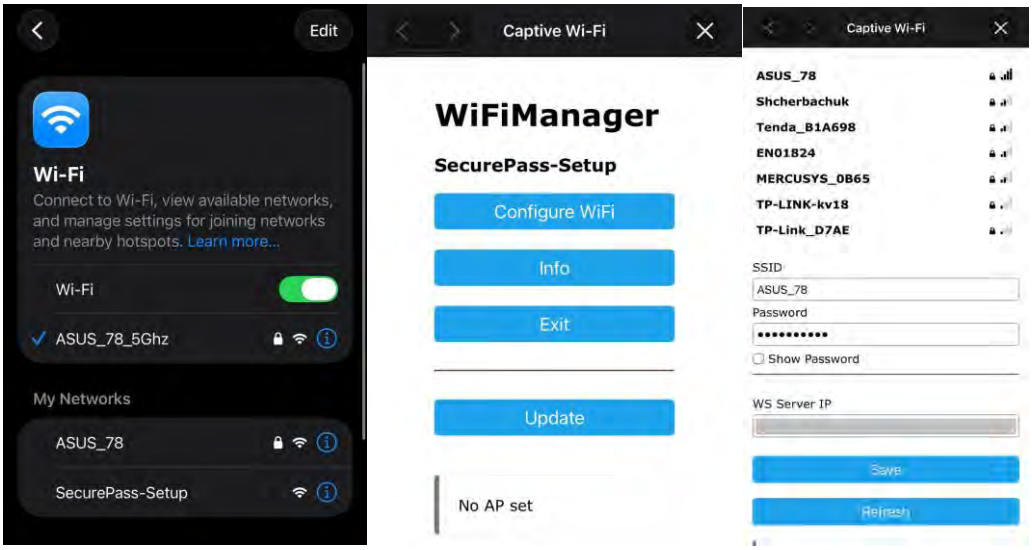

Рисунок 4.25 – Процес підключення до Wi-Fi мережі

4.5.2. Тестування програмного забезпечення

Метою цього етапу є перевірка стабільності усієї системи. Для систематизації результатів перевірки всі ключові сценарії роботи системи та їхній фактичний статус виконання зведено у табл. 4.1.

Таблиця 4.1 – Результати тестування програмного забезпечення

Модуль або Підсистема	Сценарій тестування	Очікуваний результат
1	2	3
Апаратний (ESP32)	Запуск пристрою та ініціалізація компонентів	Контролер успішно стартує, підключається до Wi-Fi, зчитувач готовий до роботи
Апаратний (ESP32)	Реакція на піднесення RFID-картки	Зчитувач фіксує UID мітки без затримок, спрацьовує звукова або світлова індикація
Апаратний (ESP32)	Керування механізмом замка (реле)	Після отримання команди дозволу реле замикається на заданий проміжок часу
WebSocket зв'язок	Встановлення з'єднання з сервером	Сервер фіксує підключення, статус пристрою в інтерфейсі змінюється на Online
WebSocket зв'язок	Розрив з'єднання (втрата живлення або Wi-Fi)	Сервер визначає втрату зв'язку, статус пристрою змінюється на Offline

