

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
РАДІОТЕХНІЧНИЙ ФАКУЛЬТЕТ
кафедра РАДІОІНЖЕНЕРІЇ**

«На правах рукопису»

УДК 004.056.5

До захисту допущено:

Завідувач кафедри

 Сергій ЛІТВІНЦЕВ

« 22 » 12 2025 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою

«Інформаційна та комунікаційна радіоінженерія»

зі спеціальності 172 «Електронні комунікації та радіотехніка»

на тему: **«Система контролю доступу на основі технологій LoRa та RFID»**

Виконав студент II курсу, групи PI-41 мп

Слободяник Марко Петрович

(прізвище, ім'я, по-батькові)


(підпис)

Науковий керівник:

к.т.н., доц. Літвінцев Сергій Миколайович

(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові)


(підпис)

Рецензент:

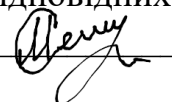
к.т.н., доц. каф. ПРЕ Шульга Аліна Вікторівна

(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент



Київ – 2025р.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО”**

РАДІОТЕХНІЧНИЙ ФАКУЛЬТЕТ

Кафедра радіоінженерії

Рівень вищої освіти – другий (магістерський)

спеціальність 172 “Електронні комунікації та радіотехніка”

Освітньо-професійна програма «Інформаційна та комунікаційна радіоінженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри РІ

 Сергій ЛІТВІНЦЕВ

« 8 » 09 2025 року

**ЗАВДАННЯ
на магістерську дисертацію студенту (тці)**

Слободянику Марку Петровичу

(прізвище, ім'я, по батькові)

1. Тема дисертації

Система контролю доступу

на основі технологій LoRa та RFID

науковий керівник дисертації

Літвінцев Сергій Миколайович, к.т.н, доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від « 11 » 11 2025 р. № 4896-с

2. Термін подання студентом дисертації

22.12.2025

3. Об'єкт дослідження: процес функціонування систем контролю доступу

4. Вихідні дані: використання технології LoRa та безконтактної ідентифікації RFID; керування з мобільного телефону.

5. Перелік завдань, які потрібно розробити: провести аналіз сучасних методів побудови систем контролю доступу та особливостей технології RFID, вибір елементної бази, розробка структурних та електричних принципових схем, розробка програмного забезпечення, проєктування апаратної частини, проєктування корпусів, виготовлення та випробування прототипу, розробка стартап-проєкту, висновки.

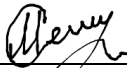
6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація, схеми електричні принципові

7. Орієнтовний перелік публікацій: Слободяник М. П., Літвінцев С. М. Система авторизації з використанням технології LoRa // Збірник праць XIV Міжнародна науково-технічна конференція “Радіотехнічні проблеми, сигнали, апарати та системи” – Київ, КПІ ім. Ігоря Сікорського, 4-5 грудня 2025 р., ст 72-74.
8. Консультанти розділів дисертації: науково-педагогічні працівники радіотехнічного факультету.
9. Дата видачі завдання: 8.09.2025 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Огляд та аналіз існуючих систем контролю	08.09.2025 – 22.09.2025	Виконано
2	Розробка структурних схем та обґрунтування вибору елементної бази	23.09.2025 – 01.10.2025	Виконано
3	Розробка схем електричних принципів	02.10.2025 – 15.10.2025	Виконано
4	Макетне моделювання та випробування базових функцій	16.10.2025 – 22.10.2025	Виконано
5	Розробка структурних схем програмної частини системи	23.10.2025 – 29.10.2025	Виконано
6	Написання та налагодження програмного забезпечення	30.10.2025 – 18.11.2025	Виконано
7	Проектування друкованих плат та корпусів	19.11.2025 – 25.11.2025	Виконано
8	Виготовлення та випробування прототипу	26.11.2025 – 02.12.2025	Виконано
9	Розробка стартап-проєкту	03.12.2025 – 09.12.2025	Виконано
10	Висновки та оформлення роботи	10.12.2025 – 15.12.2025	Виконано

Студент


(підпис)

Марко СЛОБОДЯНИК

(ім'я, ПРІЗВИЩЕ)

Науковий керівник


(підпис)

Сергій ЛІТВІНЦЕВ

(ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Актуальність теми. Системи контролю доступу відіграють ключову роль у забезпеченні безпеки будівель, виробничих та адміністративних приміщень, контролюючи фізичний доступ. Їх важливість зростає із зростанням вимог до надійності та зручності експлуатації. Однак, існуючі комерційні рішення часто відзначаються високою вартістю через використання спеціальних протоколів та мають обмеження щодо простоти керування та масштабованості.

Метою роботи є розробка бездротової системи контролю доступу з використанням сучасних методів ідентифікації користувачів та захищеної передачі інформації.

Завдання дослідження. Досягнення поставленої мети потребує вирішення таких завдань:

- провести аналіз існуючих методів і засобів ідентифікації користувачів, зокрема систем, побудованих на основі RFID-технологій;
- дослідити принципи побудови RFID-систем, типи міток і зчитувачів, їх технічні характеристики та особливості взаємодії;
- розробити апаратну частину системи контролю доступу, обґрунтувавши вибір елементної бази;
- розробити програмну частину системи, включаючи алгоритми збереження й передачі зашифрованої інформації по бездротовому каналу та адміністрування з мобільного телефону;
- виготовити та випробувати прототип.

Об'єкт дослідження. Процес функціонування бездротових систем контролю доступу та ідентифікації користувачів.

Предмет дослідження. Методи, апаратні та програмні засоби реалізації бездротової системи контролю доступу.

Методи дослідження. Застосовано системний аналіз для вивчення особливостей сучасних підходів до контролю доступу. Порівняльний підхід дав змогу оцінити різні способи ідентифікації, захисту та передачі інформації, що допомогло обрати найбільш ефективні шляхи для практичної реалізації.

Практичне значення отриманих результатів. Практична цінність отриманих результатів полягає в можливості їх безпосереднього застосування у сучасних системах контролю доступу. Розроблена система демонструє, що поєднання апаратних рішень і програмної логіки дозволяє створити надійний інструмент для організації доступу в різних сферах – від побутових до промислових. Отримані результати можуть стати основою для майбутніх комерційних або наукових проєктів.

Апробація результатів дослідження. Результати роботи були представлені автором на XIV Міжнародній науково-технічній конференції “Радіотехнічні проблеми, сигнали, апарати та системи”.

Публікації. Основні результати роботи викладено в публікації: Слободяник М. П., Літвінцев С. М. Система авторизації з використанням технології LoRa // Збірник праць XIV Міжнародна науково-технічна конференція “Радіотехнічні проблеми, сигнали, апарати та системи” – Київ, КПІ ім. Ігоря Сікорського, 4-5 грудня 2025 р., ст 72-74.

Структура та обсяг магістерської дисертації. Робота складається зі вступу, 5 розділів, висновків до розділів, загальних висновків, списку використаних джерел (26 джерел, у тому числі 13 – іноземною мовою), 4 додатків на 13 сторінках. Загальний обсяг дисертації – 127 сторінок. Основний зміст викладено на 98 сторінках. Роботу проілюстровано 24 таблицями, 51 рисунками.

Ключові слова: система контролю доступу, LoRa, RFID, ідентифікація, алгоритм авторизації, шифрування, база даних.

ABSTRACT

Relevance of the topic. Access control systems play a key role in ensuring the security of buildings, industrial and administrative premises, controlling physical access. Their importance is growing with increasing requirements for reliability and ease of operation. However, existing commercial solutions are often characterized by high cost due to the use of special protocols and have limitations in terms of ease of management and scalability.

The purpose of the work is to develop a wireless access control system using modern methods of user identification and secure information transmission.

Research objectives. Achieving the set goal requires solving the following tasks:

- to analyze existing methods and means of user identification, in particular systems built on the basis of RFID technologies;
- to study the principles of building RFID systems, types of tags and readers, their technical characteristics and interaction features;
- to develop the hardware part of the access control system, justifying the choice of the element base;
- develop the software part of the system, including algorithms for storing and transmitting encrypted information over a wireless channel and administration from a mobile phone;
- produce and test a prototype.

Object of research. The process of functioning of wireless access control systems and user identification.

Subject of research. Methods, hardware and software for implementing a wireless access control system.

Research methods. System analysis was used to study the features of modern approaches to access control. The comparative approach made it possible to evaluate different methods of identification, protection and transmission of information, which helped to choose the most effective ways for practical implementation.

Practical significance of the results obtained. The practical value of the results obtained lies in the possibility of their direct application in modern access control systems. The developed system demonstrates that the combination of hardware solutions and software logic allows you to create a reliable tool for organizing access in various areas - from household to industrial. The results obtained can become the basis for future commercial or scientific projects.

Testing of research results. The results of the work were presented by the author at the XIV International Scientific and Technical Conference “Radio Engineering Problems, Signals, Devices and Systems”.

Publications. The main results of the work are presented in the publication: Slobodyanyk M. P., Litvintsev S. M. Authorization System Using LoRa Technology // Proceedings of the XIV International Scientific and Technical Conference “Radio Engineering Problems, Signals, Devices and Systems” – Kyiv, Igor Sikorsky Kyiv Polytechnic Institute, December 4-5, 2025, pp. 72-74.

Structure and scope of the master's thesis. The work consists of an introduction, 5 chapters, conclusions to the chapters, general conclusions, a list of sources used (26 sources, including 13 – in a foreign language), 4 appendices on 13 pages. The total volume of the thesis is 127 pages. The main content is presented on 98 pages. The work is illustrated with 24 tables, 51 figures.

Keywords: access control system, LoRa, RFID, identification, authorization algorithm, encryption, database.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	11
ВСТУП.....	12
1. АНАЛІЗ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ТА ТЕХНОЛОГІЇ RFID	13
1.1 Загальна характеристика систем контролю доступу	13
1.1.1 Класифікація систем	13
1.1.2 Основні принципи функціонування систем	14
1.1.3 Переваги та недоліки різних підходів до аутентифікації.....	14
1.2 Огляд існуючих рішень на ринку.....	15
1.2.1. Комерційні RFID-системи.....	15
1.2.2. Порівняльний аналіз комерційних систем RFID	21
1.3 Технологія RFID	23
1.3.1 Історія і розвиток технології	23
1.3.2 Типи RFID-міток та зчитувачів.....	24
1.3.3 Частотні діапазони та стандарти.....	26
1.4 Безпека та протоколи передачі даних у RFID	26
1.4.1 Методи шифрування та аутентифікація.....	27
1.4.2 Вразливості та загрози	28
1.5 Висновки до розділу 1	28
2. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ	30
2.1 Розробка структурних схем апаратної частини.....	30
2.2 Вибір елементної бази та обґрунтування.....	32
2.2.1 Вибір мікроконтролера	32
2.2.2 Вибір RFID-зчитувача.....	33
2.2.3 Вибір радіомодуля LoRa.....	34
2.3 Розробка електричних принципових схем.....	40
2.4 Макетне моделювання	42
2.4.1 Збирання апаратних модулів на макетній платі.....	42
2.4.2 Випробування базових функцій та перевірка взаємодії модулів	44
2.5 Висновки до розділу 2.....	47
3. РОЗРОБКА ПРОГРАМНОЇ ЧАСТИНИ СИСТЕМИ	49
3.1 Вибір мови програмування та середовища розробки	49
3.2 Розробка структурних схем програмної частини.....	50

3.3	Реалізація функціональних блоків у коді.....	54
3.3.1	Блок «Початок»	54
3.3.2	Блок «Ініціалізація та перевірка доступності компонентів»	55
3.3.3	Блок «Асинхронні дії»	57
3.3.4	Блок «Читання та обробка RFID-міток»	58
3.3.5	Блок «Оновлення індикації та дисплея»	59
3.3.6	Блок «Очікування й обробка пакетів».....	60
3.3.7	Блок «Запит до бази даних» та структура файлу	61
3.3.8	Блок «Формування й відправка пакету»	64
3.3.9	Блок «Очікування і обробка відповіді».....	65
3.3.10	Блок «Зміна стану керуючих елементів»	66
3.4	Висновки до розділу 3	67
4.	ПРОЄКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ.....	69
4.1	Розробка друкованих плат системи	69
4.1.1	Визначення габаритів й форми	70
4.1.2	Розрахунок ширини друкованих провідників	71
4.1.3	Трасування друкованих плат.....	73
4.2	Розробка корпусів.....	75
4.2.1	Корпус головного пристрою	76
4.2.2	Корпус другорядного пристрою	80
4.3	Виготовлення та випробування прототипу.....	82
4.3.1	Виготовлення друкованих плат та складання пристроїв	83
4.3.2	Випробування прототипу	85
4.4	Висновки до розділу 4.....	88
5.	РОЗРОБКА СТАРТАП ПРОЄКТУ	89
5.1	Опис ідеї проєкту.....	89
5.2	Технічний аудит проєкту	91
5.3	Аналіз ринкових можливостей запуску стартап-проєкту	92
5.4	Розробка ринкової стратегії стартап-проєкту.....	101
5.5	Розробка маркетингової програми стартап-проєкту.....	104
5.6	Висновки до розділу 5.....	108
	ВИСНОВКИ.....	110
	СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	112

ДОДАТОК А.....	115
ДОДАТОК Б	116
ДОДАТОК В.....	117
ДОДАТОК Г	125

ПЕРЕЛІК СКОРОЧЕНЬ

СКД – система контролю доступу
БД – база даних
ГП – головний пристрій
ДП – другорядний пристрій
ШИМ – Широтно-Імпульсна Модуляція
RFID – Radio Frequency Identification
LoRa – Long Range
LF – Low Frequency
HF – High Frequency
UHF – Ultra High Frequency
Wi-Fi – Wireless Fidelity
AES – Advanced Encryption Standard
NFC – Near Field Communication
SPI – Serial Peripheral Interface
CS – Chip Select
I2C – Inter-Integrated Circuit
CSV – Comma-Separated Values
PIN – Personal Identification Number
RGB – Red Green Blue
GPIO – General Purpose Input/Output
PLA – Polylactic Acid
ABS – Acrylonitrile Butadiene Styrene

ВСТУП

У сучасному світі інформаційні технології охоплюють практично всі сфери людської діяльності, зокрема ті, що пов'язані із забезпеченням безпеки та контролю доступу. Зростання кількості електронних систем, що потребують надійної ідентифікації користувачів, спонукає до впровадження швидкодіючих, зручних та захищених механізмів авторизації. Традиційні засоби, такі як PIN-коди або механічні ключі, мають низку обмежень, серед яких основними є низька стійкість до копіювання та вразливість до несанкціонованого доступу.

У цьому контексті особливого значення набувають технології безконтактної ідентифікації, серед яких RFID є досить популярною. Завдяки можливості швидко та надійно зчитувати інформацію без фізичного контакту, такі системи роблять процес авторизації зручнішим і ефективнішим. Взаємна інтеграція технології RFID з бездротовою передачею інформації дає можливість створювати розподілені та масштабовані системи, у яких кілька пристроїв можуть взаємодіяти між собою на значній відстані.

Одним із перспективних напрямів є застосування енергоефективних технологій далекого радіозв'язку, таких як LoRa. Вони дозволяють передавати дані між вузлами системи на великі відстані, водночас споживаючи мінімум енергії. Це особливо зручно там, де прокладання дротової інфраструктури є складним, небажаним або економічно невиправданим. Створення комплексної системи авторизації, яка поєднує RFID, захищений бездротовий зв'язок і локальне збереження даних, узгоджується з сучасними тенденціями розвитку інтелектуальних систем доступу. Подібні рішення стають актуальними як у побутових і адміністративних приміщеннях, так і у виробничих середовищах, де важливими є безпека та можливість взаємодії на відстані. Таким чином, розроблення системи контролю доступу на основі технологій LoRa та RFID є актуальним завданням.

1. АНАЛІЗ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ТА ТЕХНОЛОГІЙ RFID

1.1 Загальна характеристика систем контролю доступу

Системи контролю доступом [1] є ключовим елементом для забезпечення комплексної безпеки на об'єктах різного призначення. Основне призначення таких систем полягає в автоматизованому контролі прав доступу та запобіганні проникненню сторонніх осіб на територію, що охороняється. Ефективність функціонування СКД безпосередньо залежить від обраної архітектури та технологій ідентифікації. Для розуміння принципів побудови та вибору оптимальної архітектури системи необхідно розглянути існуючі підходи до їх класифікації, а також порівняти переваги та недоліки різних методів аутентифікації.

1.1.1 Класифікація систем

СКД класифікують залежно від способу підтвердження особи користувача та типу доступу, який вони забезпечують. За методом підтвердження виділяють три основні підходи. Перший – це те, що користувач знає паролі або PIN-коди. Цей метод є найбільш поширеним завдяки простоті реалізації та низькій вартості, однак він має значні недоліки з точки зору безпеки, оскільки дані можуть бути вкрадені або підібрані за допомогою кібератак. Другий підхід – користувач має, наприклад безконтактні картки або брелоки. Такі методи дозволяють здійснювати доступ до ресурсів і забезпечують вищий рівень захисту у порівнянні з паролями, проте існує ризик втрати або крадіжки носія, а також можливість його клонування. Третій підхід — біометричні методи [2], які використовують унікальні фізіологічні параметри людини, такі як відбитки пальців, скан сітківки або розпізнавання обличчя. Біометрія забезпечує високу точність ідентифікації, проте потребує дорогого обладнання та піднімає питання конфіденційності даних.

Ще одна класифікація пов'язана з типом доступу, який контролює система – це фізичний доступ [3]. Він регулює проходи до приміщень, обладнання або серверних кімнат і часто використовує безконтактні зчитувачі, електромеханічні замки

чи турнікети. Логічний доступ контролює доступ до інформаційних систем, баз даних і мереж, використовуючи паролі, токени та сертифікати. Крім того, СКД можна розділити на централізовані та децентралізовані. Централізовані системи об'єднують всі дані про користувачів у єдиній базі, що забезпечує гнучке управління правами доступу та легке масштабування. Децентралізовані системи керують доступом локально, що зменшує навантаження на центральний сервер, але ускладнює підтримку цілісної політики безпеки.

1.1.2 Основні принципи функціонування систем

Основою роботи будь-якої СКД є взаємодія трьох процесів: ідентифікації, аутентифікації та авторизації [4]. Ідентифікація передбачає визначення користувача за унікальним ідентифікатором, таким як номер RFID-картки або логін у системі. Аутентифікація перевіряє достовірність цієї інформації та може здійснюватися однофакторно або багатфакторно, поєднуючи кілька методів підтвердження особи для підвищення рівня безпеки. Авторизація визначає, які дії дозволено виконувати користувачеві, і реалізується через політики доступу, ролі або атрибути. Сучасні СКД часто поєднують багатфакторну аутентифікацію та моніторинг дій користувачів, що дозволяє виявляти спроби несанкціонованого доступу.

1.1.3 Переваги та недоліки різних підходів до аутентифікації

Описані вище методи аутентифікації мають різні переваги та обмеження. Використання паролів та PIN-кодів дозволяє швидко впровадити систему, але такі методи уразливі до кібератак та потребують регулярної зміни даних для забезпечення безпеки. Використання фізичних носіїв, таких як безконтактні картки, забезпечує швидкий і зручний доступ, особливо в системах фізичного контролю, однак існує ризик втрати або клонування носія. Біометричні методи є найбільш точними та складними для підробки, проте їх впровадження вимагає значних фінансових

вкладень і піднімає питання захисту конфіденційності. Найбільш ефективними та безпечними є системи, що поєднують кілька методів, наприклад комбінацію PIN-коду та біометрії, що дозволяє мінімізувати ризики та забезпечити зручність користування.

1.2 Огляд існуючих рішень на ринку

Проектування системи контролю доступу вимагає аналіз сучасного ринку засобів безпеки, що дозволяє не лише ознайомитися з передовими технічними рішеннями, але й виявити типові недоліки або обмеження існуючих рішень. Сучасні виробники пропонують широкий спектр обладнання, що відрізняється за функціоналом, частотними діапазонами та рівнями захисту даних.

1.2.1. Комерційні RFID-системи

СКД на основі RFID [5] та суміжних технологій широко використовуються для управління доступом у корпоративних, промислових та громадських об'єктах. Вони поєднують швидкий і зручний контроль фізичного доступу з можливістю інтеграції з логічними системами та іншими компонентами безпеки. Розглянемо можливості та функції існуючих систем: HID Global (Hughes Identification Devices Global) [6], Dahua Technology [7], ATIS [8] та Keenfinity [9].

HID Global пропонує комплексні рішення для контролю доступу, які охоплюють як апаратні, так і програмні компоненти (рис. 1.1). Їхні системи базуються на NFC-технології з частотам в межах 860-960 МГц та підтримують багатофакторну аутентифікацію, включаючи поєднання карток, мобільних ключів та біометрії. Програмне забезпечення забезпечує централізоване управління правами доступу, моніторинг подій у режимі реального часу та інтеграцію з іншими системами безпеки, такими як відеоспостереження та сигналізація. Високий рівень шифрування

даних та захист від клонування RFID-карток забезпечують надійний контроль доступу навіть у великих корпоративних комплексах.