Продовження таблиці 4.1

1	2	3
WebSocket зв'язок	Передача ідентифікатора картки на сервер	Дані у форматі JSON успішно та миттєво доставляються на бекенд
Авторизація (Next.js)	Вхід адміністратора з правильними даними	Успішна генерація JWT-токена у cookie, перенаправлення на головний дашборд
Авторизація (Next.js)	Спроба входу з невірним паролем	Вхід відхиляється, з'являється відповідне повідомлення про помилку
Захист маршрутів	Спроба доступу без авторизації	Система блокує перехід на захищені сторінки та повертає на екран логіну
Управління ролями	Доступ звичайного працівника до панелі адміна	Маршрутизатор блокує доступ (HTTP 403 або перенаправлення), функціонал приховано
Модуль користувачів	Створення нового профілю працівника	Запис зберігається в базі (Prisma), генерується унікальний пароль для входу
Модуль користувачів	Дистанційне сканування (Remote Scan)	Сервер переводить сканер у режим очікування, піднесена картка заповнює поле форми
Модуль користувачів	Створення тимчасової перепустки (Guest)	Профіль створюється із заданими жорсткими часовими рамками дії
Модуль користувачів	Доступ гостя поза дозволеним часом	Сервер відхиляє запит, доступ заборонено, подія фіксується в журналі
Модуль користувачів	Ручне блокування користувача	Профіль деактивується, будь-які спроби проходу за його карткою миттєво відхиляються
Модуль користувачів	Налаштування дозволених дверей	Користувач отримує доступ виключно до тих контролерів, які вказані в його профілі
Модуль пристроїв	Реєстрація нового контролера	Пристрій додається в базу за його MAC-адресою, генерується картка пристрою
Модуль пристроїв	Валідація дублікатів MAC-адрес	Форма повертає помилку, якщо пристрій з такою MAC-адресою вже існує в системі
Бізнес-логіка (ACS)	Перевірка алгоритму Anti-passback	Спроба повторного входу без реєстрації виходу блокується системою
Журнал подій	Запис події успішного доступу	У базі фіксується час, особа, точка доступу та статус (Access Granted)

Продовження таблиці 4.1

1	2	3
Журнал подій	Оновлення списку логів у реальному часі	Новий запис з'являється на екрані автоматично без перезавантаження
Експорт даних	Вивантаження журналу доступу	Система генерує та віддає користувачу коректний CSV-файл із збереженням усіх полів
Інтерфейс (UI/UX)	Робота виїзного бургер-меню на смартфоні	Меню плавно відкривається та закривається, навігація працює коректно
Інтерфейс (UI/UX)	Пошук та фільтрація в базі користувачів	Список миттєво сортується за введеним ім'ям або прив'язаною точкою доступу
Інтерфейс (UI/UX)	Відображення індивідуальної статистики	При кліку на особу відкривається панель з графіками її активності та історією проходів

Висновки до розділу 4

У четвертному розділі було розроблено комплексне програмне забезпечення системи контролю доступу. Для мікроконтролера написано оптимізовану асинхронну прошивку, яка відповідає за керування апаратною периферією й постійний зв’язок із сервером. Саму ж серверну частину побудували на Node.js та Next.js, поклавши в основу базу даних PostgreSQL. Для зручного моніторингу й адміністрування розробили адаптивний клієнтський веб-застосунок, через який можна дистанційно керувати обладнанням і в реальному часі стежити за переміщенням. Було проведено комплексне тестування системи, яке підтвердило надійність та повну справність усіх її частин.

РОЗДІЛ 5. РОЗРОБКА КОНСТРУКЦІЇ ТА КОРПУСУ ПРИСТРОЮ

Для забезпечення надійного захисту всіх електронних компонентів розробленого пристрою та їх зручного практичного монтажу на об’єкті було спроєктовано спеціальні корпуси, процес створення яких повністю виконувався у середовищі моделювання SolidWorks [69]. В результаті було сформовано документи, в яких детально описуються два основних вузли пристрою у вигляді блоку входу та блоку виходу. Безпосередня розробка конструкції була поділена на кілька послідовних кроків, які охоплюють як вибір матеріалу для виготовлення, так і точний розрахунок кріплень для захисник кришок та електронних компонентів.

5.1. Вибір матеріалу для корпусів

Перед моделюванням корпусу було проведено порівняльний аналіз матеріалів для тривимірного друку. PLA пластик простий у друці, але має надмірну крихкість та низьку стійкість до підвищених температур, а пластик PETG відрізняється хорошою хімічною стійкістю, проте є занадто еластичним для забезпечення необхідної жорсткості [70]. У підсумку для виготовлення корпусів було обрано ABS пластик, оскільки він гарантує високу міцність та відмінну термічну стабільність, що дозволяє вберегти компоненти від випадкових пошкоджень та запобігти деформації від тепла, яке природним чином виділяється під час роботи модуля реле та перетворювача напруги [70].