Рисунок 1.1 – Продукція Hughes Identification Devices

У своїх пристроях Hid Global застосовує радіочастоти 125 кГц (LF) та 13,56 МГц (HF). Картки LF частоти, такі як HID Prox та Indala, використовуються у простих системах, що потребують базового рівня захисту. Більш сучасні рішення — iCLASS, MIFARE Classic та DESFire [10] — працюють на HF частоті і забезпечують підвищений рівень безпеки завдяки криптографічним алгоритмам та можливості зберігати кілька ідентифікаційних профілів на одній картці. Крім того, Hid Global активно впроваджує технологію Seos, що дозволяє використовувати смартфони як ключі доступу через NFC або Bluetooth.

Рішення HID Global підтримують стандарти ISO/IEC 14443 [11] та 15693 [12], що забезпечує сумісність із широким спектром карт і зчитувачів. Завдяки мультиформатним пристроям можна одночасно використовувати різні типи носіїв — наприклад, старі 125 кГц карти та нові 13,56 МГц ідентифікатори, що спрощує модернізацію систем без необхідності повної заміни обладнання.

Hid Global використовує 128-бітне шифрування AES [13], динамічну аутентифікацію та захист від клонування. Системи підтримують централізоване керування, ведення журналів подій та інтеграцію з іншими мережевими рішеннями безпеки. Таким чином, HID Global поєднує надійність перевірених технологій і сучасні методи захисту, забезпечуючи стабільну роботу систем доступу різного рівня складності.

До переваг даної системи можна віднести високий рівень криптографічного захисту. Класичні LF-картки на частоті 125 кГц, такі як HID Prox і Indala, застосовуються у базових системах, тоді як більш захищені платформи iCLASS, MIFARE та DESFire на 13,56 МГц пропонують розширені можливості, включно з багатопрофільною ідентифікацією та використанням складних криптоалгоритмів. Окрему роль відіграє технологія Seos, яка дозволяє використовувати смартфони як повноцінні ключі доступу через NFC або Bluetooth та забезпечує найвищий рівень захисту від клонування.

Dahua Technology є одним з виробників систем безпеки, що спеціалізується на розробці комплексних рішень для відеоспостереження, контролю доступу, домофонів та інтегрованих систем безпеки. На ринку України продукція Dahua широко представлена та активно використовується в офісних приміщеннях, житлових комплексах, складських і промислових об'єктах. Компанія пропонує як автономні рішення для однієї точки проходу, так і масштабовані мережеві системи контролю доступу з централізованим керуванням.

У сфері контролю доступу Dahua випускає зчитувачі RFID-карт, контролери доступу, комбіновані пристрої з біометрією, а також комплекси для адміністрування прав доступу. Основу RFID-рішень складають зчитувачі, що працюють у HF діапазоні (13,56 МГц, стандарт MIFARE), а також моделі з підтримкою LF карт 125 кГц стандарту EM-Marine. Для підключення контролерів використовуються стандартні інтерфейси Wiegand або RS-485.

Системи контролю доступу Dahua (рис. 1.2) можуть працювати як у автономному режимі, так і у складі мережевих багатоточкових систем. В автономному режимі зчитувач обслуговує одну точку, зберігає базу користувачів та керує електрозамком через релейний вихід. У мережевому режимі кілька зчитувачів об'єднуються в єдину систему через спеціальний контролер за допомогою дротового з'єднання.



Рисунок 1.2 – Зчитувач Dahua Technology

Рішення Dahua для контролю доступу вирізняються широким модельним рядом. Вони сумісні з поширеними стандартами RFID, мають міцні та вологозахищені корпуси та можливість масштабування. До недоліків можна віднести необхідність прокладання дротових з'єднань між зчитувачами, контролерами та сервером для побудови багатоточкової системи, що ускладнює монтаж і підвищує вартість інфраструктури.

Компанія ATIS пропонує лінійку контролерів-зчитувачів (рис. 1.3) та комплектів для контролю доступу, орієнтованих переважно на локальні (автономні) системи для малих і середніх об'єктів: офіси, склади, житлові комплекси, готелі та ін. Продукти позиціонуються як практичні, недорогі й прості в монтажі рішення з базовим набором функцій, необхідних для контролю однієї або кількох точок проходу. ATIS випускає моделі з підтримкою двох основних радіотехнологій:

- EM-Marine — низькочастотні безконтактні картки чи брелоки для базового контролю доступу з робочою частотою 125 кГц. Такі картки застосовуються у вологозахищених і зовнішніх рішеннях.
- MIFARE Classic — HF-картки стандарту 13.56 МГц, що забезпечують більшу функціональність і можливість зберігання невеликого обсягу даних на картці.



Рисунок 1.3 – Продукція ATIS

ATIS-контролери мають типові інтерфейси для інтеграції у системи контролю доступу: релейні виходи для керування замком, звукову і світлову індикацію, можливість підключення кодової клавіатури або додаткового зчитувача. Деякі моделі підтримують підключення зовнішнього зчитувача або мають вбудоване реле для безпосереднього керування замком. Типові функції, доступні в моделях ATIS із каталогу:

- автономна робота для однієї точки проходу (непотрібний зовнішній сервер);
- збереження до 2000 карт у локальній пам'яті;
- налаштування режимів роботи замка (імпульсний, тригерний), тривалості відкривання;
- індикація доступу;
- вологозахищені варіанти для зовнішнього монтажу (IP66–IP68).

До переваг можна віднести простоту та швидкість впровадження. Пристрої постачаються як готові контролери-зчитувачі, що значно скорочує час монтажу та налаштування. Вони мають металеві корпуси, вологозахищені виконання, що забезпечує надійність у побутових чи комерційних умовах.

Рішення Keenfinity (рис. 1.4) інтегрують апаратну та програмну частину для комплексного контролю доступу, включаючи мобільний доступ, біометричну аутентифікацію та управління відвідувачами. Система підтримує централізоване

управління великими об'єктами та інтегрується з відеоспостереженням та іншими системами безпеки через відкриті протоколи. Компанія пропонує комплексні СКД, орієнтовані на середні та великі об'єкти, поєднуючи RFID-технології, мобільний доступ та біометрію. Основні частоти, що використовуються у системах, — 125 кГц для базових карток EM-Marine та 13,56 МГц для смарт-карток MIFARE Classic і DESFire, які підтримують шифрування і ускладнюють клонування.



Рисунок 1.4 – Продукція Keenfinity

Системи Keenfinity підтримують багатофакторну аутентифікацію, включно з картками, PIN-кодами, біометрією та мобільними ключами через NFC або Bluetooth. Зчитувачі можуть працювати на одній або обох частотах, що забезпечує сумісність зі старими та новими картками і гнучкість інтеграції. Для захисту даних використовуються сучасні протоколи та шифрування AES-128.

Перевагою Keenfinity є масштабованість та можливість використання мобільних ключів на смартфонах, що підвищує зручність користувачів та забезпечує додатковий рівень безпеки. Система забезпечує шифрування даних, багаторівневий контроль доступу та детальний аудит дій користувачів.

Усі приклади демонструють, що сучасні RFID-системи авторизації поєднують зручність, швидкість обробки даних та багаторівневий захист. Основні тенденції включають використання багатофакторної аутентифікації, інтеграцію з мобільним

доступом, централізоване управління правами та детальний аудит подій. Незалежно від розміру об'єкта, ключовим елементом є баланс між безпекою та зручністю користування, що досягається через комбінацію апаратних засобів, програмного забезпечення та захисту даних.

1.2.2. Порівняльний аналіз комерційних систем RFID

Аналіз сучасних комерційних систем авторизації на базі RFID дозволяє виділити ключові аспекти, що впливають на вибір конкретного рішення, включно з функціональністю, рівнем безпеки, масштабованістю та інтеграційними можливостями. Усі характеристики занесено до таблиці 1.

Таблиця 1.1 – Порівняльний аналіз систем доступу

Параметр порівняння	HID Global	Dahua Technology	ATIS	Keenfinity
Тип технології	RFID (LF 125 кГц, HF 13,56 МГц), NFC, Bluetooth	RFID (LF 125 кГц, HF 13,56 МГц)	RFID (125 кГц, 13,56 МГц), клавіатура	RFID, мобільний доступ, біометрія
Типи карток	HID Prox, iCLASS, MIFARE, DESFire, Seos	EM-Marine, MIFARE	EM-Marine, MIFARE	EM-Marine, MIFARE Classic, DESFire, біометрія, мобільні ключі
Методи аутентифікації	Багатофакторна: картка + PIN + біометрія	RFID-картки, PIN-код	Картка + PIN, опційно двофакторна	Картка, мобільний ключ, біометрія, PIN

Продовження таблиці 1.1

Захист даних	AES-128, динамічні ключі, антиклонування	Базова перевірка UID	Базовий захист (Crypto-1 для MIFARE Classic), Wiegand	AES-128, контроль сесій
Масштабованість	Висока	Середня	Середня	Висока, модульна структура
Інтеграція	Відеоспостереження, сигналізація, ІТ-системи	Інтеграція з відеоспостереженням, домофонами	Контроль електрозамків, охоронні панелі	Відеоспостереження, мобільні додатки
Особливості	Мобільні ключі (Seos®), API для сторонніх систем	Простота впровадження, локальна пам'ять	Локальна пам'ять користувачів, простота налаштування	Гнучке налаштування прав, хмарне управління

Попри широкий функціонал і високий рівень безпеки, кожна з проаналізованих систем демонструє певні обмеження. HID Global забезпечує максимальну захищеність, але її рішення є дорогими, складними в інтеграції та орієнтованими насамперед на великі корпоративні об'єкти, що робить їх надлишковими для невеликих систем. Dahua Technology, навпаки, пропонує доступність і простоту впровадження, однак використовує базові механізми перевірки UID. ATIS також надає лише базовий рівень захисту (MIFARE Classic), має обмежену масштабованість та орієнтується на прості локальні системи без розширених можливостей інтеграції. Keenfinity, хоч і підтримує мобільний доступ і біометрію, має вищу вартість, складнішу конфігурацію та орієнтується переважно на комплексні рішення, що не завжди зручно для автономних або бюджетних об'єктів. Варто також зазначити, що всі розглянуті комерційні системи для забезпечення масштабованості потребують

прокладання дротових з'єднань між зчитувачами та центральним модулем, що ускладнює монтаж і підвищує загальну вартість впровадження.

Наявність зазначених обмежень і стало причиною розробки власної RFID-системи. Запропоноване рішення поєднує бездротову архітектуру обміну даними, компактність, високий рівень захисту передавання інформації, локальне збереження БД користувачів та можливість її редагування через мобільний телефон. Система є легко масштабованою без прокладання додаткових кабельних мереж й забезпечує гнучке налаштування прав доступу. Таким чином, власна розробка забезпечує збалансоване поєднання безпеки, зручності та функціональності, що бракує більшості існуючих комерційних рішень у даному сегменті.

1.3 Технологія RFID

Сучасні СКД дедалі частіше базуються на технології RFID, що дозволяє безконтактно ідентифікувати об'єкти та користувачів за допомогою радіочастотних сигналів. RFID забезпечує швидкий обмін даними між міткою та зчитувачем, без необхідності фізичного контакту, що робить цю технологію особливо зручною для контролю доступу, обліку ресурсів, транспортування та багатьох інших сфер.

1.3.1 Історія і розвиток технології

Технологія RFID бере свій початок у середині XX століття, коли були розроблені перші радіочастотні системи ідентифікації для військових цілей, зокрема для розпізнавання літаків під час Другої світової війни [14]. З існуючою на той час технологією RADAR неможливо було визначити, чи є літак, що наближається, дружнім чи ворожим. Це призвело до розробки системи під назвою «ідентифікація друг чи ворог» (рис. 1.5).

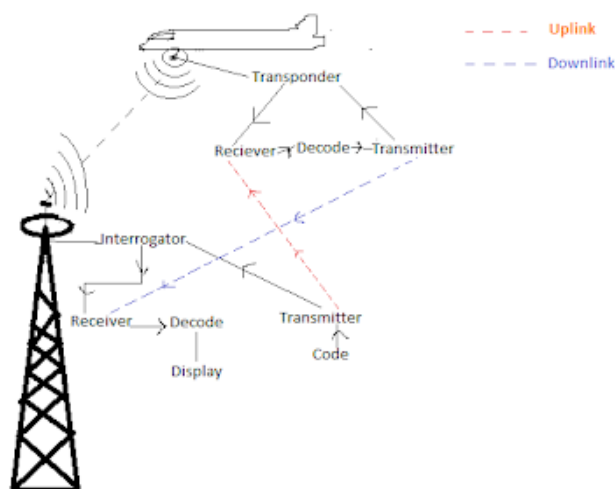


Рисунок 1.5 – Система «ідентифікація друг чи ворог»

У 1970–1980-х роках технологія почала активно застосовуватися у промисловості для контролю складів і логістики [15]. З кінця 1990-х років RFID активно впроваджується в комерційні продукти, включно з системами авторизації, транспортними картками та пропускними системами, завдяки здешевленню виробництва міток і підвищенню надійності зчитувачів. Сьогодні RFID є стандартною технологією для контролю доступу та ідентифікації користувачів у багатьох сферах, поєднуючи швидкість, безконтактність та безпеку передачі даних.

1.3.2 Типи RFID-міток та зчитувачів

RFID-мітки [16] поділяються на пасивні (рис. 1.6) та активні (рис. 1.7):

- Пасивні мітки не мають власного джерела живлення і отримують енергію від радіосигналу зчитувача. Вони мають менший радіус дії (від кількох сантиметрів до кількох метрів), але відрізняються компактністю та низькою вартістю. Завдяки цьому пасивні мітки найчастіше застосовуються у системах авторизації та контролю доступу, де потрібна висока кількість носіїв з мінімальними витратами.

- Активні мітки оснащені власним джерелом живлення, що дозволяє збільшити радіус дії до десятків метрів. Такі мітки використовуються переважно для обліку рухомих об'єктів на великих територіях та у складних логістичних системах.



Рисунок 1.6 – Різновиди пасивних RFID-міток



Рисунок 1.7 – Різновиди активних RFID-міток

Зчитувачі RFID також поділяються за типом застосування. Стационарні зчитувачі встановлюються на турнікетах або дверях і забезпечують контроль великих

потоків користувачів. Мобільні або портативні зчитувачі дозволяють перевіряти носії у полі або на виробничих ділянках, що підвищує гнучкість використання системи. Сучасні зчитувачі можуть підтримувати кілька стандартів одночасно та здійснювати шифрування даних для захисту інформації.

1.3.3 Частотні діапазони та стандарти

RFID-системи працюють у різних радіочастотних діапазонах, що визначає, дальність дії та сферу застосування:

- Низькочастотний (LF, 125–134 кГц) діапазон характеризується невеликою дальністю дії (5-10 см) та високою стійкістю до металевих перешкод. Використовується у СКД, тваринництві та деяких промислових застосуваннях.
- Високочастотний (HF, 13,56 МГц) діапазон використовується у смарт-картках, проїзних документах, RFID-картках для контролю доступу. Стандарти HF включають ISO/IEC 14443 та ISO/IEC 15693, що регламентують сумісність міток та зчитувачів. Дальність зчитування у таких карток становить 2-5 см.
- Надвисокочастотний (UHF, 860–960 МГц) діапазон забезпечує дальність дії від кількох метрів до десятків метрів, що робить його придатним для логістики, складів та транспортування. Основні стандарти — ISO/IEC 18000-6C та EPCglobal Gen2, які визначають протоколи взаємодії та захист даних.

Вибір частотного діапазону залежить від конкретних завдань. СКД зазвичай використовують HF, що забезпечує безконтактність і захист від несанкціонованого зчитування.

1.4 Безпека та протоколи передачі даних у RFID

Питання інформаційної безпеки є ключовим елементом у сучасних СКД, оскільки процес безконтактного зчитування даних супроводжується ризиком їх

перехоплення, модифікації або несанкціонованого копіювання. З огляду на активне використання RFID-технологій у системах контролю доступу, платіжних рішеннях, транспортній інфраструктурі й логістичних процесах, виникає потреба у впровадженні надійних криптографічних та протоколів аутентифікації, які забезпечують конфіденційність та цілісність переданої інформації.

1.4.1 Методи шифрування та аутентифікація

Одним з головних аспектів захисту є криптографічне кодування даних, що передаються між RFID-міткою та зчитувачем. Найпростіші та найстаріші RFID-системи, такі як мітки стандарту EM-Marine або інші LF-мітки, працюють без шифрування [17]. Дані передаються у відкритому вигляді, що робить їх вразливими до копіювання та відтворення. У відповідь на це в сучасних системах почали застосовувати багаторівневі механізми криптографічного захисту.

Аутентифікація в RFID-системах – це процес взаємного підтвердження достовірності RFID-мітки та зчитувача до обміну основними даними. Типовим підходом є використання процедур виклику-відповіді: зчитувач генерує випадкове число, яке мітка шифрує за допомогою секретного ключа і повертає у відповідь. Якщо відповідь коректна, сторони вважаються автентичними. Така модель запобігає підробці RFID-мітки, оскільки знання секретного ключа є необхідною умовою для правильної генерації криптографічної відповіді.

У різних технологічних стандартах реалізовано власні алгоритми аутентифікації. Наприклад, у MIFARE Classic використовуються механізми Crypto-1, хоча сучасні дослідження засвідчили їх уразливість до низки крипто-атак. Натомість у картах сімейства MIFARE DESFire застосовуються значно надійніші алгоритми — 3DES та AES, що відповідають сучасним вимогам безпеки.

AES-128 сьогодні є одним з найрозповсюдженіших симетричних алгоритмів шифрування в СКД завдяки його високій стійкості до криптографічного аналізу та оптимальності для апаратної реалізації. Він використовується у широкому спектрі

безпекових протоколів, включно з RFID-картами нового покоління, електронними паспортами та безконтактними платіжними системами.

Основні переваги AES-128:

- висока криптографічна стійкість -- перебір ключів є практично неможливим у межах сучасних обчислювальних можливостей;
- ефективність апаратної реалізації -- алгоритм добре піддається оптимізації у мікроконтролерах і радіочастотних модулях;
- підтримка у стандартизованих протоколах, зокрема у MIFARE DESFire.

1.4.2 Вразливості та загрози

Попри наявність механізмів шифрування, RFID-системи залишаються вразливими до низки атак. Найпоширенішими є:

- перехоплення сигналу, де зломисник може зчитати дані з RFID-мітки за допомогою потужнішого зчитувача на відстані;
- клонування та впровадження підроблених міток. Після перехоплення ідентифікатора створюється копія картки, що дозволяє несанкціонований доступ.

Також уразливість може бути спричинена недосконалістю програмного забезпечення, наприклад, відсутністю перевірки унікальності UID. При розробці СКД варто враховувати, що окремі типи карток (зокрема ранні версії MIFARE Classic) мають нижчий рівень криптографічного захисту порівняно із сучасними реалізаціями MIFARE DESFire або NFC.

1.5 Висновки до розділу 1

Проведений аналіз сучасних RFID-технологій показав, що питання інформаційної безпеки є одним із найважливіших для ефективної та надійної роботи систем безконтактної ідентифікації. Найпростіші RFID-мітки передають інформацію у

відкритому вигляді та не мають вбудованого криптографічного захисту, що створює ризики клонування карток і перехоплення даних. Саме тому в сучасних системах широко застосовуються криптографічні методи захисту, взаємна аутентифікація та апаратні засоби безпеки. Найпоширенішим алгоритмом симетричного шифрування є AES-128, який забезпечує високий рівень захищеності та добре підходить для використання в апаратних реалізаціях.

Додаткову роль у захисті інформації відіграють механізми контролю цілісності даних, зокрема криптографічні коди автентичності, які дозволяють вчасно виявляти помилки передачі або спроби підміни даних. Також сучасні RFID-чіпи оснащуються апаратними механізмами безпеки, такими як захищені зони пам'яті.

Отже, надійний захист RFID-систем досягається завдяки поєднанню шифрування, аутентифікації та апаратних механізмів безпеки. У межах цього розділу розглянуто використання алгоритму AES-128 для захисту переданих даних та зберігання інформації безпосередньо на RFID-картці.

2. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ

2.1 Розробка структурних схем апаратної частини

Оскільки розроблювана СКД мінімально складається з головного та другорядного пристроїв, необхідно сформувати їх структурні схеми, що дозволяє визначити логіку взаємодії між компонентами. Спочатку було сформовано структурну схему апаратної частини ГП, що наведена на рисунку 2.1. Вона відображає всі основні елементи та зв'язки між ними. Даний пристрій виконує роль центрального елемента системи, який відповідає за обробку інформації та керування доступом.

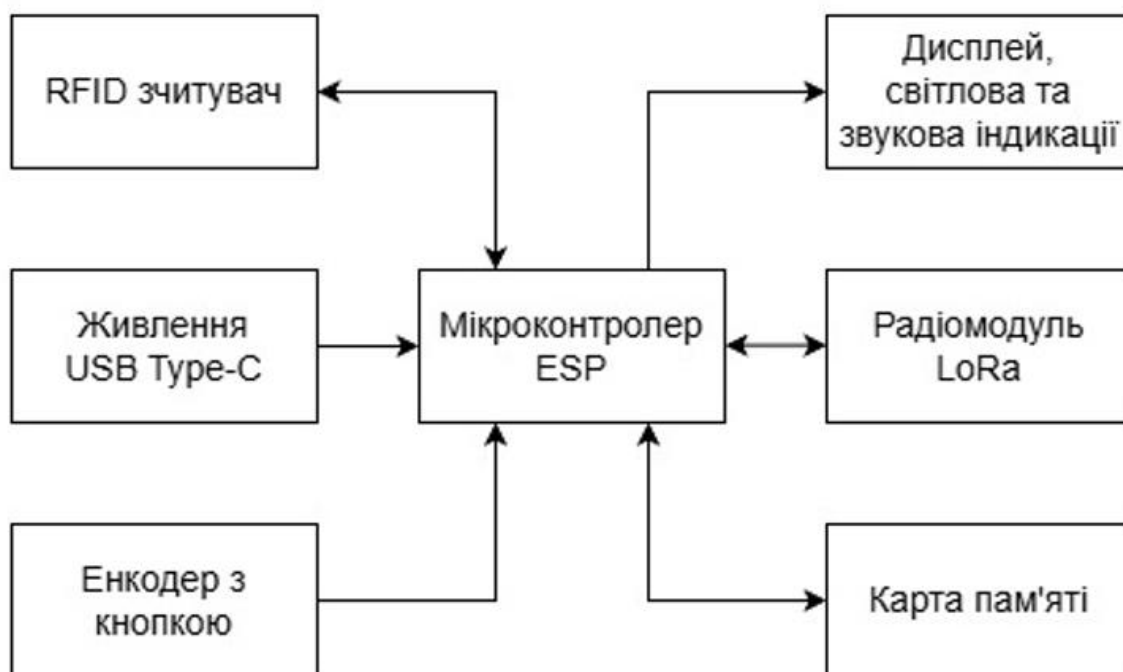


Рисунок 2.1 – Структурна схема ГП

Мікроконтролер ESP [18] є центральним елементом ГП, що виконує координацію роботи системи: прийом подій від локального зчитувача RFID, обробка запитів й повідомлень від ДП по LoRa, доступ до локальної файлової системи на карті пам'яті та надання веб-інтерфейсу для адміністрування.

RFID-зчитувач підключається до мікроконтролера по апаратній шині SPI. Використовується для локального сканування карток MIFARE Classic. Зчитувач

отримує UID й дані секторів. Протокол обробки та політика доступу реалізуються на стороні мікроконтролера.

Дисплей, світлова та звукова індикації відображають стан системи (очікування картки, результат авторизації, повідомлення). Дисплей підключається по інтерфейсу I2C. RGB-світлодіод слугує для швидкої візуальної зворотної реакції типу успіх, відмова або помилка.

Радіомодуль LoRa [19] забезпечує бездротовий зв'язок між головним і другим пристроями. Підключається по SPI. ГП отримує повідомлення з UID від ДП й відправляє повідомлення у відповідь на запит.

Карта пам'яті виконує роль локального сховища БД карток у форматі CSV. В ролі фізичного органу керування для навігації по локальному меню та підтвердженні дій обрано енкодер з кнопкою. Для живлення пристрою обрано USB Type-C. На платі встановлено понижувальний стабілізатор на 3.3 В для мікроконтролера і периферії.

Далі наведено структурну схему апаратної частини ДП (рис. 2.2).



Рисунок 2.2 – Структурна схема ДП

Мікроконтролер ESP, RFID-зчитувач, радіомодуль LoRa, світлова та звукова індикації, живлення через USB Type-C – є такими самими як і в головному пристрої.

В ДП присутні реле, MOSFET-транзистор та виводи GPIO мікроконтролера для підключення зовнішньої периферії, наприклад електрозамок. ДП реалізує сканування RFID, локальну логіку зчитування та передає інформацію на ГП по LoRa.

2.2 Вибір елементної бази та обґрунтування

Після розробки структурних схем системи наступним етапом є визначення конкретних електронних компонентів. Головними критеріями при підборі компонентів слугували: повна апаратна сумісність, наявність необхідних комунікаційних інтерфейсів, підтримка сучасних середовищ розробки, а також доступність на ринку. У даному підрозділі наведено технічне обґрунтування вибору ключових вузлів системи.

2.2.1 Вибір мікроконтролера

Мікроконтролер повинен забезпечити одночасну роботу локального інтерфейсу (дисплей, енкодер з кнопкою), RFID-зчитувача, карти пам'яті для зберігання БД у форматі CSV, радіомодулю LoRa для зв'язку, керування реле, MOSFET-транзистором, світловою та звуковою індикаціями, а також забезпечувати веб-інтерфейс для користування пристроєм і бездротове оновлення прошивки. ESP32 [20] обрано за рахунок вбудованих інтерфейсів (SPI, I2C, UART, достатньої кількості GPIO), підтримки Wi-Fi для локального веб-інтерфейсу і достатньої обчислювальної потужності для роботи з CSV-базою та логікою авторизації (рис. 2.3).



Рисунок 2.3 – Мікроконтролер ESP32

Інтегрований радіоінтерфейс Wi-Fi забезпечує можливість реалізації локального веб-інтерфейсу на пристрої без додаткових модулів (зручне редагування бази, OTA). Це значна перевага перед MCU без вбудованого Wi-Fi. Даний мікроконтролер має двоядерний процесор і достатній обсяг вбудованої пам'яті, що дозволяють обробляти CSV-файли, шифрування, роботу LoRa та інших асинхронних дій без помітних затримок. В екосистемі ESP32 існує велика кількість стабільних бібліотек для роботи з обраними в наступних підрозділах модулями, що спрощує розробку прототипу.

2.2.2 Вибір RFID-зчитувача

MFRC522 – це популярний і доступний зчитувач [21] з частотою роботи антени 13.56 МГц (рис. 2.4). Підключається по SPI, має компактний форм-фактор, низьку вартість і реалізований у багатьох прикладах для ESP32 — це робить його придатним для прототипування систем контролю доступу. До переваг варто віднести його низьку ціну, широку доступність, просту інтеграцію та коротку робочу дистанцію. З врахуванням поставлених вимог та з можливістю подальшого розвитку проекту в якості карток використано MIFARE Classic (13.56 МГц, ISO14443).

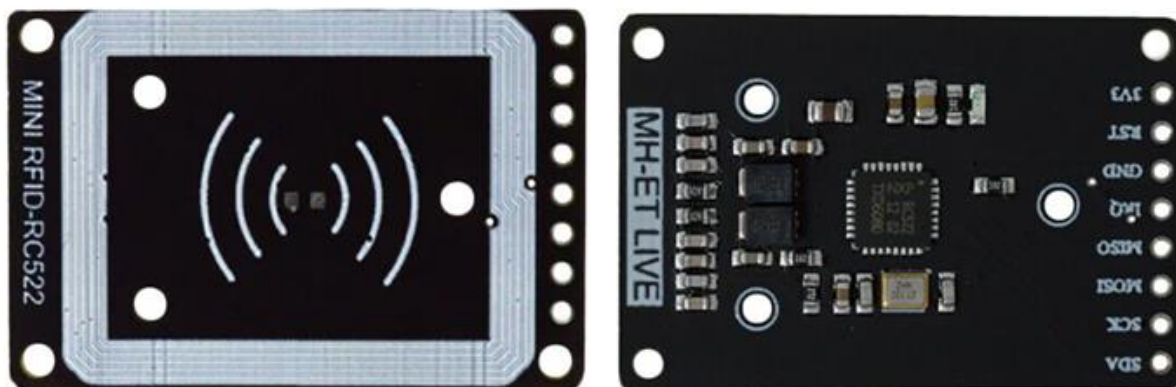


Рисунок 2.4 – Модуль MFRC522

2.2.3 Вибір радіомодуля LoRa

Модуль SX1278 один із найбільш розповсюджених та доступних радіомодулів стандарту LoRa [22], призначений для роботи на частоті 433 МГц (рис. 2.5). Модуль підтримує довготривалий зв'язок на великі відстані завдяки використанню розширеної модуляції з лінійною частотною модуляцією, що забезпечує високу чутливість приймача та стійкість до завад [23]. SX1278 працює через інтерфейс SPI, що дозволяє без проблем інтегрувати його з платформою ESP32. До його ключових переваг належать низька вартість, стабільна робота в умовах перешкод, наявність великої кількості бібліотек та прикладів реалізації.

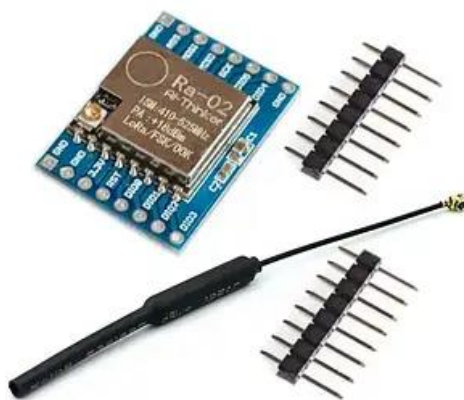


Рисунок 2.5 – Модуль SX1278

2.2.4. Вибір дисплею, світлової та звукової індикації

Для візуальної індикації в головному пристрої використано дисплей SSD1306 (рис. 2.6), який відзначається компактними розмірами, низьким енергоспоживанням та високою контрастністю зображення. Дисплей керується за допомогою інтерфейсом I2C, що мінімізує кількість необхідних виводів мікроконтролера та спрощує підключення до ESP32. Наявність великої кількості бібліотек і прикладів для цього контролера робить його зручним рішенням для відображення службової інформації, статусів системи, повідомлень та діагностичних даних.



Рисунок 2.6 – Дисплей SSD1306

Світлова індикація реалізована через RGB-світлодіод діаметром 5 мм зі спільним катодом (рис. 2.7), що дозволяє відображати різні стани системи за допомогою кольорів. Такий вид індикації є інтуїтивно зрозумілим для кінцевого користувача: зелений сигналізує про успішний доступ, червоний – про відмову, синій може використовуватися для позначення режимів налаштування чи очікування, а комбіновані кольори – для спеціальних режимів роботи. Підключення RGB-світлодіода до ESP32 через три окремі GPIO забезпечує гнучке керування всією палітрою кольорів.



Рисунок 2.7 – RGB-світлодіод

Для звукової індикації обрано бузер MLT-8530 (рис. 2.8), який відзначається малими розмірами, низьким енергоспоживанням і здатністю формувати чіткі короткі звукові сигнали. Бузер застосовується для підтвердження натискань кнопок, сигналізації про коректне чи некоректне сканування картки та для привернення уваги користувача у випадку системних подій. Компактність MLT8530 дає змогу легко інтегрувати його у друковану плату й корпус.



Рисунок 2.8 – Бузер MLT-8530

2.2.5. Вибір органів керування

Для взаємодії користувача з системою на ГП було обрано механічний енкодер із вбудованою тактовою кнопкою (рис. 2.9). Дане рішення є оптимальним для переміщення по меню, оскільки дозволяє одночасно виконувати два види дій:

поворот (вибір пунктів меню, навігація) та натискання (підтвердження вибору, активація команд). Енкодер забезпечує високу точність та зручність керування завдяки тактильним відчуттям, що робить його інтуїтивно зрозумілим навіть без додаткових елементів інтерфейсу.



Рисунок 2.9 – Енкодер з кнопкою

Для другорядного пристрою обрано більш простий елемент управління – тактова кнопка (рис. 2.10). Вона виконує роль локального фізичного тригера, який використовується для вибору режиму при завантаженні. Такий вибір обумовлений тим, що функціональні можливості другорядного пристрою значно простіші порівняно з головним вузлом, і він не потребує складної системи меню чи багатоетапної взаємодії з користувачем.



Рисунок 2.10 – Тактова кнопка

2.2.6. Вибір карти пам'яті

Для локального зберігання БД користувачів у ГП використано стандартну карту пам'яті формату micro-SD [24], підключену через відповідний слот (рис. 2.11). micro-SD обрана завдяки своїй доступності та компактності. Слот підключається через інтерфейс SPI, що дозволяє інтегрувати його у систему разом із модулями MFRC522 та SX1278 завдяки використанню окремих ліній CS. Форматування карти у FAT32 та використання стандартних бібліотек спрощують роботу з файлами та зберігання даних у форматі CSV.



Рисунок 2.11 – Слот та карта пам'яті формату micro-SD

2.2.7. Вибір реле та MOSFET-транзистора

Для керування виконавчими елементами в ДП використано електромеханічне реле на 220 В, що активується керуючим сигналом 5 В (рис. 2.12). Такий тип реле є простим та надійним рішенням для комутації мережевих навантажень, зокрема електрозамків чи інших пристроїв, що потребують гальванічної розв'язки від низьковольтної частини схеми.



Рисунок 2.12 – Реле

Для комутації низьковольтних навантажень та швидкодіючих ланцюгів обрано MOSFET-транзистор A09T (рис. 2.13), який є польовим транзистором із низьким опором каналу при напрузі затвора 3.3 В. Це дає змогу безпосередньо керувати ним від ESP32 без додаткових драйверів. A09T може комутувати навантаження зі споживанням струму 2.5 А та напругою до 30 В.



Рисунок 2.13 – MOSFET-транзистор

2.2.8. Вибір роз'єму живлення

Для підведення живлення до пристроїв обрано 6-піновий роз'єм USB Type-C (рис. 2.14). Цей роз'єм забезпечує надійну механічну фіксацію, зручність підключення та універсальність, оскільки кабелі USB-C є розповсюдженими. Використання 6-пінової конфігурації дозволяє реалізувати базові функції подачі напруги 5 В згідно зі стандартом USB-C без підтримки повноцінного Power Delivery. Такий роз'єм забезпечує стабільне живлення для ESP32 та периферійних модулів.



Рисунок 2.14 – Роз'єм живлення USB Type-C

2.3 Розробка електричних принципових схем

Структурна схема ГП була розроблена та обґрунтована у підрозділі 2.1, на основі якої виконано подальше проєктування електричної принципової схеми, що наведена у додатку А. До її складу входять як готові модулі, так і окремі елементи, розміщені безпосередньо на друкованій платі.

Мікроконтролер ESP32-WROOM-32E є центральним елементом головного пристрою. У схемі враховано резистор та конденсатор підтягування для лінії EN.

Подавання живлення до пристрою здійснюється через роз'єм USB Type-C, який обраний як найбільш сучасний, механічно зносостійкий і сумісний зі стандартними адаптерами 5 В. У схемі реалізовано базову конфігурацію USB Type-C з резисторами R6 і R8 на контактах A5 і B5, що задає пристрою роль споживача живлення. Це дозволяє працювати з будь-яким стандартним зарядним пристроєм без реалізації протоколу USB Power Delivery.

Після входу застосовані керамічні конденсатори 104, розміщені максимально близько до роз'єму, що забезпечує первинне приглушення високочастотних завад. Напруга живлення 5 В, що надходить із роз'єму, безпосередньо використовується для живлення дисплея.

Оскільки основні модулі пристрою, такі як ESP32-WROOM, SX1278, та MFRC522 живляться від напруги 3.3 В, тому у схемі передбачено лінійний стабілізатор з низьким рівнем власних шумів. Лінійний стабілізатор навідріз від імпульсних перетворювачів не створює високочастотних пульсацій, що особливо важливо для радіочастотних модулів. Навколо стабілізатора застосовано набір фільтрувальних конденсаторів (C8 на вході та C11 на виході), що відповідає рекомендаціям виробника мікросхеми.

SPI є загальною шиною для MFRC522, SX1278 та карти пам'яті. LoRa-модуль на схемі підключений до SPI з окремим CS та лініями RST й DIO0 для обробки. Даний радіомодуль має на собі розпаяні компоненти, тому не потребує додаткової обв'язки.

Енкодер з кнопкою підключений до мікроконтролера з усією необхідною обв'язкою, яка включає підтягувальні резистори та фільтруючі конденсатори, що забезпечують стабільне зчитування імпульсів та усунення брязкоту контактів.

Бuzzer, що є звуковою індикацією, підключено за схемою що приведена у дашиті. Паралельно бужеру встановлено діод Шоткі для захисту транзистора та мікроконтролера від високовольтних імпульсів, які виникають при вимиканні струму.

Структурна схема ДП також була розроблена та обґрунтована у підрозділі 2.1, на основі якої виконано проєктування електричної принципової схеми, котра наведена у додатку Б. До її складу також входять як готові модулі, так і окремі елементи,

розміщені безпосередньо на друкованій платі. ДП має таку ж саму топологію побудови, як і в ГП, за винятком відсутності дисплея, карти пам'яті та енкодера з кнопкою.

На цьому пристрої наявне реле для керування виконавчим механізмом (наприклад, електрозамком). Паралельно реле встановлено діод Шоткі для захисту транзистора та мікроконтролера від високовольтних імпульсів, які виникають при вмиканні струму. Встановлено MOSFET-транзистор для подачі напруги +5 В на вихідний роз'єм.

2.4 Макетне моделювання

На цьому етапі виконано апаратне формування прототипів двох пристроїв СКД на макетній платі. Основним завданням збирання було налагодити коректну взаємодію всіх периферійних компонентів із мікроконтролером ESP32 перед створенням друкованої плати.

2.4.1 Збирання апаратних модулів на макетній платі

Збирання розпочато з підготовки макетної плати, розведення живлення та формування загальної шини 5 В (рис. 2.15). Мікроконтролер ESP32 розташований на спеціальному програматорі. В якості джерела живлення використовується USB, що підключається до плати програматора. Далі на макетну плату послідовно встановлено основні модулі, а саме MFRC522, SX1278, карту пам'яті, RGB світлодіод та дисплей, що з'єднуються з мікроконтролером макетними дротами.

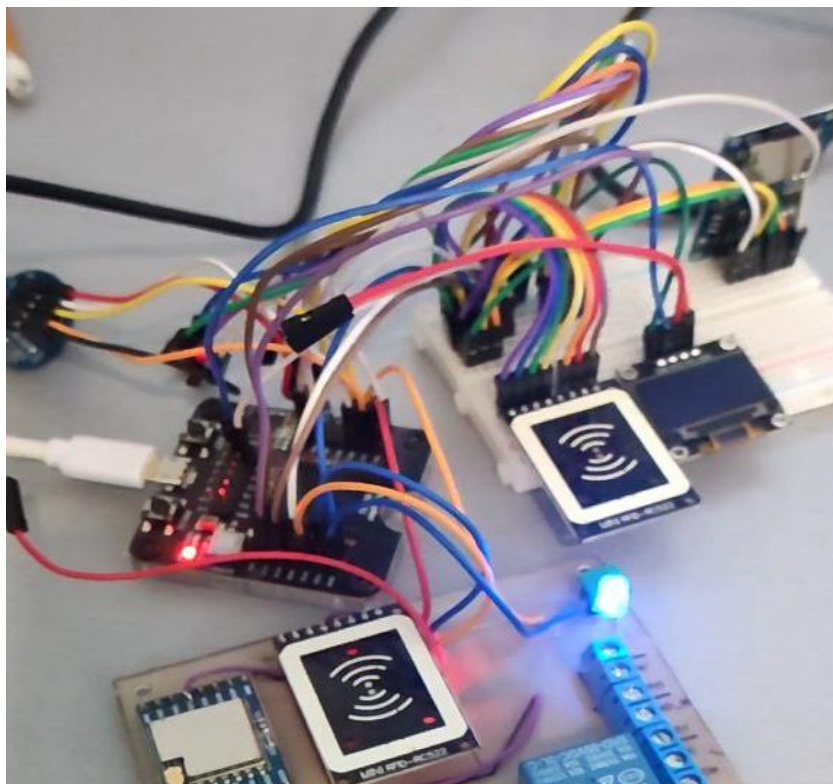


Рисунок 2.15 -- Прототип на макетній платі

До ESP32 під'єднано RFID-зчитувач, радіомодуль LoRa та карту пам'яті, котрі працюють через SPI-інтерфейс. З огляду на те, що SPI-шина в системі спільна для двох модулів, було передбачено індивідуальний пін CS для LoRa, RF-модуля та карти пам'яті. Це дозволяє уникати конфліктів на шині та забезпечує паралельну роботу модулів без помилок. LoRa-модуль винесено за межі плати, щоб антена мала достатній відступ від металевих ділянок та інших компонентів. Це необхідно для забезпечення максимальної дальності зв'язку, оскільки модуль LoRa чутливий до розміщення антени та близьких джерел шуму.

Після встановлення ключових модулів виконано з'єднання допоміжних компонентів: енкодера з кнопкою, світлодіоду, дисплея на ГП. Світлодіоди підключено через обмежувальні резистори. Усі модулі живляться від стабілізованої напруги 3.3 В, котру видає програматор мікроконтролера ESP32. Здійснено перевірку коректності розведення живлення, цілісності ліній даних та надійності механічних контактів.