5.2. Проєктування форми та габаритів корпусів

На першому етапі конструювання було розроблено базову геометричну форму та визначено загальні габаритні розміри обох блоків системи, причому особлива увага приділялась наявності достатнього вільного місця всередині для укладанні дротів. Розроблені кресленики із загальними розмірами корпусів наведені на перших сторінках у ДОДАТКАХ Е та Ж, на яких детально зображено розміри деталей,

товщину стінок та розташування усіх технологічних отворів. 3Д моделі корпусу блоку входу та виходу наведено на рисунках 5.1 та 5.2 відповідно.

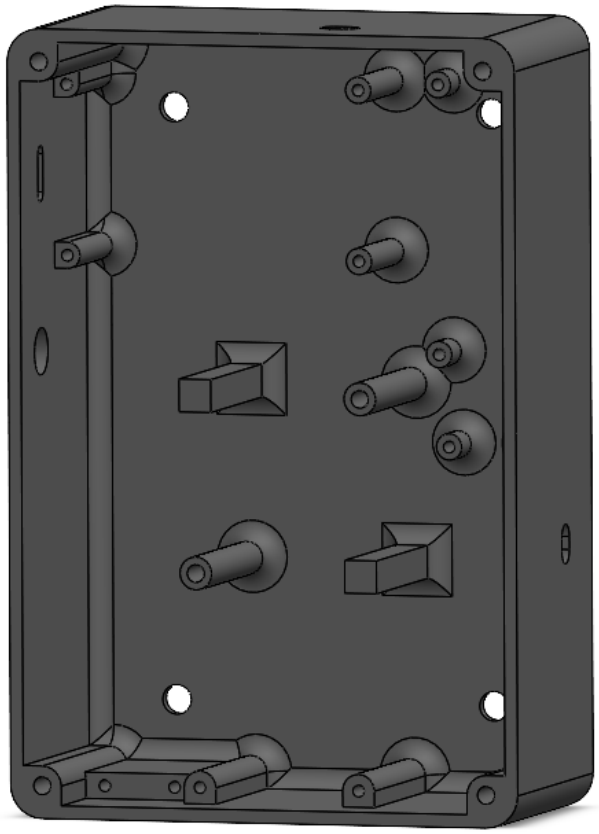

Рисунок 5.1 – 3Д модель корпусу блоку входу

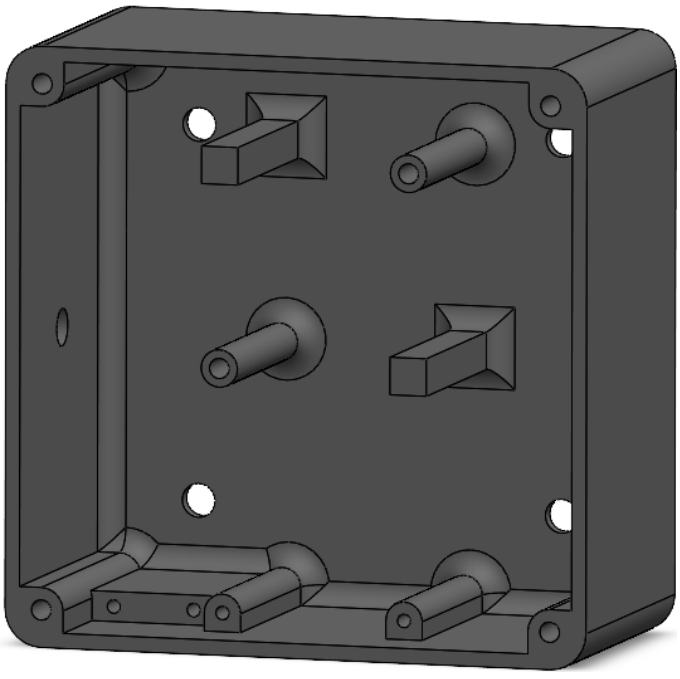

Рисунок 5.2 – 3Д модель корпусу блоку виходу

5.3. Деталювання внутрішніх кріплень компонентів у корпусі

Оскільки всередині кожного блоку повинні розміститись одразу кілька різних електронних плат та компонентів, виникла потреба чітко організувати внутрішній простір корпусу шляхом винесення координат усіх монтажних елементів на окремі аркуші, які містяться на других сторінках у ДОДАТКАХ Е та Ж. Діаметри отворів у стійках для компонентів розраховувалися індивідуально під конкретні елементи кріплення, тому для монтажу зчитувачів передбачено отвори під стандартизовані гвинти М3, тоді як для фіксації мікроконтролера, модуля реле, перетворювача напруги та інших компонентів запроєктовано менші посадкові місця під кріплення гвинтами М2.