2.4.2 Випробування базових функцій та перевірка взаємодії модулів

Проведено тестування базових функціональних можливостей системи з метою перевірки коректності роботи окремих компонентів, а також їх взаємодії між собою. Виконана поетапна перевірка кожного модуля, що дозволило локалізувати можливі проблеми та забезпечити стабільне функціонування системи перед об'єднанням усіх складових у єдиний пристрій.

Першою частиною тестування стало випробування RFID-зчитувача MFRC522. Для модуля завантажено мінімальний тестовий код, який ініціалізує радіочастотний чип та подає інформацію про його готовність через послідовний порт. Після запуску скетчу проводилося піднесення MIFARE Classic карток до антени RFID-зчитувача з різних відстаней та під різними кутами. Основним завданням було перевірити стабільність зчитування UID карток, коректність обробки команд модуля та відсутність збоїв під час повторних запитів. На цьому етапі зафіксовано стартове повідомлення про успішну ініціалізацію MFRC522 та виконано сканування картки (рис. 2.16).

The image shows a screenshot of an IDE with a code editor and a Serial Monitor window. The code in the editor is for initializing an RFID module (MFRC522) and printing information to the serial port. The Serial Monitor window shows the output of the code, including the initialization status and the UID of a scanned card.

```

1294 //===== RFID =====
1295 rfid.PCD_Init();
1296 rfid.PCD_SetAntennaGain(rfid.RxGain_max); // Установка підсилення антени
1297 rfid.PCD_AntennaOff(); // Перезавантаження антени
1298 delay(50);
1299 rfid.PCD_AntennaOn(); // Вмикаємо антену
1300 Serial.println("RFID ініціалізовано");
1301 oled.println("RFID -> OK");
-----

```

PROBLEMS 2 OUTPUT DEBUG CONSOLE TERMINAL PORTS SERIAL MONITOR

+ Open an additional monitor

Monitor Mode Serial View Mode Text Port COM7 - USB-Enhanced-SERIAL CH9102 (COM7) Baud rate

Stop Monitoring

OLED: Очікую картку...
 RFID ініціалізовано
 Стандартний ключ не підходить!
 Data: 0x18, 0x2F, 0xE8, 0x1F, 0x84, 0xAB, 0xCD, 0x2F, 0x37, 0xE8, 0x1F, 0x84, 0xFF, 0xAB, 0xCD,
 UID: 82F50B06
 Невідомий UID!

Рисунок 2.16 – Ініціалізація модуля та результат зчитування картки у послідовний монітор комп'ютера

Далі проведено тестування роботи радіомодуля LoRa SX1278. На першому етапі модуль було протестовано в односторонньому режимі — у вигляді передачі

фіксованого повідомлення ГП та приймання його ДП. У тестовому коді ініціалізуємо LoRa-модуль, налаштовуємо на робочу частоту, потужність та параметри модуляції, після чого відправляємо тестовий пакет. У діагностичному моніторі на комп'ютері відображаються діагностичні повідомлення про успішну ініціалізацію та дані пакету прийняті від другорядного пристрою (рис. 2.17, а). Після підтвердження одностороннього зв'язку перевірено двосторонню комунікацію — передавання та отримання даних між двома пристроями з короткими інтервалами, що дозволило переконатися у стабільності каналу (рис. 2.17, б).

```

978 void handleIncomingPacket()
979 {
980   int packetSize = LoRa.parsePacket(); // Перевіряємо, чи прийшов новий LoRa пакет
981   if (packetSize <= 0) // Якщо пакет не прийшов або його розмір 0
982     return; // Виходимо з функції, нічого робити не потрібно
983
984   uint8_t buf[256]; // Локальний буфер для зберігання пакета
985   int i = 0; // Лічильник зчитаних байтів
986   while (i < packetSize && LoRa.available() && i < (int)sizeof(buf)) // Читаємо, поки не досягли розміру пакета
987   { // I поки є доступні байти в LoRa буфері
988     buf[i] = LoRa.read(); // I поки не переповнили локальний буфер
989     i++; // Зчитуємо байт у buf[i] та збільшуємо i
990   }
991   Serial.print("Прийнято пакет розміром: ");
992   Serial.println(i); // Лог повідомлення про розмір пакета
993
994   if (i < 8 || buf[0] != PREAMBLE) // Мінімальний пакет 8 байт + перевірка преамбули
995     return; // Якщо менше 8 байт або неправильна преамбула – вихід
996
997   // Перевірка CRC пакета:
998   uint8_t rcv_crc = buf[i - 1]; // Останній байт пакета – CRC
999   if (crc8(buf, i - 1) != rcv_crc) // Перевіряємо CRC всіх попередніх байтів
1000  {
1001    // CRC не збігається
1002    return;
1003  }
1004
1005  String uidDeviceStr = "";
1006  for (uint8_t k = 0; k < uid_len; ++k) // Формуємо рядок для логу
1007  {
1008    if (uid_buf[k] < 0x10)
1009      uidDeviceStr += "0"; // Додаємо провідний нуль для однобайтових значень
1010    uidDeviceStr += String(uid_buf[k], HEX);
1011  }
1012  uidDeviceStr.toUpperCase(); // Приводимо до великих літер
1013  Serial.println(uidDeviceStr);
1014  show_on_display(LINE_UID, uidDeviceStr);
1015
1016  if (findUser(uidDeviceStr, name_DB, access_level_DB, date_time_DB)) // Перевіряємо, чи є користувач з таким UID
1017  {
1018    Serial.println("Прийнятий UID є в БД");
1019
1020    if (access_level_DB >= accessLevel)
1021    {
1022      logger.println(sets::logger::warn() + "UID: " + uidDeviceStr + " дозволено");
1023      buildAndSend(device, msgId, CMD_OPEN, NULL, 0);
1024    }
1025    else
1026    {
1027      logger.println(sets::logger::warn() + "UID: " + uidDeviceStr + " не дозволено");
1028    }
1029  }
1030  }
  
```

PROBLEMS 2 OUTPUT DEBUG CONSOLE TERMINAL PORTS SERIAL MONITOR

+ Open an additional monitor

Monitor Mode Serial View Mode Text Port COM7 - USB-Enhanced-SERIAL CH9102 (COM7) Baud rate 115200

Stop Monitoring

Прийнято пакет розміром: 24b
 REQ від: 1 msgId: 1 Назва: 'Test' UID картки: 82F50B06
 REQ від: 1 msgId: 2 Назва: 'Test' UID картки: 82F50B06
 REQ від: 1 msgId: 3 Назва: 'Test' UID картки: 82F50B06
 REQ від: 1 msgId: 4 Назва: 'Test' UID картки: 82F50B06

PROBLEMS 2 OUTPUT DEBUG CONSOLE TERMINAL PORTS SERIAL MONITOR

+ Open an additional monitor

Monitor Mode Serial View Mode Text Port COM7 - USB-Enhanced-SERIAL CH9102 (COM7) Baud rate 115200

Stop Monitoring

Прийнято пакет розміром: 24b
 REQ від: 1 msgId: 1 Назва: 'Test' UID картки: 82F50B06
 Відправлено CMD_OPEN до: 1 msgId: 1 UID картки: 82F50B06
 REQ від: 1 msgId: 2 Назва: 'Test' UID картки: 82F50B06
 Відправлено CMD_OPEN до: 1 msgId: 2 UID картки: 82F50B06

(a)

(б)

Рисунок 2.17 – Вивід інформації у серійний монітор: а - ініціалізація модуля та одностороннє прийняття пакету даних; б - двосторонній зв'язок

Наступним етапом стала перевірка роботи з картою пам'яті, що використовується у ГП для зберігання БД користувачів. SD-модуль підключений до ESP32 також через SPI, тому важливо переконатися, що спільне використання шини з LoRa та MFRC522 не викликає конфліктів. Під час тестування SD-модуль пройшов ініціалізацію, після чого виконувалась операція відкриття файлу, запису тестового рядка та подальшого читання цього ж файлу. Наведено скріншот успішної ініціалізації карти з фрагментом журналу, де показано створення тестового файлу та його читання (рис. 2.18).

```

1369 File file = SD.open(DB_FILE_NAME);
1370 if (!file)
1371 {
1372     Serial.println("Файл не знайдено");
1373     Serial.println("Створення файлу...");
1374     oled.println("Нема файлу. Створення...");
1375     writeFile(SD, DB_FILE_NAME, "UID,Name,Level,DateTime \r\n");
1376 }
1377 else
1378 {
1379     Serial.println("Файл знайдено");
1380     oled.println("Файл -> ОК");
1381 }
1382 file.close();
1383 listDir(SD, "/", 0);
1384 readFile(SD, DB_FILE_NAME);

```

PROBLEMS 2 OUTPUT DEBUG CONSOLE TERMINAL PORTS SERIAL MONITOR

+ Open an additional monitor

Monitor Mode Serial View Mode Text Port COM7 - USB-Enhanced-SERIAL CH9102 (COM7) Baud rate 115200

Stop Monitoring

```

[ 1729][E][vfs_api.cpp:105] open(): /sd/TEST1.csv does not exist, no permits for creation
Файл не знайдено
Створення файлу...
Writing file: /TEST1.csv
File written
Listing directory: /
DIR : System Volume Information
FILE: TEST1.csv SIZE: 26
FILE: mydatabase.csv SIZE: 182
FILE: TEST_FILE.csv SIZE: 26
FILE: TEST1_FILE.csv SIZE: 26
UID,Name,Level,DateTime

```

Рисунок 2.18 -- Результат ініціалізації карти пам'яті та читання інформації з неї виведений у серійний монітор

Після окремого тестування кожного апаратного елементу виконане комплексне тестування взаємодії модулів у межах однієї прошивки. Створено тестовий код, у якому три модулі працюють одночасно:

- локальний RFID-зчитувач на ГП відстежує картку;
- LoRa-модуль приймає повідомлення від ДП і передає відповідь про зчитаний UID до ДП;
- карта пам'яті зберігає зчитану інформацію про користувачів.

Під час тесту перевірялося, чи не відбувається накладення даних, а також чи стабільно працює система під час швидкого повторного зчитування карток. У серійному моніторі фіксувалися всі етапи роботи — ініціалізація, зчитування, передача та запис, що дозволяє однозначно встановити порядок подій (рис. 2.19).

```

Connect to ..... Не вдалося підключитися до WiFi
Створюю AP успішно: 192.168.4.1
BEEP_ONCE: 0
OLED: 1. Info по картці
Перестав мерехкотіти
Перестав мерехкотіти
click
OLED: Очікую картку...
RFID ініціалізовано
Стандартний ключ не підходить!
Data:0x18, 0x2F, 0x37, 0xE8, 0x1F, 0x84, 0xAB, 0xCD, 0x18, 0x2F, 0x37, 0xE8, 0x1F, 0x84, 0xAB, 0xCD,
UID: 5C596106
UID,Name,Level,DateTime
5C596106,Артем,1,01.01.2000 00:00:00
F3251D06,Пес Патрон,0,20.11.2025 16:43:36
A1F06F06,Слободяник Марк,2,20.11.2025 16:44:02
Користувача знайдено!
Name: Артем
Level: 1
DateTime: 01.01.2000 00:00:00
Відправлено дозвіл CMD_OPEN: REQ: 1 msgId: 1 UID: 5C596106
3
BEEP_OK
Перестав мерехкотіти
OLED: 1. Info по картці

```

Рисунок 2.19 -- Вивід результату одночасної роботи усіх модулів схеми

Після завершення тестування було підтверджено, що всі модулі ініціалізуються коректно, взаємодіють один з одним без збоїв та виконують свої функції в умовах тестового навантаження.

2.5 Висновки до розділу 2

В даному розділі сформовано структурні схеми апаратної частини головного та другорядного пристроїв, обґрунтовано вибір елементної бази, розроблено електричні принципові схеми та виконано макетне моделювання.

На першому етапі проведено вибір елементної бази на основі побудованих структурних схем, що забезпечує оптимальне поєднання функціональності та можливості подальшого масштабування системи. Як основний керуючий елемент обрано мікроконтролер ESP32, який завдяки високій продуктивності та наявності необхідних інтерфейсів забезпечує взаємодію з усіма периферійними модулями. Для зчитування RFID-карток використано модуль MFRC522, що підтримує технологію MIFARE Classic, а для організації надійного бездротового каналу – радіомодуль SX1278, який дозволяє будувати розподілену систему з великим радіусом дії. До складу головного вузла також увійшли дисплей SSD1306, RGB-світлодіод, бузер,

енкодер, карта пам'яті micro-SD та інші допоміжні компоненти. На другорядному пристрої реалізовано аналогічну структуру з акцентом на комутацію навантажень за допомогою реле та MOSFET-транзистора.

У процесі розробки електричних принципових схем підключення модулів та окремих елементів виконано згідно рекомендацій виробників. Особливу увагу приділено організації живлення, зокрема впровадженню USB Type-C як універсального і механічно надійного джерела живлення із застосуванням стандартної конфігурації для отримання 5 В. Також реалізовано коректну обв'язку енкодера з кнопкою, включаючи захист транзисторів у схемі бузера й реле та формування лінії EN для ESP32.

Після створення усіх необхідних схем було проведено тестування кожного функціонального елемента на макетній платі. Окремо перевірено роботу RFID-зчитувача, радіомодуля LoRa та карти пам'яті. Здійснено піднесення карток до MFRC522 з різних відстаней, передавання тестових пакетів по LoRa у двох напрямках та ініціалізацію SD-карти з доступом до файлів. Усі випробування підтвердили коректність роботи модулів та їх повну сумісність із обраним мікроконтролером. Після цього проведено тест, в якому усі компоненти працювали одночасно в межах спільної прошивки, що дозволило переконатися у відсутності конфліктів на шині SPI та стабільності системи в реальних умовах.

3. РОЗРОБКА ПРОГРАМНОЇ ЧАСТИНИ СИСТЕМИ

3.1 Вибір мови програмування та середовища розробки

Зважаючи на технічні вимоги системи, апаратну платформу та необхідність забезпечення стабільності, сумісності й розширюваності програмного забезпечення, для реалізації проєкту було обрано мову програмування C++ та середовище розробки Visual Studio Code з розширенням PlatformIO, що базується на Arduino Framework. Дане середовище розробки придатне для роботи з мікроконтролером сімейства ESP32.

Мова C++ обрана завдяки своїм перевагам у поєднанні доступу до апаратних ресурсів і можливості створення структурованого коду. Це дозволяє ефективно працювати з периферією мікроконтролера, такими модулями, як RFID-зчитувач, LoRa-модуль, дисплей, енкадер з кнопкою та реле і водночас підтримувати читабельність і масштабованість програмного коду. Крім того, C++ забезпечує сумісність із великою кількістю бібліотек, розроблених для платформи ESP32, що значно пришвидшує процес розробки, тестування та налагодження системи.

Середовище Visual Studio Code було обрано через його універсальність, підтримку сучасних інструментів для розробки вбудованих систем і розширену інтеграцію з PlatformIO. Останнє надає можливість створювати й підтримувати багаторівневі конфігурації, автоматизувати процес компіляції, прошивки, тестування та відлагодження програмного забезпечення для різних типів контролерів. Завдяки цьому стало можливим забезпечити централізоване керування бібліотеками, налаштуваннями збірки та профілями для пристроїв СКД.

Використання Arduino Framework забезпечило простоту та швидкість реалізації базової логіки, оскільки ця платформа має широку підтримку драйверів та бібліотек для популярних периферійних пристроїв. Зокрема, це дало змогу інтегрувати RFID-зчитувач, модуль бездротового зв'язку LoRa, дисплей SSD1306, карту пам'яті та інші компоненти без необхідності створювати драйвери з нуля. Такий підхід є оптимальним для створення прототипу системи та проведення експериментальних досліджень у межах магістерської роботи.

Таким чином, вибір мови C++, середовища Visual Studio Code із розширенням PlatformIO та фреймворку Arduino є обґрунтованим і оптимальним для реалізації СКД. Така комбінація дозволила створити модульну, гнучку та розширювану архітектуру програмного забезпечення, яка поєднує зручність розробки з надійністю.

3.2 Розробка структурних схем програмної частини

Оскільки система складається з двох окремих пристроїв, необхідно розробити окремі структурно-логічні схеми програмного забезпечення для кожного з них. Такі схеми дозволяють описати порядок виконання ключових операцій, взаємодію між блоками та функціями обробки подій. Структурно-логічна схема коду ГП наведена на рисунку 3.1.

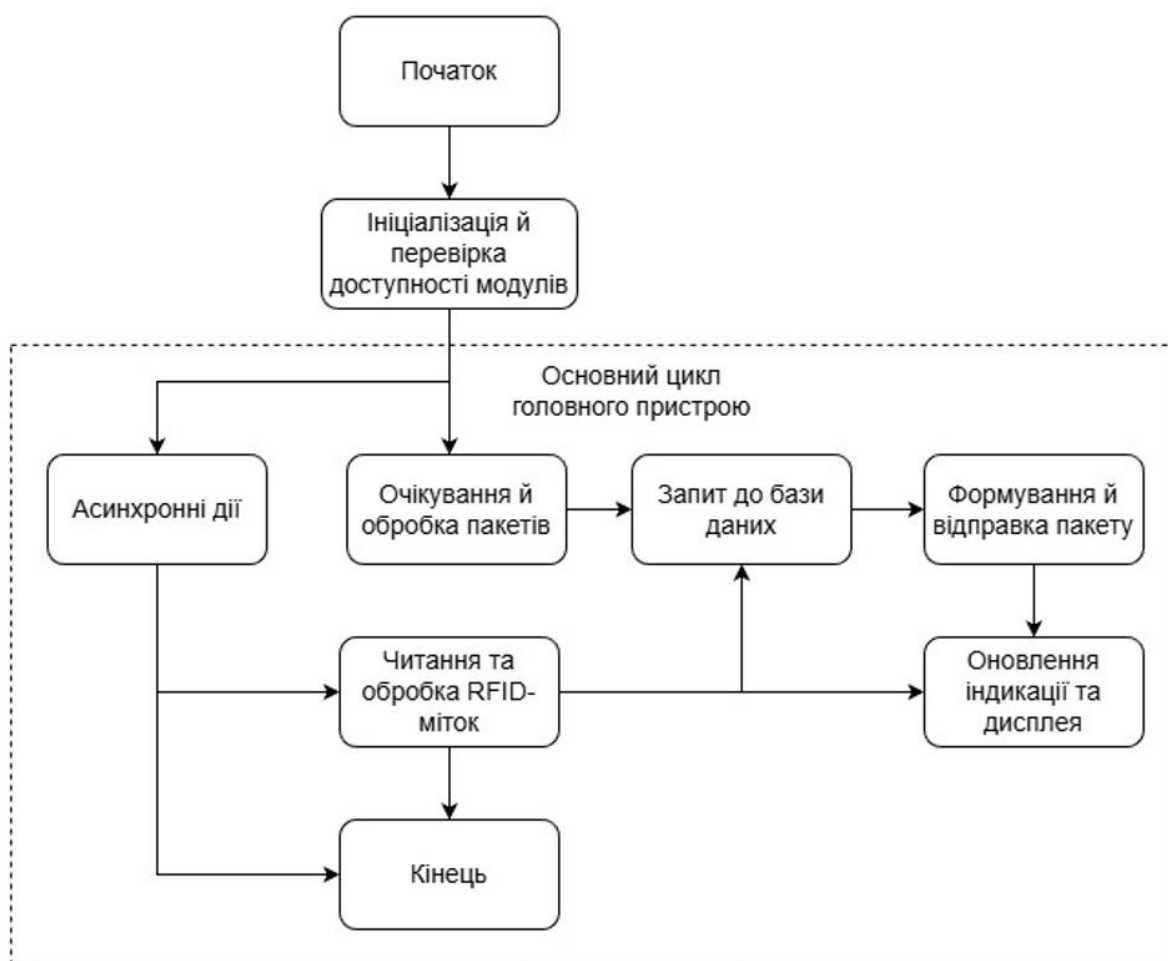


Рисунок 3.1 – Структурно-логічна схема коду ГП

Структурно-логічна схема коду ДП наведена на рисунку 3.2. Вона демонструє алгоритм роботи віддаленого виконавчого пристрою, який безпосередньо взаємодіє з користувачем.

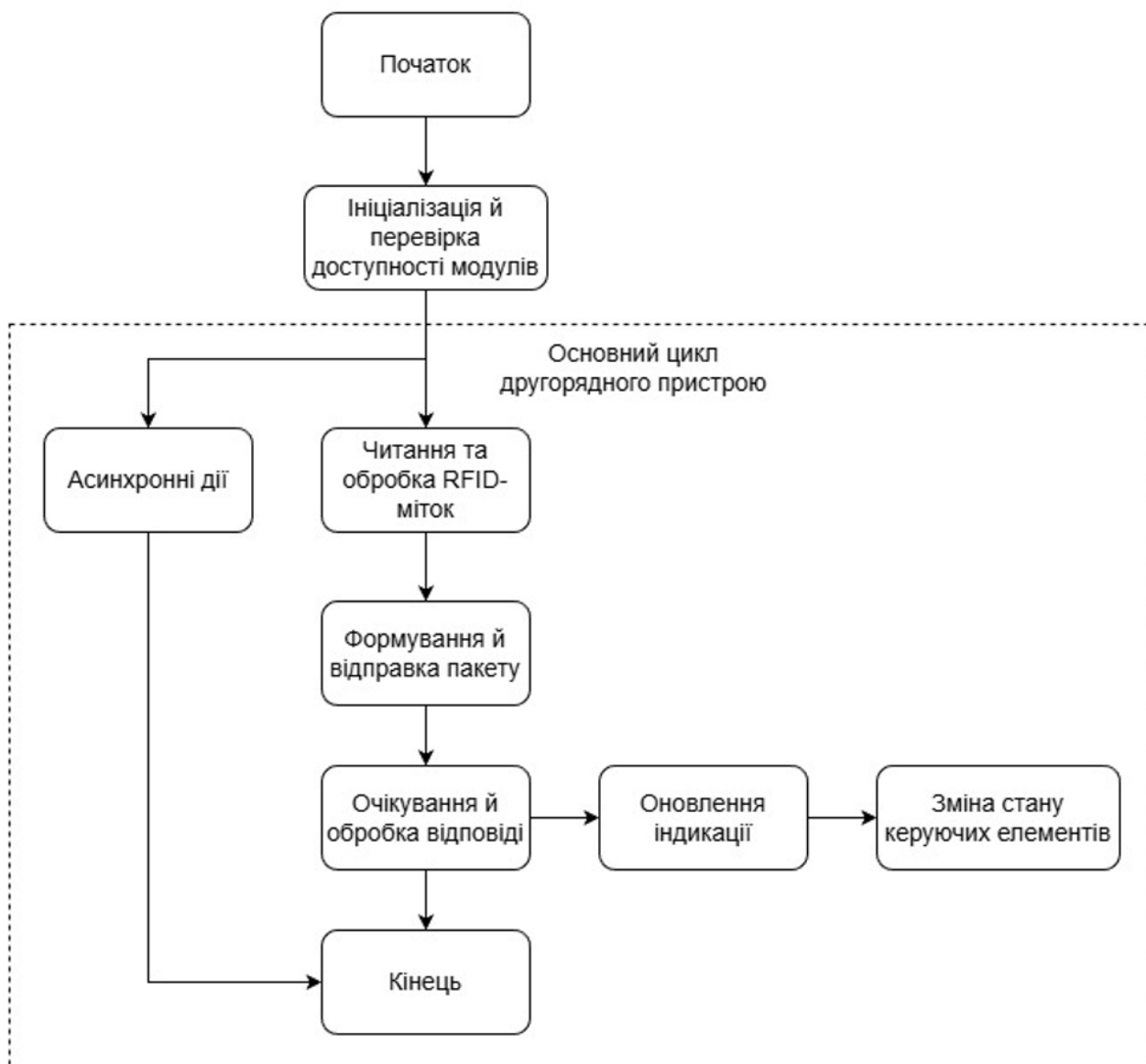


Рисунок 3.2 – Структурно-логічна схема коду ДП

Логіка взаємодії цих двох пристроїв полягає в наступному:

- користувач підносить картку до ДП. RFID-зчитувач зчитує UID та інформацію з пам'яті картки;
- мікроконтролер формує зашифрований пакет і відправляє його по LoRa на ГП;

- ГП дешифрує отриманий пакет та порівнює отриманий UID з БД карти пам'яті. Далі згідно збережених даних приймає рішення та повертає зашифровану відповідь ДП;
- другорядний пристрій отримує відповідь, дешифрує її і активує виконавчі ланцюги з індикацією відповідно до типу повідомлення.

На головному пристрої реалізовано такі основні функції для роботи з RFID-мітками:

- інформація по UID – ця функція дозволяє зчитати всю інформацію про користувача з бази даних та вивести її на дисплей;
- швидке додавання карти – ця функція дозволяє швидко занести в базу даних UID нового користувача, але без вказування його персональних даних. Ці дані необхідно потім внести вручну;
- видалення користувача з бази даних – ця функція дозволяє швидко видалити користувача з бази даних просто відсканувавши його картку;
- прошивання картки та додавання у базу даних – ця функція активується з веб-інтерфейсу ГП й вимагає фізичного відсканування картки, внесення персональних даних користувача та підтвердження дій;
- редагування запису в базі даних – є аналогічною до попередньої функції, але призначена для редагування вже існуючого запису в базі даних.

У системі бездротового обміну даними пакет LoRa має чітко визначену структуру, що дозволяє визначати відправника, одержувача, тип повідомлення, його унікальний ідентифікатор та вміст. Формування пакету відбувається у функції `buildAndSend()`, де байти записуються у визначеному порядку. Кожна позиція пакета виконує окрему службову функцію і забезпечує коректність обміну між пристроями. Вигляд пакету передачі повідомлення наведено в таблиці 3.1.

Таблиця 3.1 – Вигляд пакету LoRa

Позиція	Назва поля	Кількість байт	Приклад (HEX)
1	PREAMBLE	1	0xAA

Продовження таблиці 3.1

2	DEVICE_ACCESS_LEVEL	1	0x02
3	DEVICE_ID	1	0x01
4	DEST_ID	1	0x20
5	MSG_ID (старший байт)	1	0x03
6	MSG_ID (молодший байт)	1	0x5E
7	TYPE	1	0x01
8	PAYLOAD_LEN	1	0x0D
9...N	PAYLOAD	змінна	-
9+N+1	CRC8	1	0x7F

Перший байт пакета PREAMBLE — використовується як службовий маркер початку пакету. Він дозволяє приймачу визначити, що почалася передача даних за протоколом системи, а не сторонній шум.

Другий байт містить значення DEVICE_ACCESS_LEVEL, тобто рівень доступу відправника.

Третій байт пакета DEVICE_ID, який позначає адресу (ідентифікатор) відправника.

Четвертий байт містить значення DEST_ID, тобто ID пристрою, якому призначений пакет.

П'ятий та шостий байти містять MSG_ID — унікальний ідентифікатор повідомлення, розбитий на старший і молодший байт. Цей байт дозволяє ГП розрізняти різні пакети, визначати повторні спроби відправки або співставляти запит із відповіддю.

Сьомий байт визначає тип пакета, наприклад TYPE_REQ для запиту від другорядного до головного пристрою або інші типи, передбачені протоколом.

Восьмий байт містить довжину PAYLOAD, що дозволяє приймачу точно знати, скільки байтів корисної інформації йде далі. Після цього послідовно записується сам PAYLOAD, який містить ім'я пристрою, UID картки та службові дані.

Завершується пакет контрольним байтом CRC8, який обчислюється функцією `crc8()` на основі всіх попередніх байтів пакету. Додавання CRC дозволяє приймачу виявити випадкові спотворення даних під час передавання і відхилити некоректний пакет. Це ключовий елемент надійності, особливо в умовах сильних радіоперешкод. Таким чином, структура пакета має фіксовану службову частину та змінну корисну частину, але завжди починається з преамбули та завершується контрольним числом CRC, що забезпечує цілісність і надійність передачі.

Після побудови структурних схем програмного забезпечення, де визначені основні блоки системи та їхня взаємодія, переходимо до опису того, як ці елементи реалізовані безпосередньо у програмному коді. У наступних підрозділах розглянуто реалізацію кожного блоку, приведеного на структурних схемах.

3.3 Реалізація функціональних блоків у коді

Програмне забезпечення складається з окремих блоків, які взаємодіють між собою. Такий поділ на блоки дозволяє структурувати програму та спростити її подальше масштабування. Кожен блок має власний набір змінних, станів, алгоритмів та допоміжних функцій, які разом забезпечують коректну роботу всієї СКД. У наступних підрозділах послідовно подано опис усіх блоків.

3.3.1 Блок «Початок»

На початку коду зібрані всі бібліотеки та глобальні об'єкти:

- GyverDBFile.h, SettingsGyver.h — локальна БД налаштувань;
- LittleFS.h – підключення файлової системи;
- MFRC522.h — робота з RFID-зчитувачем;

- LoRa.h — передавання та приймання пакетів LoRa;
- SD.h і FS.h — доступ до CSV-файлу на SD-карті;
- AESLib.h — бібліотека для шифрування протоколом AES-128;
- EncButton.h — енкодер з кнопкою;
- GyverOLED.h — бібліотека для роботи з дисплеєм;
- Blinker.h, BeepESP.h — світлова та звукова індикації.

Поруч із підключенням кожної бібліотеки оголошені відповідні змінні та службові об'єкти, необхідні для її подальшого використання. Це зокрема тимчасові буфери для зберігання проміжних даних, структури для обробки UID-кодів, об'єкти керування, змінні оголошення. Такий розподіл забезпечує логічну організацію коду та дозволяє кожному програмному блоку використовувати лише ті ресурси, які безпосередньо пов'язані з його функціональністю. В архітектурі програми використано підхід станів машини (state machine):

- RfidState — взаємодія з RFID-зчитувачем;
- BlinkState — режими індикації світлодіодів;
- BeepState — звукові оповіщення;
- DisplayInfo — режими відображення інформації на екрані.

Такий підхід спрощує читання коду та дозволяє уникнути глибоко вкладених умовних конструкцій.

3.3.2 Блок «Ініціалізація та перевірка доступності компонентів»

Даний блок відповідає за початкову ініціалізацію всіх компонентів системи після подачі живлення або перезавантаження пристрою. Його реалізація зосереджена у функції `setup()`, яка виконується один раз під час запуску мікроконтролера. Основним завданням цього етапу є приведення всіх модулів у робочий стан, перевірка їх доступності та формування початкових параметрів роботи системи.

На першому етапі виконується ініціалізація послідовного інтерфейсу обміну даними зі швидкістю 115200 біт/с за допомогою функції `Serial.begin(115200)`. Далі відбувається ініціалізація бузера функцією `beep.init(BUZZER_PIN,`

PWM_CHANNEL, PWM_RESOLUTION), де вказується пін до якого підключено бузер, ШІМ канал та його бітність. Наступним етапом є ініціалізація дисплея `oled.init()`. Дисплей очищується, встановлюється початкове положення курсора та масштаб відображення.

Після цього виконується ініціалізація модулю MFRC522 через виклик `rfid.PCD_Init()`. Модуль ініціалізується, встановлюється максимальний рівень підсилення антени (`rfid.PCD_SetAntennaGain(rfid.RxGain_max)`), виконується короткочасне перезавантаження антени та повторне вмикання. Це є вимогою автора бібліотеки до цього модулю. Далі формується унікальний ідентифікатор пристрою на основі апаратної MAC-адреси ESP32 (`uint64_t mac = ESP.getEfuseMac()`), який використовується для формування унікального електронного ключа.

Після цього виконується ініціалізація модуля бездротового зв'язку LoRa SX1278 (`LoRa.begin(433E6)`). Попередньо задаються апаратні виводи керування модулем та здійснюється кілька спроб запуску передавача на заданій частоті. У разі успішної ініціалізації система повідомляє про готовність модуля, в іншому випадку інформує користувача через дисплей.

Після цього проводиться перевірка доступності карти пам'яті за допомогою циклу `while (!SD.begin(SD_CS))`. Якщо карта успішно ініціалізується, система перевіряє наявність файлу бази даних користувачів у форматі CSV: `File file = SD.open(DB_FILE_NAME); if (!file)`. У випадку його відсутності файл створюється автоматично із заголовком таблиці за допомогою функції `writeFile(SD, DB_FILE_NAME, "UID,Name,Level,DateTime \r\n")`.

Наступним етапом є налаштування Wi-Fi. Пристрій переводиться в комбінований режим клієнта та точки доступу у функції `WiFi.mode(WIFI_AP_STA)`. Далі виконується ініціалізація налаштувань веб-інтерфейсу та локальної БД (`sett.begin(); sett.onBuild(build); sett.onUpdate(update); db.begin()`). Завантажуються збережені параметри пристрою, а в разі відсутності окремих параметрів вони автоматично набувають значень за замовчуванням. Після завантаження параметрів виконується спроба підключення до мережі Wi-Fi. Завершується цей блок завантаженням службових параметрів із БД та підготовкою системи до основного циклу роботи.

3.3.3 Блок «Асинхронні дії»

Даний блок відповідає за виконання фонових, неблокуючих процесів, які повинні постійно викликатися в основному циклі програми незалежно від поточного режиму роботи системи. Його основне призначення — підтримка стабільної роботи апаратних модулів, оновлення станів інтерфейсу користувача, індикації та приймання запитів.

Для запобігання зависанню RFID-зчитувача реалізовано періодичне апаратне перезавантаження модуля за таймером, що базується на порівнянні значень `millis()`. Кожні 2 секунди виконується скидання лінії (`digitalWrite(RC522_RST_PIN, LOW);`) з подальшою повторною ініціалізацією модуля методом `rfid.PCD_Init()`. Далі виконується створення веб-інтерфейсу (рис. 3.3) та обробка налаштувань через виклик `sett.tick()`, а також обробка стану енкодера за допомогою функції `encoderB_tick()`, що забезпечує безперервну взаємодію користувача з меню пристрою. Постійно оновлюється стан світлової та звукової індикацій шляхом викликів `blink_tick()` та `beep_tick(beep_freq_temp)`, які реалізують керування відповідними скінченними автоматами без зупинки виконання програми.

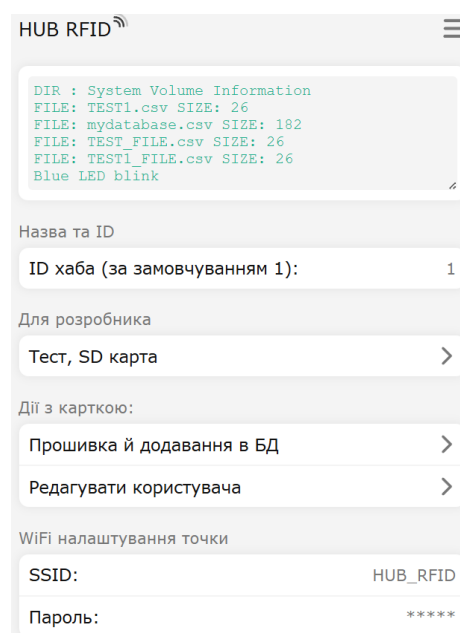


Рисунок 3.3 – Веб-інтерфейс головного пристрою

Приймання вхідних бездротових пакетів LoRa здійснюється у фоновому режимі за допомогою функції `handleIncomingPacket()`. Завершальним елементом асинхронного блоку є автоматичне повернення інтерфейсу до головного меню, що виконується викликом `back_to_main_menu()`.

3.3.4 Блок «Читання та обробка RFID-міток»

Даний блок відповідає за взаємодію зі зчитувачем MFRC522, приймання RFID-міток стандарту MIFARE Classic, отримання UID картки та зчитування службових даних із пам'яті карти. Для роботи створено службові структури:

- MFRC522::MIFARE_Key key — ключ доступу до секторів карти;
- MFRC522::MIFARE_Key keyDefault — стандартний ключ доступу до секторів карти;
- MFRC522::MIFARE_Key keyESP — унікальний ключ доступу до секторів карти;
- MFRC522::StatusCode status — статус виконання команд контролера;
- byte block = 7 — номер блоку пам'яті, з якого виконується зчитування (за потреби може містити ім'я або службові байти).

Процес взаємодії зі зчитувачем відбувається циклічно, з перевіркою наявності нової карти у полі:

- виконується виклик `PICC_IsNewCardPresent()`, який визначає, чи з'явився новий об'єкт у зоні дії антени;
- Спроба зчитування UID -- метод `PICC_ReadCardSerial()` повертає масив байтів UID та кількість байтів у UID, котрий є основним ідентифікатором користувача;
- аутентифікація блоку пам'яті викликається за допомогою `PCD_Authenticate()` із ключем типу `keyDefault`, що дозволяє отримати доступ до вмісту сектора. Якщо даний ключ не підходить, використовується унікальний ключ B, яким і прошивається картка. Таким чином вона автоматично

стає належною до даної системи. Якщо операції по отриманню доступу до картки і застосуванню ключів є успішними, програма виконується далі;

- зчитуються додаткові дані за допомогою функції `MIFARE_Read()` для отримання 16 байтів інформації з блоку даних. Цей механізм використовується для зчитування внутрішніх параметрів доступу. Якщо зчитані дані відповідають очікуваним, то програма виконується далі. В разі невідповідності даних, програма видає помилку;
- формується структура даних після успішного зчитування UID та 16 байтів інформації з блоку даних. Вони переводяться у рядок HEX. Далі дані передаються в блок аутентифікації для порівняння з базою даних;
- відбувається керування світловою та звуковою індикацією, реалізованою через стани. При очікуванні мигає синій, при успішному зчитуванні вмикається зелене світло та 2 коротких звукових сигнали, а при помилці чи забороні доступу вмикається червоне світло та 1 довгий звуковий сигнал з низьким тоном.

Даний блок є першим рівнем обробки даних користувача. Він визначає факт прикладання RFID-мітки, сканує UID та додаткову інформацію, перетворює UID у стандартизований формат та передає у наступний блок для перевірки прав доступу й зміни індикації. Тому тут передбачено декілька рівнів контролю:

- неправильний UID або неможливість прочитати карту – статус «відмова»;
- помилка аутентифікації сектора – повторна спроба або ігнорування;
- некоректні дані у блоці пам'яті – UID все одно обробляється, але службові дані ігноруються.

3.3.5 Блок «Оновлення індикації та дисплея»

Даний блок відповідає за формування світлової та звукової індикацій роботи системи, а також за відображення меню й службового тексту на дисплеї. Для підготовки області відображення меню використовується допоміжна функція очищення частини екрану `clear_area_for_menu()`, у якій виконується очищення заданої

ділянки дисплея командою `oled.clear(0, 8, 127, 63)`. Основне оновлення інформації на дисплеї реалізовано функцією `show_on_Display(DisplayInfo line, const String &text, uint8_t page)`, яка залежно від переданого режиму (`LINE_UID`, `LINE_MENU`, `LINE_ERROR`, `LINE_WAIT_CARD` тощо) змінює масштаб, позицію курсора та виводить відповідні повідомлення, наприклад: `oled.print("UID: ")`, `oled.print("Очікую картку...")` чи `oled.print("Видалено успішно!")`.

Для формування світлової та звукової індикації використовуються функції `void blink_tick()` та `void beep_tick(uint16_t freq)` відповідно. В цих функціях використовуються стани машин. Дані стани забезпечують налаштовані реакції світлодіодів, бузера або ж реле з транзистором на стороні ДП. При “позитивній” відповіді від головного пристрою активується зелений світлодіод, звукова індикація та вмикається реле з транзистором на встановлений час.

3.3.6 Блок «Очікування й обробка пакетів»

Даний блок реалізований виключно на ГП та призначений для приймання, дешифрування та перевірки запитів, що надходять від ДП. Основна логіка зосереджена у функції `handleIncomingPacket()`.

На першому етапі виконується перевірка наявності нового пакета за допомогою виклику `LoRa.parsePacket()`. Якщо пакет відсутній або його розмір нульовий (`if (packetSize <= 0)`), виконання функції негайно завершується, що забезпечує неблокуючий режим роботи. Зчитування пакета виконується у локальний буфер `buf` циклом `while (i < packetSize && LoRa.available() && i < sizeof(buf)) buf[i++] = LoRa.read();`, після чого додатково перевіряється мінімальна довжина повідомлення та правильність преамбули (`if (i < 8 || buf[0] != PREAMBLE)`). Контроль цілісності даних реалізовано шляхом перевірки контрольної суми CRC8. Для цього останній байт пакета приймається як контрольний (`uint8_t recv_crc = buf[i - 1]`), після чого виконується порівняння з обчисленим значенням `crc8(&buf[1], i - 2)`. У разі невідповідності пакет ігнорується.

Далі виконується дешифрування корисних даних за алгоритмом AES-128 викликом `decryptBlock(&buf[1], i - 2, decrypted)`. Після успішного дешифрування із пакета зчитуються рівень доступу, ідентифікатор пристрою, ідентифікатор головного пристрою, номер повідомлення та тип пакета (`accessLevel, device, hub, msgId, type, len`). Пакет приймається до обробки лише у випадку, якщо він адресований ГП або має загальну адресу (`if (hub != HUB_ID && hub != 0) return`). Додатково виконується перевірка коректності довжини корисного навантаження (`if (len > decLen - 7)`)).