5.4. Проєктування захисних кришок

Наступним кроком проєктування стала розробка захисних кришок для обох блоків системи, які наведено у ДОДАТКАХ З та К, котрі призначені для щільного закриття корпусів з метою захисту внутрішньої електроніки від потрапляння пилу чи випадкових механічних пошкоджень. У кресленниках визначено точні габарити кришок, які повністю відповідають посадковим пазам на основних корпусах і містять точні координати наскрізних отворів під метричні гвинти М3. Такий підхід до вибору кріпильних елементів гарантує надійне та щільне прилягання панелей до основи корпусу, що в результаті забезпечує високу міцність та монолітність усієї конструкції у зібраному стані. 3Д моделі кришки блоку входу та виходу наведено на рисунках 5.3 та 5.4 відповідно.

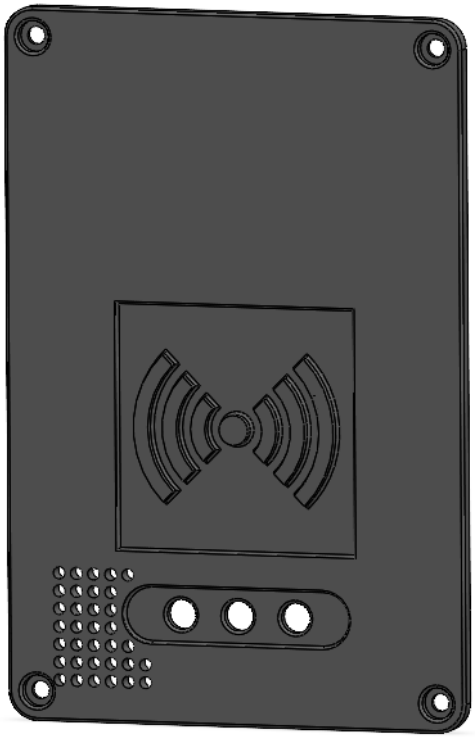

Рисунок 5.3 – 3Д модель кришки блоку виходу

Рисунок 5.4 – 3Д модель кришки блоку виходу

5.5. Створення складальних креслеників та специфікацій вузлів

Для забезпечення правильного та послідовного процесу збирання готового пристрою було розроблено два складальні кресленики, які детально описують

фінальну конструкцію блоку входу та виходу і наведені у ДОДАТКАХ Л та М. На цих графічних документах наочно відображено взаємне розташування всіх раніше спроєктованих деталей, електронних модулів, плат та елементів кріплення у зібраному стані з урахуванням необхідних технологічних зазорів.

Додатково для кожного складального кресленика було сформовано відповідні специфікації, які наведені у ДОДАТКАХ Н та П. Вони містять повний перелік усіх складових частин, включаючи деталі корпусу, кріпильні гвинти та стандартні вироби із зазначеннями їхньої точної кількості.

5.6. Конструктивне забезпечення монтажу корпусів

Фіксація кожного корпусу на несучій поверхні стіни реалізується за допомогою внутрішніх наскрізних отворів із діаметром 4,5 мм, які спеціально розташовані у дні корпусу для забезпечення надійного прикріплення. Для досягнення максимальної міцності встановлення пристрою передбачено використання розпірних полімерних дюбелів розміром 6х40 мм у комплекті з універсальними металевими шурупами розміром 4х40 мм.

Висновки до розділу 5

У п’ятому розділі було розроблено конструкцію корпусів для елементів системи контролю доступу та підготовлено відповідну конструкторську документацію. Аналіз характеристик полімерів дозволив обґрунтувати вибір АБС пластику як найбільш міцного та термостійкого матеріалу для зовнішнього захисту електроніки. Створені документи точно описують просторову геометрію ключових елементів, демонструють будову блоків входу і виходу, положення кріпильних стійок під монтажні гвинти М2 та М3, а також захисних кришок та загальну схему складання кожного вузла.