Для пакетів типу запиту (`if (type == TYPE_REQ)`) виконується поетапне зчитування імені пристрою, UID-коду картки та шести байтів. UID формується у текстовий HEX-рядок у циклі `uidDeviceStr += String(uid_ptr[k], HEX)`, після чого відображається на дисплеї викликом `show_on_Display(LINE_UID, uidDeviceStr)`. Реалізована перевірка вмісту відсканованої картки на другорядному пристрої шляхом побайтового порівняння прийнятих шести байт з еталоном (`if (mac_ptr[j] != macBytes[j])`). У разі невідповідності формується відповідь відмови функцією `buildAndSend(device, msgId, CMD_DENY, NULL, 0)`.

3.3.7 Блок «Запит до бази даних» та структура файлу

Даний блок приведено у додатку В. Для зберігання інформації про користувачів у системі контролю доступу використовується текстова БД у форматі CSV, розміщена на карті пам'яті. Основний файл БД зберігається за фіксованим шляхом: `/mydatabase.csv`. Перший рядок містить заголовки стовпців, що спрощує читання та обробку файлу як самою системою, так і зовнішніми засобами (Excel, Google Sheets, текстові редактори). Структура файлу має наступні колонки:

- UID — унікальний ідентифікатор RFID-картки (hex-рядок без пробілів);
- Name — текстове ім'я користувача (Прізвище + Ім'я);
- Level — числовий рівень доступу (наприклад, 0 — гість, 1 — співробітник, 2 — адміністратор);

- DateTime — дата та час останньої модифікації запису, отримані з внутрішнього RTC (бібліотека SettingsGyver.h).

Для роботи з БД використовується стандартна бібліотека SD.h, а файл визначено як: `const char *DB_FILE_NAME = "/mydatabase.csv"`. Під час запуску системи виконується ініціалізація карти пам'яті: `SD.begin(SD_CS)`. Усі операції зчитування, редагування та видалення виконуються без завантаження файлу в пам'ять, тобто обробка здійснюється потоково, рядок за рядком. Це підвищує стабільність системи й дозволяє працювати з великими файлами не завантажуючи їх в пам'ять ESP32. Приклад записаних даних наведено на рисунку 3.4.

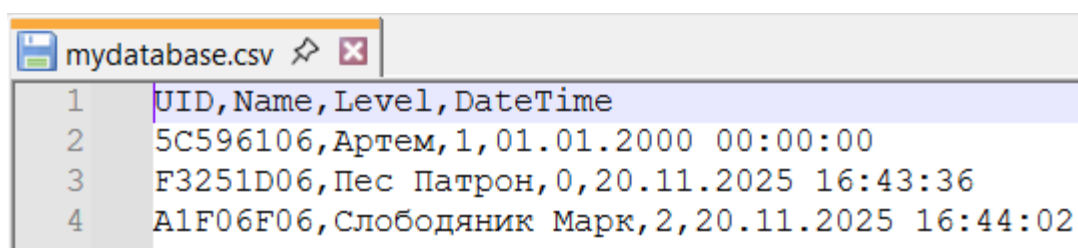


Рисунок 3.4 – Файл mydatabase.csv

Для перегляду та діагностики БД застосовується функція `readFile(fs::FS &fs, const char *path, int linesPerChunk)`. Вона підтримує пакетне виведення по кілька рядків, що спрощує логування через послідовний порт та SD-логер (`loggerSDcard`). Формат CSV зберігається без змін.

Для пошуку користувача створено функцію `findUser(String uid, String &outName, int8_t &outLevel, String &outDateTime)`. Алгоритм пошуку полягає у послідовному зчитуванні кожного рядка:

- читання рядка до символу `\n`;
- виділення UID як підрядку до першої коми;
- порівняння UID зі значенням, отриманим із RFID-мітки;
- у разі збігу парсинг решти полів та повернення структурованого результату.

Оскільки формат CSV не підтримує внутрішнього видалення, застосовується загальноприйнята техніка перепакування, котра реалізована у функції `bool deleteUserFromDB(String uid)`:

- відкривається вихідний файл (`mydatabase.csv`) у режимі читання;
- створюється тимчасовий файл `/tmp.csv`;
- усі записи, крім заданого UID, копіюються у тимчасовий файл;
- якщо UID знайдено, то старий файл видаляється і замінюється новим.

Редагування виконується схожим методом до видалення, але замість пропуску потрібного рядка система формує новий рядок із оновленими полями: `bool editUser(const String &uid, const String &newName, int newLevel)`. Структура нового рядка повністю відповідає загальному формату CSV, а новий `DateTime` автоматично записується через `RTC`, що дозволяє відслідковувати зміни.

Даний блок також відповідає за створення, перегляд та редагування записів бази даних, що зберігається на SD-карті у форматі CSV, через веб-інтерфейс. Створення веб-інтерфейсу відбувається через: `SettingsGyver sett("HUB RFID", &db)`, а виклик і постійне функціонування через `void build(sets::Builder &b)`. Ця функція формує веб-інтерфейс для редагування бази даних, створює групи налаштувань (`device name`, `access level`, `WiFi` і тд), визначає класи `Input`, `Slider`, `Switch`, `Select`, `Button` для кожного параметра, обробляє події натискання кнопок на веб-інтерфейсі та записує значення у локальні змінні та в пам'ять мікроконтролера після натискання кнопки `"Save & Restart"`.

Для того щоб додати новий запис чи відредагувати існуючий, порядок дій є ідентичним та відрізняється лиш вибором необхідного пункту меню на веб-сторінці. При відкритті відповідної вкладки (рис. 3.5), користувач має спочатку відсканувати картку, при цьому при скануванні картки викликається функція `bool uidExists(String uid)`, котра перевіряє чи немає такого UID в базі даних. Це зроблено для захисту та запобігання колізій при обробці бази даних. Потім у формі треба ввести прізвище та ім'я, вибрати рівень доступу та підтвердити дії натиснувши кнопку внизу.

< Прошивка й додавання в БД

Сканувати картку

UID картки:

Прізвище та ім'я: ...

Рівень доступу: низький ▾

Прошити й додати в БД

< Редагувати користувача

Сканувати картку

UID картки:

Прізвище та ім'я: ...

Рівень доступу: низький ▾

Редагувати

(a)

(б)

Рисунок 3.5. Пункти меню: а - для додавання нового запису у базу даних; б - для редагування існуючого.

Після натискання кнопки підтвердження, у коді викликається функція `bool addRecord(String uid, String name, int level)` для додавання нового запису або `bool editUser(const String &uid, const String &newName, int newLevel)` для редагування вже існуючого.

Редагування також можливе через енкодер з кнопкою, що забезпечує швидке додавання або видалення карток без доступу до веб-інтерфейсу. З його допомогою можна отримати всю інформацію по картці на дисплеї, відсканувавши її, швидко додати нову та видалити картку з БД.

3.3.8 Блок «Формування й відправка пакету»

Даний блок наведено в додатку В. Він реалізований на обох пристроях системи та призначений для формування, шифрування й передавання службових повідомлень по каналу LoRa. Принцип роботи цього блока є однаковим для головного і другорядного пристроїв, але відмінність полягає лише у структурі та наповненні пакета залежно від напрямку передавання даних.

Безпосереднє формування логічної структури повідомлення виконується у функції `buildAndSend(uint8_t to, uint16_t msgId, uint8_t type, const uint8_t *payload,`

uint8_t len) у масив raw[r]. У разі наявності корисного навантаження воно додається до пакета викликом memcpy(&raw[r], payload, len).

Після формування масиву пакета виконується його шифрування. Для цього застосовується функція encryptBlock(), у якій формується вектор ініціалізації memcpy(iv_enc, aes_iv, 16) та виконується шифрування AES-128 викликом aesLib.encrypt((byte *)input, inLen, (byte *)output, aes_key, sizeof(aes_key), iv_enc). Після цього створюється фінальний пакет для передавання, у якому спочатку додається преамбула buf[idx++] = PREAMBLE, потім зашифровані байти. Для забезпечення цілісності переданих даних в кінці пакету додається контрольна сума CRC8, яка обчислюється у функції crc8(const uint8_t *data, size_t len).

Безпосереднє передавання пакета по бездротовому каналу здійснюється за допомогою викликів LoRa.beginPacket(), LoRa.write(buf, idx), LoRa.endPacket(). Після завершення передавання модуль переводиться в режим приймання LoRa.receive() для очікування наступних запитів.

3.3.9 Блок «Очікування і обробка відповіді»

Даний блок реалізований на ДП та призначений для очікування, приймання, дешифрування й аналізу відповіді від ГП після передавання запиту по каналу LoRa. Основна логіка реалізована у функції bool waitForResponse(uint16_t expectedMsgId, unsigned long timeout, uint8_t *outType, uint8_t *outPayload, uint8_t *outLen, size_t outPayloadMaxLen).

На першому етапі виконується ініціалізація процедури дешифрування за допомогою функції decryptBlock(), у якій формується вектор ініціалізації командою memcpy(iv_dec, aes_iv, 16), після чого здійснюється AES-128 дешифрування викликом aesLib.decrypt((byte *)input, inLen, (byte *)output, aes_key, sizeof(aes_key), iv_dec).

Очікування відповіді відбувається протягом заданого тайм-ауту за умовою while (millis() - t0 < timeout). У кожному циклі перевіряється наявність вхідного

пакета за допомогою `LoRa.parsePacket()`. Якщо пакет відсутній (`if (packetSize <= 0)`), виконання продовжується без блокування.

Прийнятий пакет зчитується в локальний буфер циклом `while (LoRa.available() && i < packetSize) buf[i++] = LoRa.read()`. Далі виконується перевірка мінімальної довжини повідомлення (`if (i < 5)`), преамбули (`if (buf[0] != PREAMBLE)`) та контрольної суми CRC8 за допомогою `if (crc8(&buf[1], i - 2) != recv_crc)`.

Після успішної перевірки цілісності виконується дешифрування корисних даних викликом `decryptBlock(&buf[1], i - 2, decrypted)`. Із дешифрованого блоку зчитуються службові поля пакета: ідентифікатор відправника (`from`), отримувача (`to`), номер повідомлення (`msgId`), тип команди (`type`) та довжина корисного навантаження (`len`). Для захисту від приймання сторонніх або застарілих відповідей здійснюється перевірка відповідності ідентифікатора повідомлення умові `if (msgId != expectedMsgId) continue`. Лише у разі повного співпадіння відповідь приймається до подальшої обробки.

Після цього тип відповіді та корисне навантаження передаються у вихідні змінні за допомогою: `*outType = type`, `*outLen = len`, `memcpy(outPayload, &decrypted[7], len)`, а функція повертає логічне значення успішного приймання (`return true`). Якщо відповідь не надійшла у межах встановленого часу, функція завершується з результатом `return false`.

3.3.10 Блок «Зміна стану керуючих елементів»

Даний блок призначений для керування виконавчими елементами системи, а саме реле та MOSFET-транзистором, які безпосередньо здійснюють комутацію навантаження. Реалізація блока здійснюється у вигляді асинхронної функції `blink_tick(uint8_t relay_tim, uint8_t mosfet_tim)`.

На початковому етапі у фоновому режимі виконується оновлення станів усіх керованих елементів викликами `relay.tick()`, `mosfet.tick()`. Зміна режиму роботи відбувається лише у разі переходу системи в новий стан, що контролюється умовою

if (blink_state != blink_prevState). Після фіксації нового стану попередній режим індикації вимикається командою led_B.stop().

У режимі очікування (LED_WAIT) активується синє миготіння світлодіода викликом led_B.blinkForever(300, 1500), що сигналізує про готовність пристрою до обробки запитів. У разі дозволу доступу (RELAY_ON) виконується увімкнення реле та MOSFET-ключа на заданий часовий інтервал: relay.blink(1, relay_tim * 1000, 0) та mosfet.blink(1, mosfet_tim * 1000, 0). Паралельно вмикається зелена світлова індикація викликом led_G.blink(1, relay_tim * 1000, 0). Значення relay_tim та mosfet_tim задаються користувачем через веб-інтерфейс налаштувань. У разі відмови в доступі (LED_DENIED) активується червона світлова індикація командою led_R.blink(1, 500, 0). Після завершення роботи реле або сигналу відмови виконується автоматичне повернення системи в режим очікування за умовою if (relay.ready() || led_R.ready()) blink_state = LED_WAIT.

3.4 Висновки до розділу 3

У розділі розроблено повноцінне програмне забезпечення для СКД, яке забезпечує взаємодію всіх апаратних модулів та логіку роботи головного і другорядних пристроїв. Під час проєктування програмної частини поділено логіку роботи системи на окремі функціональні блоки. Це дозволило створити чітку модульну структуру коду, де кожен блок відповідає за свою частину: обробку RFID-карток, передачу даних LoRa, роботу з інтерфейсом користувача, читання й редагування даних на SD-карті тощо. Така архітектура спростила налагодження, покращила читабельність та дала змогу легко розширювати систему.

Одним із ключових елементів програмної частини стала реалізація БД у форматі CSV, що зберігається на карті пам'яті. Розроблено механізми додавання, читання, редагування та видалення записів без завантаження всього файлу в оперативну пам'ять. Також створено функції для перевірки UID-карток, пошуку потрібного запису та формування структурованих даних.

Важливою частиною роботи було формування структури LoRa-пакету та механізмів його шифрування й дешифрування. Це забезпечило коректний і безпечний обмін даними між пристроями. Окрему увагу приділено інтерфейсу користувача. Реалізовано меню на дисплеї, де за допомогою енкодера з кнопкою можна додавати або видаляти картки та переглядати інформацію про них.

Створено веб-інтерфейс, який дозволяє редагувати базу даних і параметри системи через браузер, що робить пристрій зручним для практичного використання. У межах цього інтерфейсу реалізовано додавання нових користувачів, редагування існуючих записів та перегляд структури файлів на карті пам'яті.

4. ПРОЄКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ

4.1 Розробка друкованих плат системи

Розроблення друкованої плати для головного та другорядного пристроїв здійснюється відповідно до вимог, що висуваються до виробів другого класу точності IPC 6011 [25] згідно з чинними стандартами виготовлення друкованих плат. Даний клас широко використовується в побутовій й офісній техніці та в комунікаційному обладнанні, до якого відноситься розроблювана система. На цьому етапі визначаються базові параметри конструкції, матеріал плати, технологічні обмеження та правила трасування, які необхідно врахувати під час подальшого проєктування.

Для виготовлення плати обрано поширений матеріал FR-4 – фольгований склотекстоліт на основі епоксидного композиту, що забезпечує оптимальне поєднання механічної стійкості, діелектричних характеристик та вартості. Товщина плати становить 1 мм, що відповідає стандартним умовам монтажу та забезпечує достатню жорсткість конструкції.

Мідне покриття виконане з двох сторін із товщиною провідникового шару 35 мкм. Такий тип металізації є стандартним для двосторонніх друкованих плат. Під час проєктування друкованої плати для даного пристрою встановлюються такі початкові вимоги:

- дотримання параметрів 2 класу точності, що регламентує мінімальну ширину провідника 0,15 мм, мінімальне значення відстані між провідниками 0,15 мм, мінімальний діаметр отворів 0,4 мм, гарантований пасок 0,3 мм, а також граничні відхилення діаметрів отворів і контактних площадок відповідно до нормативів;
- забезпечення електромагнітної сумісності шляхом коректного розмежування сигнальних та силових трас, використання суцільних полігонів землі й мінімізації кількості розривів у лінії GND;
- виділення окремих шин живлення для шин 3.3 В та 5 В з урахуванням струмових навантажень;
- мінімізація довжини високочастотних ліній (SPI, I2C, лінії до радіомодуля) з дотриманням рекомендованих вимог;

- забезпечення сумісності топології з механічними вимогами, включаючи правильне розміщення корпусних компонентів, роз'ємів, монтажних отворів і модулів.

Встановлення цих вимог формує технічне підґрунтя для подальшого етапу трасування плат та дозволяє створити конструкцію, що відповідає експлуатаційним й технологічним характеристикам системи.

4.1.1 Визначення габаритів й форми

Визначаємо площу кожного компонента та елементів кріплення плати для того, щоб встановити, якої форми й розмірів повинна бути плата, аби коректно розвести зв'язки та забезпечити правильне розташування всіх компонентів з урахуванням кріплень. Для цього скористаємось формулою 4.1. Площу компонента обчислюємо за його Footprint. Результати обчислень для головного та другорядного пристроїв наведено на рисунку 4.1.

$$S_{\text{дп}} = \Sigma S_{\text{мг}} + 1,5 * \Sigma S_{\text{сг}} + 2 \dots 3 * \Sigma S_{\text{вг}} + \Sigma S_{\text{кр}}, \quad (4.1)$$

де $S_{\text{дп}}$ – площа ДП, $S_{\text{мг}}$ – площа малогабаритних компонентів, $S_{\text{сг}}$ – площа середньогабаритних компонентів, $S_{\text{вг}}$ – площа великогабаритних компонентів, $S_{\text{кр}}$ – площа кріплення.

ГОЛОВНИЙ ПРИСТРІЙ					ДРУГОРЯДНИЙ ПРИСТРІЙ				
Назва:	Площа:	Коефіцієнт:	Кількість:	Сума:	Назва:	Площа:	Коефіцієнт:	Кількість:	Сума:
Конденсатори 0805	2,73	1	9	24,57	Конденсатори 0805	2,73	1	5	13,65
Конденсатори BD 4.0	20,25	1	2	40,5	Конденсатори BD 4.0	20,25	1	2	40,5
Діод SS110	18	1	1	18	Діод SS110	18	1	2	36
Транзистор S8050	4,5	1	1	4,5	Транзистор S8050	4,5	1	1	4,5
Резистори 0805	2,73	1	12	32,76	Транзистор A09T	4,5	1	2	9
Роз'єм USB-TYPE-C	88	1	1	88	Резистори 0805	2,73	1	11	30,03
Бузери	81	1	1	81	Роз'єм USB-TYPE-C	88	1	1	88
Слот під карту пам'яті	225	1,5	1	337,5	Бузери	81	1	1	81
Енкодер з кнопкою	210	2	1	420	Кнопка тактова	35	1	1	35
Дисплей	756	2	1	1512	Реле	320	2	1	640
Мікроконтролер	540	1,5	1	810	Роз'єм 2-контактний	65	1,5	2	195
Стабілізатор	34	1	1	34	Роз'єм 3-контактний	100,5	1,5	1	150,75
Модуль LoRa	588	2,5	1	1470	Мікроконтролер	540	1,5	1	810
Модуль RFID	1040	2,5	1	2600	Стабілізатор	34	1	1	34
Світлодіод RGB	36	1	1	36	Модуль LoRa	588	2,5	1	1470
Кріплення	100	1	4	400	Модуль RFID	1040	2,5	1	2600
					Світлодіод RGB	36	1	1	36
Σ друкованої плати				7908,83	Кріплення	100	1	4	400
					Σ друкованої плати				6673,43

Рисунок 4.1 -- Розрахунки габаритних розмірів плат

Відповідно до розрахунків мінімальна площа друкованої плати ГП становить 7908,83 мм², а ДП 6673,43 мм². Плати будуть прямокутної форми.

Розраховані розміри плат є мінімальними. Так як розроблювані прототипи будуть виготовлені методом ЛПТ (лазерно-праскова технологія), то було обрано дещо більші габарити плат. Розміри друкованої плати ГП становлять 96,5х91,5мм, що дорівнює площі 8830мм², а розміри друкованої плати ДП становить 92,5х70мм, що дорівнює площі 6475мм². Отримана площа плати ДП має менший розмір, через те що було вирішено SMD компоненти розмістити на нижньому шарі плати, а вивідні компоненти на верхньому. Кріпитись плата до корпусу буде за допомогою саморізів.

4.1.2 Розрахунок ширини друкованих провідників

Основними критеріями при виборі ширини провідників є: робочий струм у ланцюзі, допустиме падіння напруги та технологічні обмеження виробництва. Для плати прийнято матеріал FR-4, товщина основи 1 мм, товщина мідного шару 35 мкм.

Перш ніж визначитись з мінімальною шириною друкованих провідників, проаналізуємо споживання струму основних ланцюгів наших схем та зведемо результати до таблиці 4.1.

Таблиця 4.1 – Споживання струму ланцюгів схеми

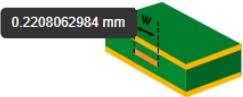
Назва, NET	I, A
+3.3 B	0,4
+5 B	0,3
Signal	0,005

За допомогою онлайн-калькулятора [26] виконаємо розрахунок, яка має бути мінімальна ширина друкованого провідника для кожного ланцюга схеми.

Current (I)	0.4 A	Ambient Temperature	26 °C
Thickness (t)	35 μm	Trace Length	45 mm
Temperature Rise (T _{Rise})	10 °C		

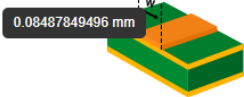
↓ ↓ ↓

Minimum Trace Width



0.2208062984 mm

Minimum Trace Width



0.08487849496 mm

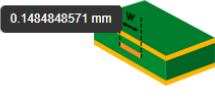
*Internal Layers:		*External Layers in Air:	
Required Trace Width (W)	0.2208062984 mm	Required Trace Width (W)	0.08487849496 mm
Resistance	0.1032344387 Ω	Resistance	0.2685581818 Ω
Voltage Drop	0.04129377549 V	Voltage Drop	0.1074232727 V
Power Loss	0.01651751020 W	Power Loss	0.04296930910 W

Рисунок 4.2 – Розрахунок ширини провідника для ланцюга +3.3 В

Current (I)	0.3 A	Ambient Temperature	26 °C
Thickness (t)	35 μm	Trace Length	45 mm
Temperature Rise (T _{Rise})	10 °C		

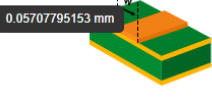
↓ ↓ ↓

Minimum Trace Width



0.1484848571 mm

Minimum Trace Width



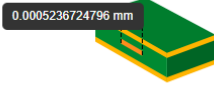
0.05707795153 mm

*Internal Layers:		*External Layers in Air:	
Required Trace Width (W)	0.1484848571 mm	Required Trace Width (W)	0.05707795153 mm
Resistance	0.1535160873 Ω	Resistance	0.3993628656 Ω
Voltage Drop	0.04605482618 V	Voltage Drop	0.1198088597 V
Power Loss	0.01381644785 W	Power Loss	0.03594265790 W

Рисунок 4.3 – Розрахунок ширини провідника для ланцюга +5 В

Current (I)	0.005	A	Ambient Temperature	26	°C
Thickness (t)	35	μm	Trace Length	45	mm
Temperature Rise (T _{Rise})	10	°C			

Minimum Trace Width



0.0005236724796 mm

Minimum Trace Width



0.0002013010147 mm

*Internal Layers:		*External Layers in Air:			
Required Trace Width (W)	0.0005236724796	mm	Required Trace Width (W)	0.0002013010147	mm
Resistance	43.52876115	Ω	Resistance	113.2374535	Ω
Voltage Drop	0.2176438058	V	Voltage Drop	0.5661872674	V
Power Loss	0.001088219029	W	Power Loss	0.002830936337	W

Рисунок 4.4 – Розрахунок ширини провідника для ланцюга Signal

Розраховані значення ширин провідників є замалими, адже повинні відповідати вимогам 2 класу точності, згідно з яким мінімальна номінальна ширина провідника становить 0,15 мм. Тому, для струмових ліній доцільно застосовувати ширини, що перевищують мінімально допустимі значення:

- для сигнальних ліній (Signal) достатньо 0,3 мм;
- для ліній живлення +3.3 В та +5 В, які можуть піддаватися короткочасним піковим струмам, доцільно збільшити ширину до 0,5 мм, що підвищує надійність.

Таким чином, задані параметри не тільки відповідають нормам 2 класу точності, але й забезпечують додатковий запас надійності для силових ділянок.

4.1.3 Трасування друкованих плат

Трасування друкованих плат для головного та другорядного пристроїв здійснювалося у середовищі EasyEDA, яке забезпечує підтримку компонентної

бібліотеки, інструментів трасування, перевірки правил та інтеграцію з виробничими файлами формату Gerber. У процесі створення топології було застосовано єдині принципи побудови, узгоджені з вимогами 3 класу точності та з урахуванням електричних і теплових характеристик пристроїв. Плати головного та другорядного пристроїв проєктувались за спільними принципами. У процесі компоновання плати роз'єм USB Type-C та тримач карти пам'яті були розташовані з краю друкованої плати, що забезпечує зручність доступу під час експлуатації пристроїв.

Для ліній живлення +5 В та +3.3 В застосовано розширені провідники та окремі полігони, що дозволило зменшити падіння напруги на доріжках та покращити тепловідведення. Полігони землі GND виконують роль екрана для зниження електромагнітних наведень.

Для модуля RFID передбачено окремі вимоги до топології. Зокрема, під антеною RFID-модуля виключено будь-які полігони землі, живлення або широкі металізовані доріжки, що могло б призвести до зміни характеристик антени, втрати чутливості або зменшення робочої відстані зчитування. Ділянка під антеною була залишена вільною від широких доріжок, що відповідає рекомендаціям розробників RFID-модулів на базі MFRC522 та дозволяє уникнути проблем з дальністю роботи антени. Вигляд плат пристроїв наведено на рисунках 4.5 та 4.6.

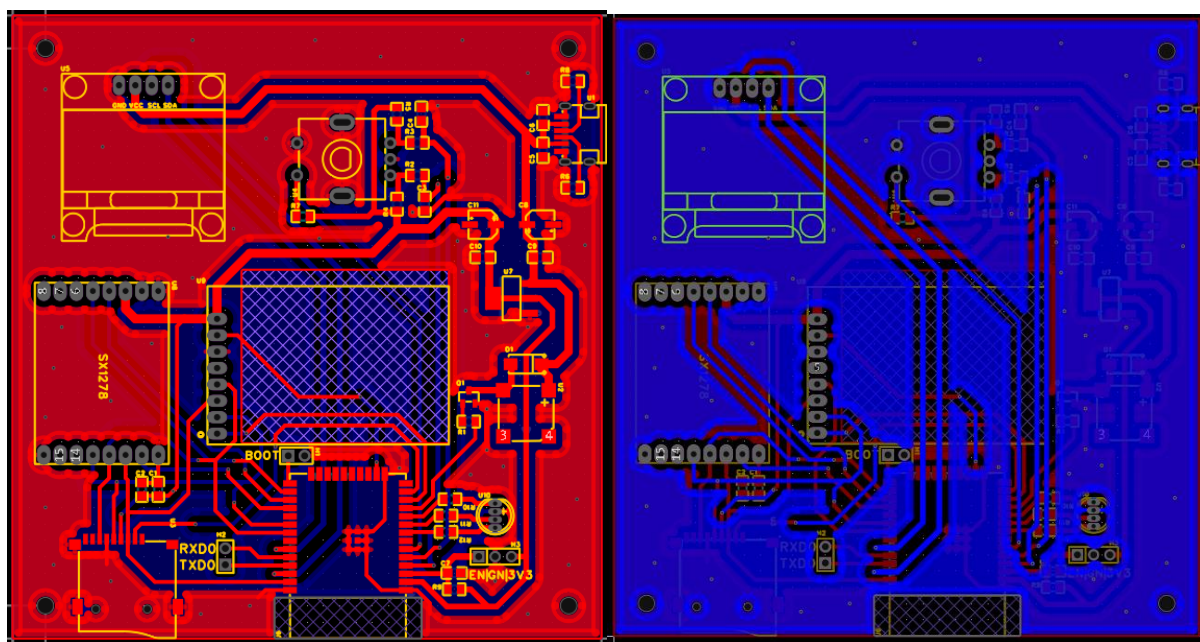


Рисунок 4.5 – Верхній та нижній шари плати ГП

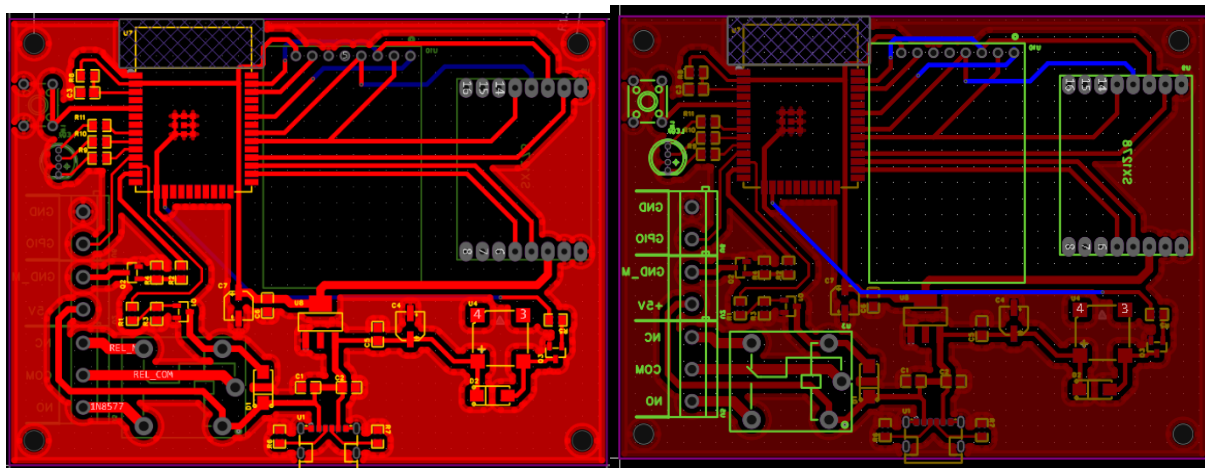


Рисунок 4.6 – Верхній та нижній шари плати ДП

Після завершення розміщення компонентів та трасування доріжок, проводилася автоматична перевірка з урахуванням параметрів 2 класу точності. Перевірка включала:

- контроль мінімальної ширини провідників;
- контроль зазорів між провідниками та падами;
- відповідність діаметрів отворів нормативам;
- коректність підключення полігонів;
- відсутність непідключених сегментів та неповних з'єднань.

Коректність проходження перевірки гарантує, що плата може бути виготовлена у більшості промислових виробників без необхідності додаткової ручної корекції.

4.2 Розробка корпусів

Конструкцію корпусів головного й другорядного пристроїв розроблено в середовищі SolidWorks, що дає можливість провести попередню оцінку ергономіки та сумісності з електронною частиною

Проектування здійснювалося із врахуванням вимог до надійності, зручності користування та можливості багаторазового монтажу й демонтажу плати під час тестування. Крім того, конструкція повинна забезпечувати механічний захист

друкованої плати та елементів, мінімізувавши вплив зовнішніх факторів (ударів, пилу, вібрації).

4.2.1 Корпус головного пристрою

Для того щоб провести моделювання корпусу, слід отримати 3Д модель плати, яка зображена на рисунку 4.7.

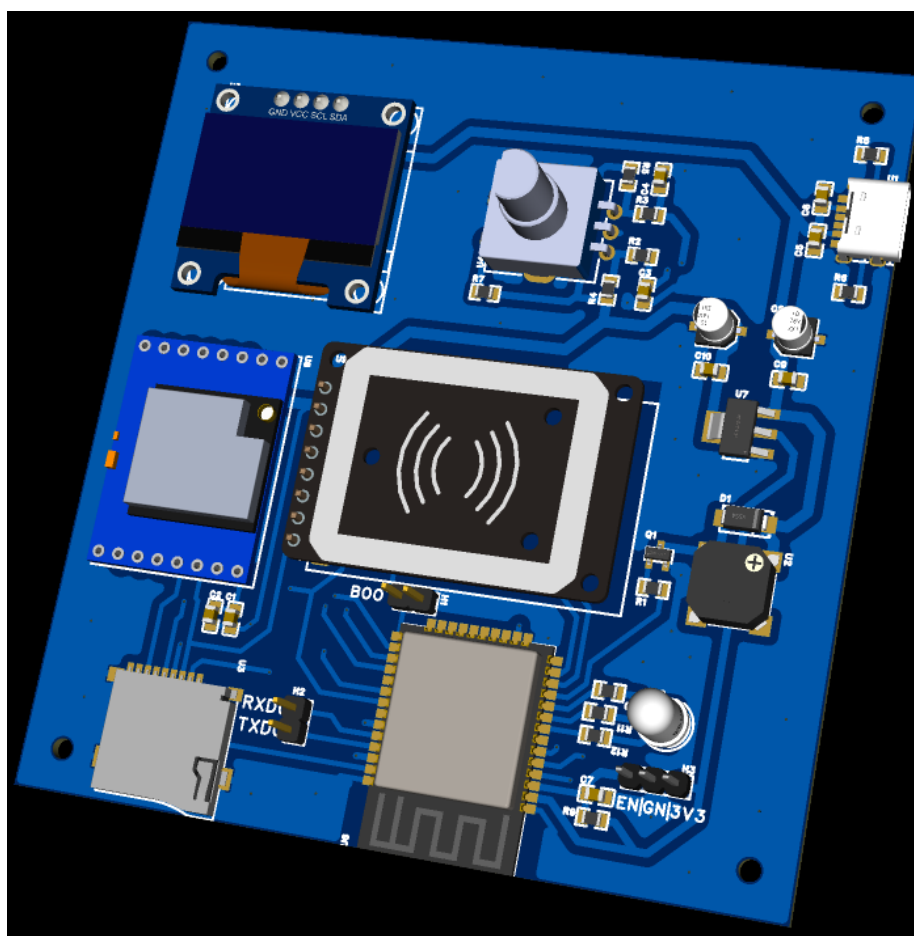


Рисунок 4.7 – 3Д модель друкованої плати ГП

Корпус ГП складається з двох основних половин – верхньої та нижньої кришок. Обидві половини корпусу утворюють замкнену порожнину, всередині якої розміщено друковану плату. Верхня частина корпусу (рис. 4.8) виконує функції основної оболонки та містить усі необхідні елементи взаємодії з користувачем.

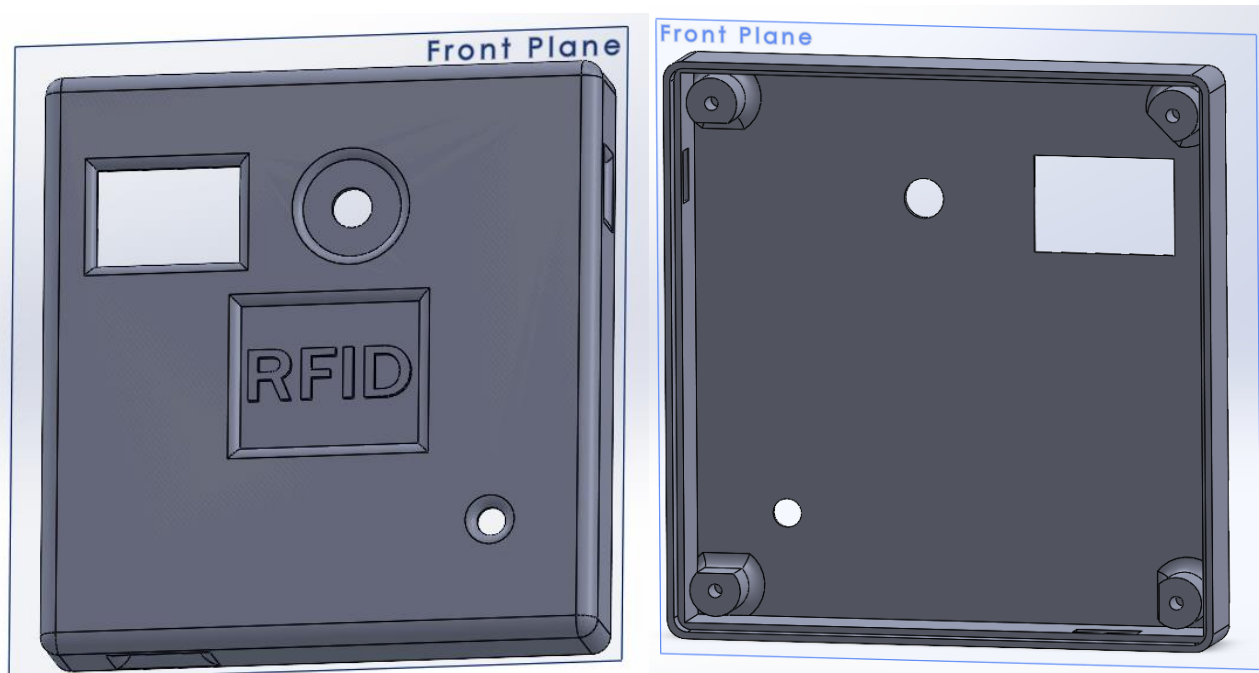


Рисунок 4.8 – Верхня частина корпусу ГП

Вона сформована як монолітна деталь, що включає:

- отвір під роз'єм USB Type-C;
- отвір для SD-карти, що проєктувався з урахуванням стандартних габаритів роз'єму та необхідного технологічного люфту, який гарантує можливість легкого виймання та вставлення носія;
- отвір під дисплей, який має мінімальний зазор для запобігання проникненню пилу та одночасно забезпечує надійне розташування екрана відносно корпусу;
- отвір під енкодер, спроектований таким чином, щоб забезпечити вільний хід осі та правильне положення ручки регулювання;
- отвір під індикаторний світлодіод, розташований у зоні прямої видимості користувача;
- рельєфний напис, котрий позначає місце розташування модуля MFRC522;
- чотири внутрішні монтажні стійки, які відповідають розташуванню монтажних отворів на друкованій платі та забезпечують жорстку фіксацію плати у просторі.

Для кожного отвору передбачено припуски, що враховують можливі похибки 3D-друку та забезпечують сумісність зі стандартними компонентами.

Нижня половина корпусу (рис. 4.9) виконує функції захисного елемента, який закриває корпус із нижнього боку та утворює разом з верхньою частиною цілісну конструкцію.

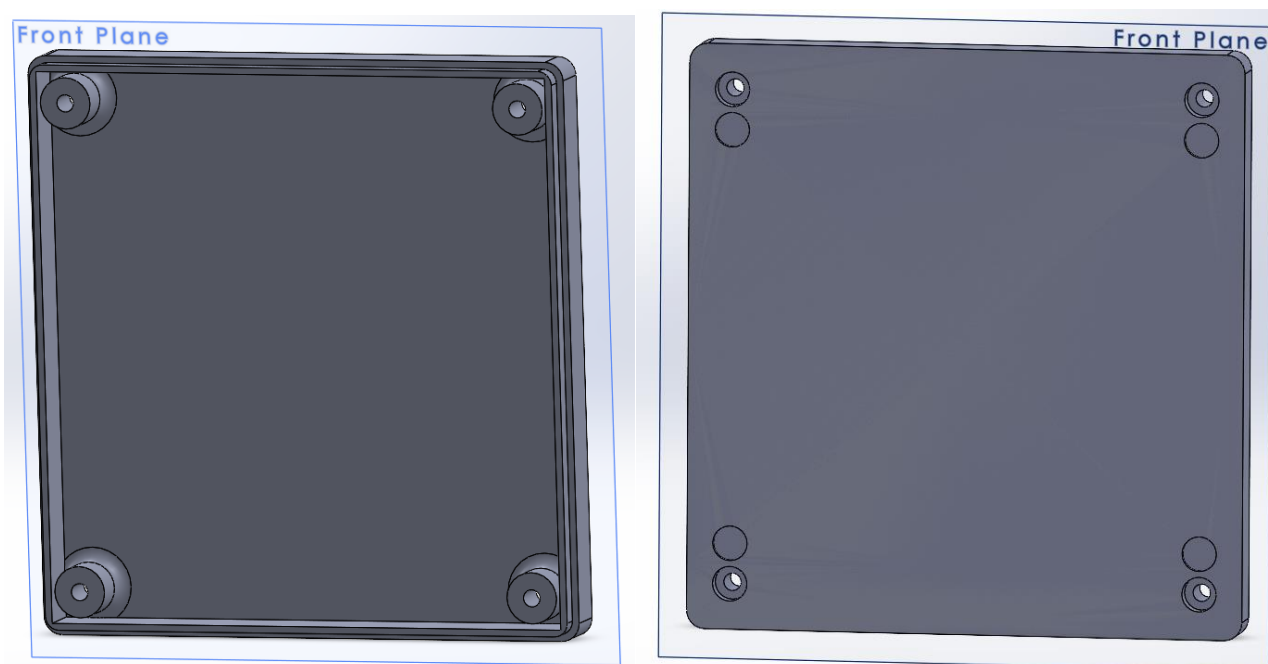


Рисунок 4.9 – Нижня частина корпусу ГП

Основними конструктивними елементами нижньої кришки є:

- чотири монтажні стійки, що слугують нижньою опорою для друкованої плати;
- отвори для гвинтів, завдяки яким обидві половини корпусу з'єднуються в єдину жорстку конструкцію.

Таке рішення дозволило реалізувати конструкцію, у якій плата фактично затиснута між двома кришками, що гарантує її стабільне положення, захищає від вібрацій і виключає зміщення навіть у разі ударів.

Корпус виготовлений за допомогою технології адитивного виробництва (3D-друк). В якості матеріалу застосовано ABS-пластик, що має низку переваг:

- висока механічна міцність і ударостійкість;

- стійкість до підвищених температур (порівняно з PLA);
- можливість післяобробки ацетоном для покращення зовнішнього вигляду;
- низька маса при достатній жорсткості.

ABS було обрано як оптимальний матеріал для корпусів електронних пристроїв, що можуть піддаватися незначному нагріву від внутрішніх компонентів та потребують достатньої міцності.

Процес друку відбувався зі стандартними параметрами для ABS (температура сопла 250 °C, нагріта платформа 90 °C), що забезпечило геометричну точність та однорідність конструкції. Для уникнення деформації під час охолодження було використано закриту камеру друку.

Складання корпусу (рис. 4.10) здійснюється шляхом поєднання верхньої та нижньої частин за допомогою саморізів М3. Перед з'єднанням плата встановлюється на стійки верхньої кришки, після чого нижня кришка притискає її з протилежного боку та затягується саморізами.