ВИСНОВКИ

У проєкті було реалізовано автоматизований пристрій контролю доступу до приміщень, який поєднує апаратну й програмну частини. Аналіз готових рішень підтвердив, що власна розробка дає змогу отримати гнучкіший інструмент для автоматизації пропускного режиму.

Архітектура системи визначає, як обладнання, сервер і веб-застосунок взаємодіють між собою. На основі цієї логіки підібрано компоненти, розроблено принципову та функціональну електричні схеми. Програмна частина складається з прошивки для мікроконтролера, сервера для обробки даних і перевірки прав доступу, а також адаптивного веб-застосунком для адміністрування системи, управління користувачами та відстеження подій у реальному часі. Особливу увагу приділено безпеці програмної частини, а саме автентифікації користувачів, захисту запитів і шифруванню критичних даних. Окремо розроблено корпуси, якій захищають електроніку у блоці входу та виходу.

Розроблена система може застосовуватися для організації пропускного режиму на різних об’єктах. Пристрій підходить для встановлення в офісах, навчальних закладах, на складах або житлових комплексах.

Проєкт має хороший потенціал для масштабування й чимало перспектив для подальшого розвитку. Апаратну частину в майбутньому можна легко доповнити сучасними модулями ідентифікації, наприклад біометричними сканерами або системами розпізнавання обличчя. Програмна архітектура дає змогу без жодних перешкод збільшувати кількість контролерів, об’єднуючи сотні віддалених пристроїв у єдину глобальну мережу, а також інтегрувати комплекс із корпоративними системами.

Готовий комплекс пройшов тестування, стабільно виконує всі заявлені функції та повністю відповідає поставленій меті та вимогам.

Список використаних джерел

[1] A. Al-Fuqaha, M. Guizani, and M. Mohammadi, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications." Accessed: May 31, 2026. [Online]. Available: https://www.researchgate.net/publication/279177017_Internet_of_Things_A_Survey_on_Enabling_Technologies_Protocols_and_Applications

[2] А. М. Котенко, *Системи контролю та управління доступом на об'єкти інформаційної діяльності*. Київ: Державний університет інформаційно-комунікаційних технологій, 2024.

[3] T. L. Norman, "Industry History That Can Predict the Future," in *Electronic Access Control*. 2012, pp. 207-208.

[4] "Від простих логічних пристроїв до інтелектуальних вбудованих систем в історії мікроконтролерів." Accessed: May 31, 2026. [Online]. Available: https://www.wonderfulpcb.com/uk/blog/microcontroller-evolution-from-logic-devices-to-embedded-systems

[5] "What is RFID technology - a definition and how it works." Accessed: May 31, 2026. [Online]. Available: https://iotjourney.orange.com/en/support/faq/what-is-rfid-technology-a-definition-and-how-it-works

[6] *Cards and security devices for personal identification - Contactless proximity objects - Part 3: Initialization and anticollision*, ISO/IEC 14443-3:2018, Geneva, 2018. Accessed: May 31, 2026. [Online]. Available: https://www.iso.org/standard/73598.html

[7] "Класифікація систем контролю доступу." Accessed: May 31, 2026. [Online]. Available: http://solis.in.ua/klasyfikatsiya-system-kontrolyu-dostupu.html

[8] S. Waters, "5 Access Control System Components - How They Work?." Accessed: May 31, 2026. [Online]. Available: https://www.coram.ai/post/access-control-system-components

[9] "Best Access Control System Technologies." Accessed: May 31, 2026. [Online]. Available: https://www.getkisi.com/resources/technologies

[10] "Why Web Applications Are Replacing Traditional Desktop Software." Accessed: May 31, 2026. [Online]. Available: https://www.smartdatainc.com/knowledge-hub/why-web-applications-are-replacing-traditional-desktop-software

[11] "Hub 2 Plus Jeweller." Accessed: May 31, 2026. [Online]. Available: https://ajax.systems/ua/products/hub2-plus

[12] "KeyPad Plus Jeweller." Accessed: May 31, 2026. [Online]. Available: https://ajax.systems/ua/products/keypad-plus

[13] "Relay Jeweller." Accessed: May 31, 2026. [Online]. Available: https://ajax.systems/ua/products/relay

[14] "Контролер для 2-дверей DS-K2602." Accessed: May 31, 2026. [Online]. Available: https://hikvision.co.ua/ua/hikvision-ds-k2602/

[15] L. Richardson and S. Ruby, *RESTful Web Services*. 2007.

[16] I. Fette and A. Melnikov, "The WebSocket Protocol." Accessed: May 31, 2026. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6455

[17] "Види замків для СКУД." Accessed: May 31, 2026. [Online]. Available: https://dneprsecurity.com/statji/vidi-zamkov-dlja-skud-.html

[18] Л. Р. Ладієва, *Проєктування систем автоматизації*. Київ: Національний технічний університет України "Київський політехнічний інститут", 2013.

[19] "Нормально розімкнені та замкнуті контакти. NC, NO, COM, що це?." Accessed: May 31, 2026. [Online]. Available: https://angemart.com.ua/statti/35_normalno-rozimkneni-ta-zamknuti-kontakti-nc-no-com-ssho-ce.html?cs=1&hl=en-US&biw=1920&bih=911

[20] *ATmega328P 8-bit AVR Microcontroller with 32K Bytes In-System Programmable Flash*, Datasheet, Atmel, 2015.

[21] *STM32F103C8T6 Datasheet*, STMicroelectronics, 2015.

[22] *ESP32 Series Datasheet*, ver. 5.2, Espressif Systems, 2024.

[23] "About Espressif." Accessed: May 31, 2026. [Online]. Available: https://www.espressif.com/en/company/about-espressif

[24] "ESP32 A Feature-Rich MCU with Integrated Wi-Fi and Bluetooth Connectivity for Wide-Range Applications." Accessed: May 31, 2026. [Online]. Available: https://www.espressif.com/en/products/socs/esp32

[25] "ESP32 for IoT: A Complete Guide." Accessed: May 31, 2026. [Online]. Available: https://www.nabto.com/guide-to-iot-esp-32/

[26] A. Prabhu, "ESP32 Pinout Reference." Accessed: May 31, 2026. [Online]. Available: https://lastminuteengineers.com/esp32-pinout-reference/

[27] "Power Management," in *ESP32 Series Datasheet*, ver. 5.2, Espressif Systems, 2024.

[28] "Security," in *ESP32 Series Datasheet*, ver. 5.2, Espressif Systems, 2024.

[29] "ESP32 Pinout Guide (GPIO - ADC - DAC - Touch): Complete Hardware Reference for Stable Circuit Design." Accessed: May 31, 2026. [Online]. Available: https://www.sunfounder.com/blogs/news/esp32-pinout-guide-gpio-adc-dac-touch-complete-hardware-reference-for-stable-circuit-design

[30] "ESP32 NODEMCU-32S ESP-32S Kit: high resolution pinout, datasheet, and specs." Accessed: May 31, 2026. [Online]. Available: https://mischianti.org/esp32-nodemcu-32s-esp-32s-kit-high-resolution-pinout-datasheet-and-specs

[31] *MFRC522 Standard Performance MIFARE and NTAG Frontend*, Datasheet, NXP Semiconductors, 2016.

[32] "PN532 NFC Arduino: Contactless Card Projects for PCB Engineers." Accessed: May 31, 2026. [Online]. Available: https://pcbsync.com/pn532-nfc-arduino/

[33] *PN532/C1*, Datasheet, NXP Semiconductors, 2017.

[34] *PN532 - NFC RFID Module*, Datasheet, Components101, 2021.

[35] "Study of vulnerabilities in MIFARE Classic cards." Accessed: May 31, 2026. [Online]. Available: https://www.sidechannel.blog/en/mifare-classic-2

[36] "MIFARE Classic vs DESFire: Key Differences, Security, Applications, and How to Choose the Right RFID Card." Accessed: May 31, 2026. [Online]. Available: https://www.rfidcard.com/mifare-classic-vs-desfire-key-differences-security-applications-and-how-to-choose-the-right-rfid-card

[37] "Android C. Understand the Key Diversification on Mifare DESFire EVx NFC cards." Accessed: May 31, 2026. [Online]. Available:

https://medium.com/@androidcrypto/understand-the-key-diversification-on-mifare-desfire-evx-nfc-cards-309183aa687b

[38] "Модуль реле 12В 10А з опторозв'язкою (low level)." Accessed: May 31, 2026. [Online]. Available: https://arduino.ua/prod2968-modyl-rele-12v-10a-s-optorazvyazkoi

[39] "Світлодіод 5мм ультраяскравий." Accessed: May 31, 2026. [Online]. Available: https://arduino.ua/prod450-Svetodiod_5mm_zelenii

[40] "Модуль з динаміком KY-006 (пасивний)." Accessed: May 31, 2026. [Online]. Available: https://arduino.ua/prod1153-modyl-s-dinamikom-ky-006-passivnii

[41] "Датчик відкриття дверей MC-38." Accessed: May 31, 2026. [Online]. Available: https://arduino.ua/prod588-datchik-otkritiya-dverei-mc-38

[42] "Що таке геркон: усе про датчики відкриття дверей." Accessed: May 31, 2026. [Online]. Available: https://nadzor.ua/uk/blog/signalizacii/scho-take-gerkon-use-pro-datchiki-vidkrittya-dverey?srsltid=AfmBOopdOyHQdE3Xbxxl9OHDurE4UMvnN6O301rhuoDryRLewI-5BmAa

[43] "Електромагнітний замок ML-180." Accessed: May 31, 2026. [Online]. Available: https://vision-s.pro/ua/p858916580-elektromagnitnyj-zamok-180.html?srsltid=AfmBOooXyRjc8fgLsaCarpWLeYc9FgaJ75ExvpCy06-UYEVPNxBSC7RG

[44] "NO, NC, Fail Safe та Fail Secure у замках, дверях та контактах." Accessed: May 31, 2026. [Online]. Available: https://www.bezpeka-shop.com/ua/blog/poleznye-sovety/no-nc-fail-safe-y-fail-secure-v-zamkakh-dveryakh-y-kontaktakh/?srsltid=AfmBOorU-9Fe7AS9_CYa5ql2iGHiVtYQ2KhJzOsoqAfjxUTZSNeJDxCo

[45] *NodeMCU-32 Specification*, ver. 1.3, Ai-Thinker, 2020.

[46] *PN532 Module V3 Schematic*, Elechouse, 2014.

[47] *MINI-360 MP2307 Buck Converter*, Datasheet, Monolithic Power Systems, 2012.

[48] "Arduino IDE." Accessed: May 31, 2026. [Online]. Available: https://docs.arduino.cc/software/ide

[49] "The React Framework for the Web." Accessed: May 31, 2026. [Online]. Available: https://nextjs.org/

[50] "React: The library for web and native user interfaces." Accessed: May 31, 2026. [Online]. Available: https://react.dev/

[51] "TypeScript is JavaScript with syntax for types," What is TypeScript?. Accessed: May 31, 2026. [Online]. Available: https://www.typescriptlang.org/

[52] "Understanding SQL vs NoSQL Databases." Accessed: May 31, 2026. [Online]. Available: https://www.mongodb.com/resources/basics/databases/nosql-explained/nosql-vs-sql

[53] "Що таке ACID?." Accessed: May 31, 2026. [Online]. Available: https://codefinity.com/ua/courses/v2/d90d9403-ce34-4555-b549-6bb5773a48a2/a3ac8c0f-a247-4098-befd-1c1b90eef079/054f93b2-600b-4bd9-b6a7-0089bc186a16

[54] "Next-generation Node.js and TypeScript ORM," Prisma. Accessed: May 31, 2026. [Online]. Available: https://www.prisma.io/orm

[55] "The JavaScript and TypeScript IDE." Accessed: May 31, 2026. [Online]. Available: https://www.jetbrains.com/webstorm/

[56] "HttpClient." Accessed: May 31, 2026. [Online]. Available: https://github.com/amcewen/HttpClient

[57] "ArduinoJson." Accessed: May 31, 2026. [Online]. Available: https://github.com/bblanchon/ArduinoJson

[58] "A Comprehensive Guide to Finite State Machines in Computer Science." Accessed: May 31, 2026. [Online]. Available: https://mehmet-tosun.medium.com/a-comprehensive-guide-to-finite-state-machines-in-computer-science-9fc74f96e1f4

[59] "Denial-of-service attack." Accessed: May 31, 2026. [Online]. Available: https://www.ebsco.com/research-starters/military-history-and-science/denial-service-attack

[60] "WiFiManager." Accessed: May 31, 2026. [Online]. Available: https://github.com/tzapu/WiFiManager

[61] "About Node.js." Accessed: May 31, 2026. [Online]. Available: https://nodejs.org/en/about

[62] "What is PostgreSQL?." Accessed: May 31, 2026. [Online]. Available: https://www.postgresql.org/about/

[63] "Ws: a Node.js WebSocket library." Accessed: May 31, 2026. [Online]. Available: https://www.npmjs.com/package/ws

[64] "Що таке middleware? Приклади в Express, FastAPI та інших фреймворках." Accessed: Jun. 01, 2026. [Online]. Available: https://itproger.com/ua/news/chto-takoe-middleware-primeri-v-express-fastapi-i-drugih-freymvorkah

[65] "Introduction to JSON Web Tokens." Accessed: Jun. 01, 2026. [Online]. Available: https://www.jwt.io/introduction#what-is-json-web-token

[66] "Bcrypt.js." Accessed: Jun. 01, 2026. [Online]. Available: https://www.npmjs.com/package/bcryptjs

[67] "Rapidly build modern websites without ever leaving your HTML." Accessed: Jun. 01, 2026. [Online]. Available: https://tailwindcss.com/

[68] "Heroicons." Accessed: Jun. 01, 2026. [Online]. Available: https://heroicons.com/

[69] "SOLIDWORKS Design." Accessed: Jun. 01, 2026. [Online]. Available: https://www.solidworks.com/product/solidworks-design

[70] "PLA, ABS, PETG: Порівняння властивостей і відмінності пластиків." Accessed: Jun. 01, 2026. [Online]. Available: https://lbl-corp.com/blog/pla-abs-petg/?srsltid=AfmBOooQwtNyksoYqgRfjI3Dx5Zl37FBJ81Q4Qqni6Xf-m0yvozf5Ibx

[71] Спеціальні розділи математики: конспект лекцій : навч. посіб. / КПІ ім. Ігоря Сікорського ; уклад.: Ю. В. Куц, Ю. Ю. Лисенко, В. М. Сокуренко. – Київ : КПІ ім. Ігоря Сікорського, 2024. – 192 с.

[72] Муравйов О. В. Передача даних та сучасні методи обробки сигналів. Практикум: навчальний посібник / О. В. Муравйов; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім.Ігоря Сікорського, 2022. – 55 с.

[73] Статистичні методи визначення залежностей між випадковими величинами: навчальний посібник / Ю. В. Куц, Ю. Ю. Лисенко; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2023. – 115 с.

[74] Комп'ютерне проєктування електронних схем. Комп’ютерний практикум [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Комп’ютерно-інтегровані системи та технології в приладобудуванні» спеціальності 151 «Автоматизація та комп’ютерно-інтегровані

технології» та 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Р. М. Галаган ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 21,33 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2023. – 419 с.

[75] Баженов В.Г. Електроніка. Лабораторний практикум: навчальний посібник / В. Г. Баженов, Є. Ф. Суслов, Ю. Ю. Лисенко, А.С. Момот; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2022. – 70 с.

[76] Куц Ю.В. Новітні системи та технології: навчальний посібник / Ю. В. Куц, Ю. Ю. Лисенко, А.С. Момот; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2022. – 123 с.