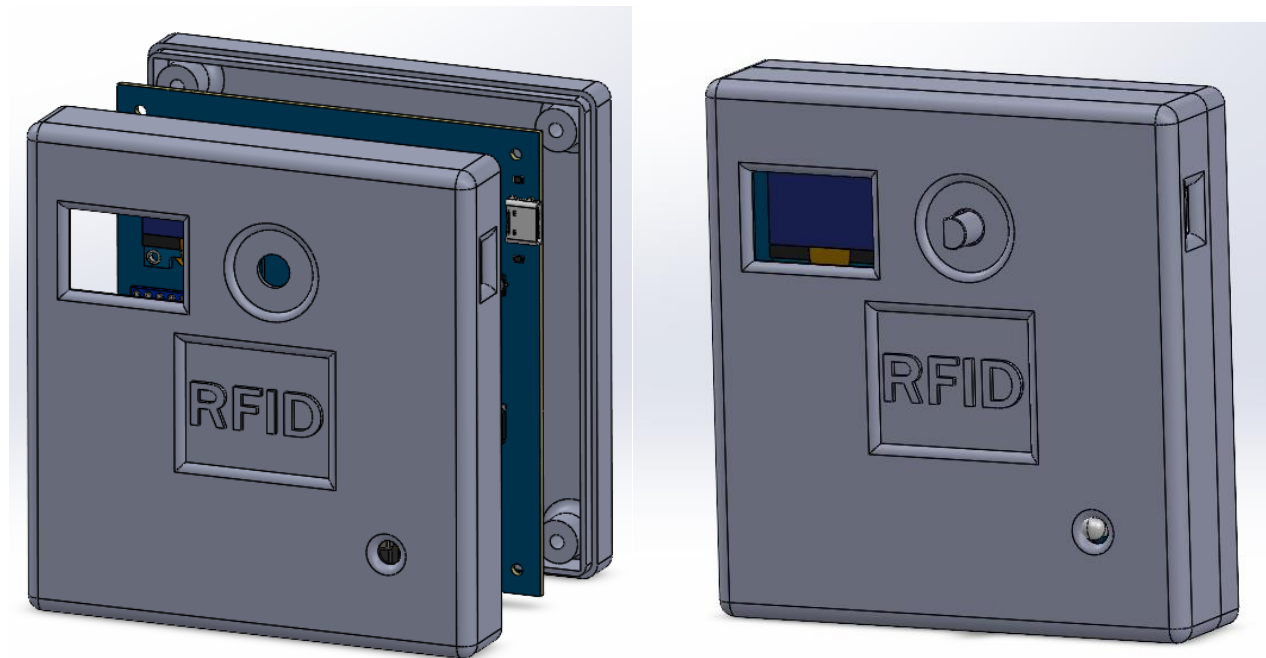


Рисунок 4.10 – Моделювання складання корпусу ГП

Корпус задовольняє сучасні вимоги до компактності та портативності. Всі елементи керування зосереджені на одній панелі, а компактні габарити забезпечують зручність транспортування та інтеграції у більші системи. Використання ABS гарантує довговічність корпусу та достатню стійкість до зовнішніх впливів.

4.2.2 Корпус другорядного пристрою

Корпус ДП розроблено за тим самим принципом, що і корпус ГП. Моделювання виконано в середовищі SolidWorks з використанням 3Д моделі друкованої плати (рис. 4.11).

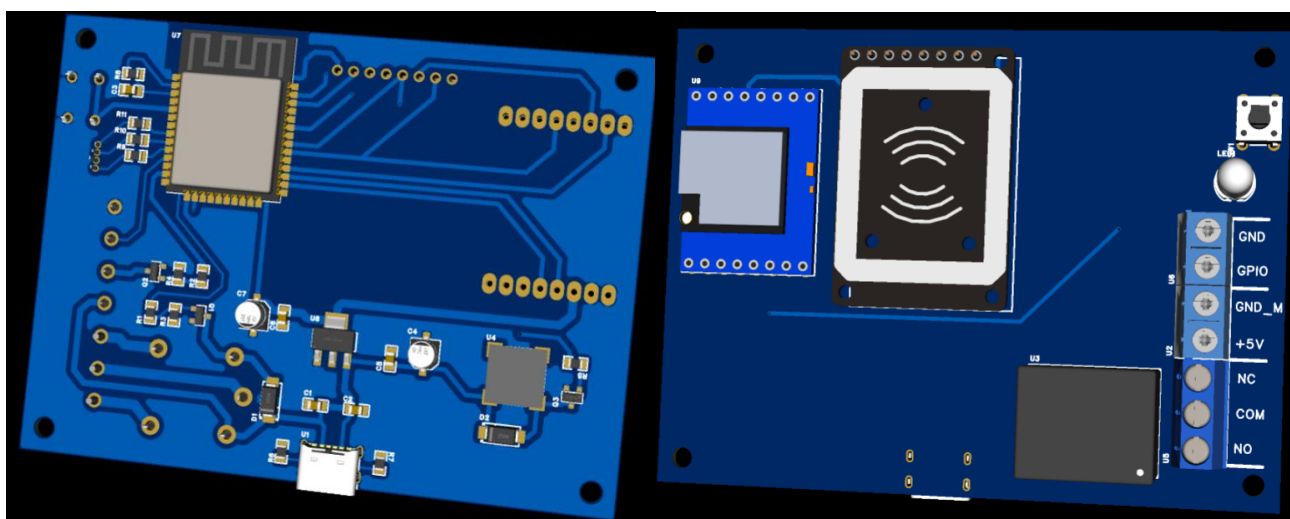


Рисунок 4.11 – 3Д модель друкованої плати ДП

Як і у випадку з ГП, корпус складається з двох половин – верхньої та нижньої кришок, які після з'єднання утворюють замкнену порожнину для розміщення плати. Внутрішня частина обох кришок містить чотири монтажні стійки, що відповідають отворах на друкованій платі та дозволяють закріпити її у фіксованому положенні. Після складання плата опиняється затиснутою між двома половинами корпусу, що виключає її зміщення.

Верхня половина корпусу (рис. 4.12) виконує функцію основної зовнішньої оболонки та містить мінімально необхідні елементи взаємодії з користувачем. У

конструкції передбачено отвір під індикаторний світлодіод, розташований у зоні прямої видимості користувача та рельєфний напис, котрий позначає місце розташування модуля MFRC522.

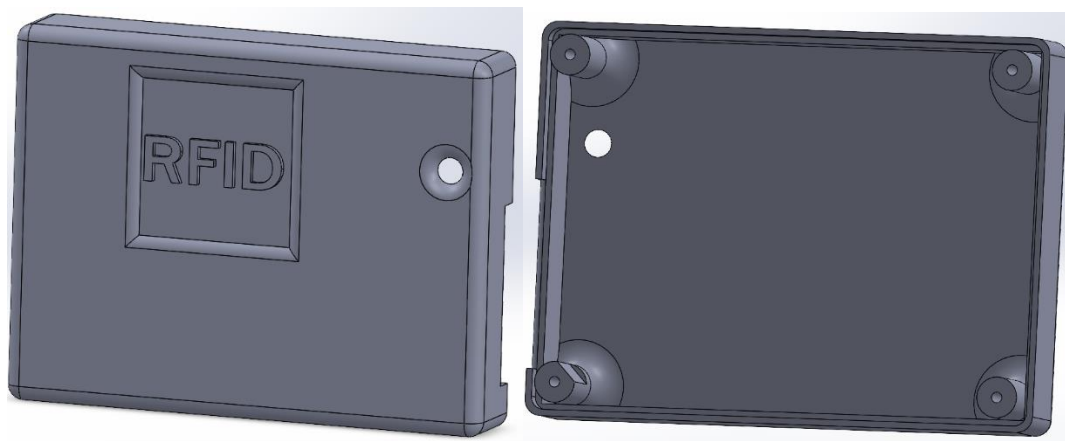


Рисунок 4.12 – Верхня частина корпусу ДП

Нижня частина корпусу (рис. 4.13) має отвір під роз'єм USB Type-C та два спеціальні отворами під гвинти, що дозволяють закріплювати пристрій на стіні або іншій вертикальній поверхні. Також на задній поверхні є заглиблені отвори для саморізів М3, за допомогою яких верхня та нижня частини корпусу стягуються у єдину конструкцію.

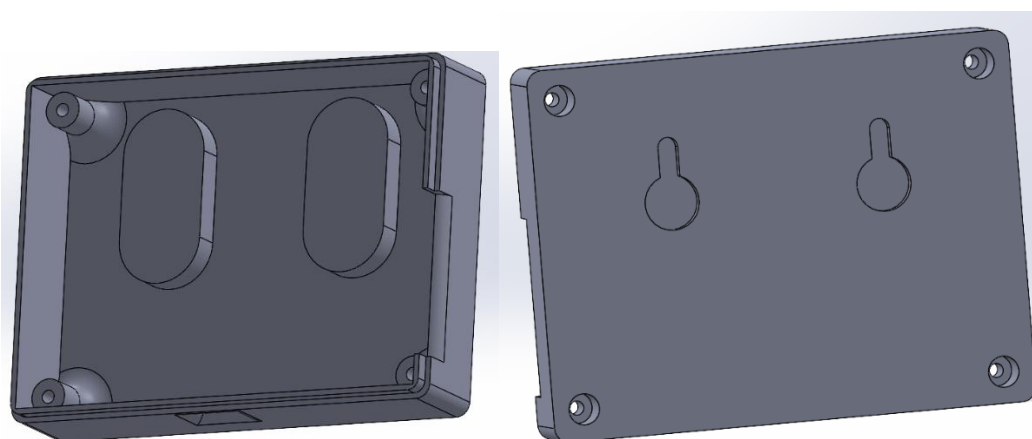


Рисунок 4.13 – Нижня частина корпусу ДП

Складання корпусу другорядного пристрою (рис. 4.14) здійснюється аналогічно до ГП, де верхня та нижня частини поєднуються між собою за допомогою саморізів. Перед з'єднанням друкована плата встановлюється на внутрішні монтажні стійки верхньої кришки, після чого нижня кришка притискає її з протилежного боку та фіксується саморізами. Завдяки такому підходу плата надійно затиснута між двома половинами корпусу та не зміщується під час експлуатації.

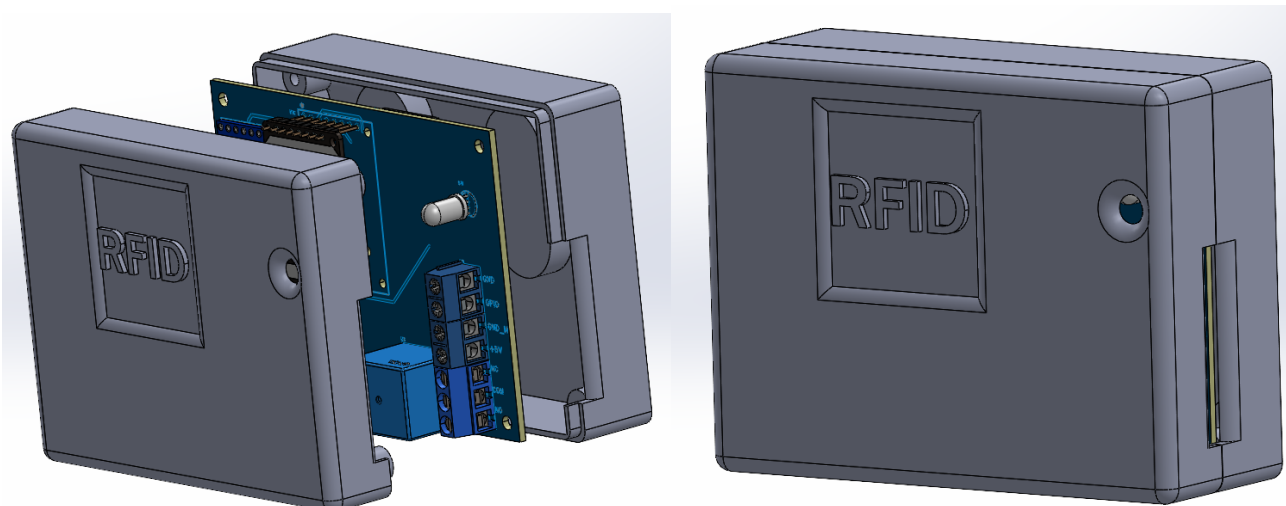


Рисунок 4.14 – Моделювання складання корпусу ДП

Корпус ДП спроектовано з урахуванням компактності та можливості стаціонарного монтажу. На відміну від ГП, у нижній частині передбачено виріз для підключення дротів до роз'ємів та спеціальні отвори для монтажу на стіну або іншу вертикальну поверхню.

4.3 Виготовлення та випробування прототипу

Створення дослідного зразка необхідне для підтвердження коректно прийнятих схемотехнічних рішень. Цей процес дозволяє виявити потенційні недоліки конструкції, які неможливо відслідкувати на етапі комп'ютерного моделювання. Нижче описано технологічний процес виготовлення друкованих плат, їх складання, а також результати комплексного тестування працездатності системи.

4.3.1 Виготовлення друкованих плат та складання пристроїв

Для виготовлення друкованих плат, розроблених у пункті 4.1, було обрано метод ЛПТ, який дозволяє отримати друковані плати прийнятної якості в домашніх умовах. В якості матеріалу плати використано фольгований склотекстоліт марки FR-4 товщиною 1 мм, розміри якого були визначені та обґрунтовані в попередніх розділах.

Процес виготовлення включав наступні етапи:

- друк дзеркального відображення топології провідників на глянцевому папері за допомогою лазерного принтера;
- термоперенесення тонеру на мідну поверхню текстоліту;
- хімічне травлення плати у розчині хлорного заліза для видалення зайвої міді;
- свердління отворів для вивідних компонентів, перехідних отворів та лудіння контактних площадок;
- монтаж SMD-компонентів на плату за допомогою нагрівальної поверхні;
- монтаж вивідних компонентів та перевірка цілісності усіх з'єднань.

Зовнішній вигляд виготовленої плати ГП наведено на рисунку 4.15, а вигляд плати ДП на рисунку 4.16.

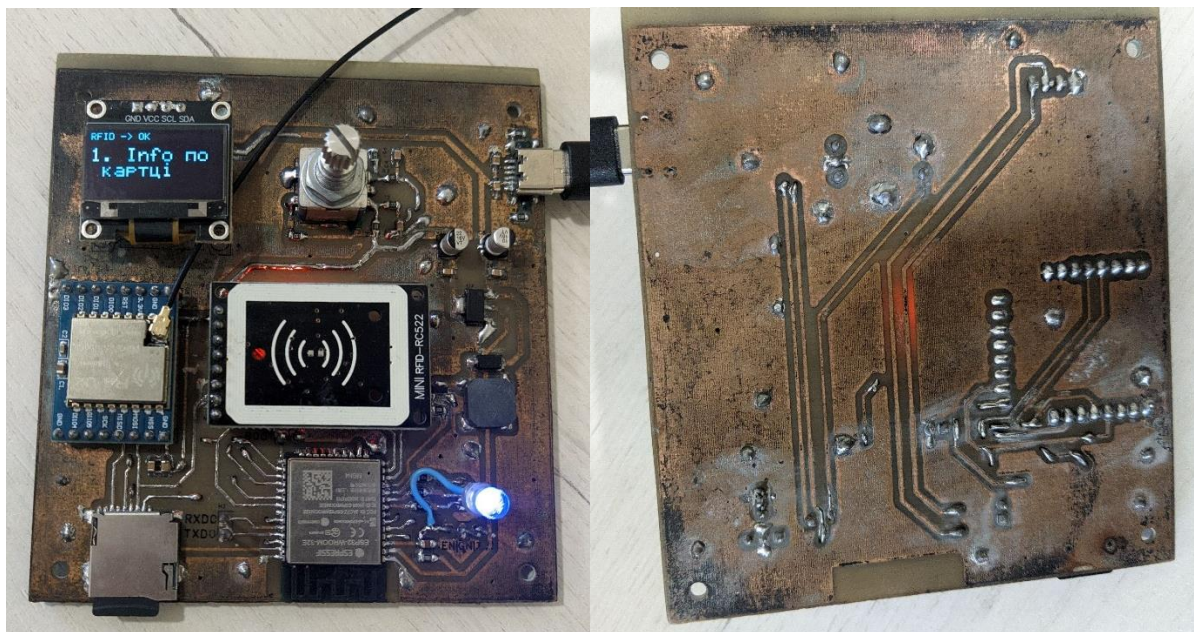


Рисунок 4.15 – Виготовлена плата ГП

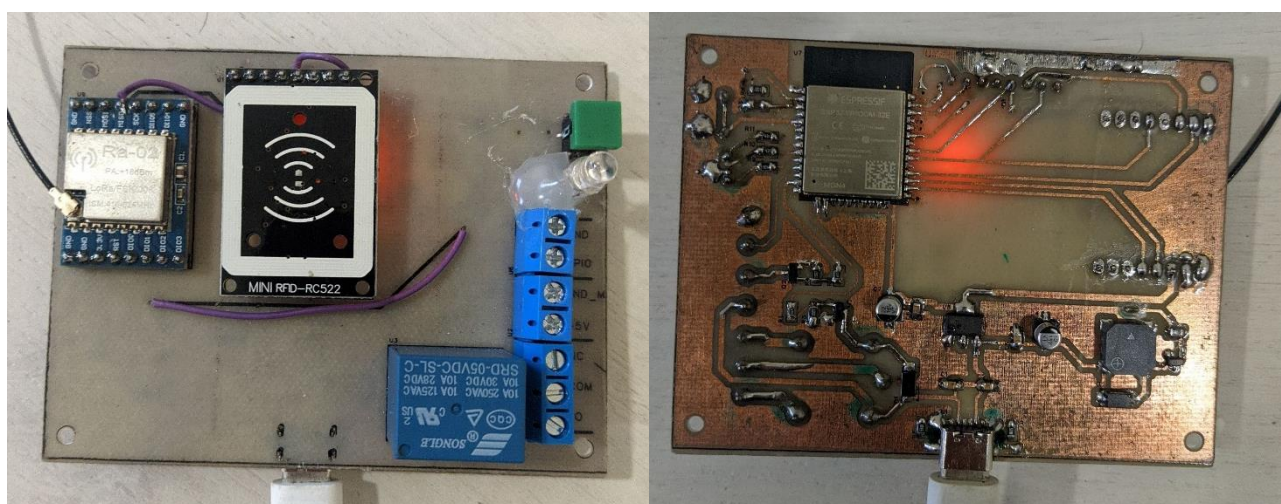


Рисунок 4.16 – Виготовлена плата ДП

Далі плати були встановлені у корпуси, що були спроектовані у пункті 4.2 та виготовлені на 3Д-принтері. Фіксація плат у корпусі здійснена за допомогою внутрішніх стійок та саморізів М3, що гарантує механічну стійкість пристрою. Зібрані головний та другорядний пристрої у готовому вигляді наведено на рис. 4.17.



Рисунок 4.17 – Зібраний у готовому вигляді прототип системи

Таким чином, фізична реалізація прототипу підтвердила правильність конструкторських розрахунків, виконаних на етапі проектування друкованих плат та корпусів. Компонування елементів забезпечило щільне й безпечне розміщення електроніки, а також вільний доступ до всіх інтерфейсних роз'ємів та органів керування.

4.3.2 Випробування прототипу

Після апаратної реалізації було проведено випробування для перевірки працездатності створеної системи. Тестування відбувалося у декілька етапів, що охоплювали перевірку ідентифікації міток, запит до БД та стабільність радіозв'язку.

Першим кроком була перевірка ідентифікації карток. Викликався перший пункт меню, котрий зчитує прикладену картку та показує інформацію про неї на дисплеї, якщо ця картка є в БД. Результати приведено на рисунку 4.18.



Рисунок 4.18 – Результат розпізнавання RFID-міток

Наступним етапом була перевірка швидкого додавання RFID-мітки в БД. Для цього активується другий пункт меню та прикладається картка. Якщо помилок не виникло, бачимо напис “Додано!” та зелене світло світлодіода. Результат наведено на рисунку 4.19.



Рисунок 4.19 – Результат додавання RFID-мітки до БД

Далі було перевірено процес авторизації користувача у системі. Для цього на ДП прикладається картка і в разі успішної відправки й отримання пакету по радіоканалу LoRa активується реле, відповідний звуковий сигнал та бачимо зелене світло світлодіода. Результат випробування зображено на рисунку 4.20.



Рисунок 4.20 – Результат авторизації користувача у системі

Для визначення реальних експлуатаційних характеристик радіоканалу LoRa було проведено випробування дальності в умовах міської забудови. Головний пристрій знаходився стаціонарно всередині будівлі, а другорядний переміщувався на відстань до втрати зв'язку.

У ході експерименту було встановлено, що система забезпечує стабільний двосторонній обмін пакетами даних на відстані до 107 метрів. При цьому на лінії прямої видимості знаходилася перешкода у вигляді двох цегляних стін та дерев. На цій відстані втрат пакетів зафіксовано не було, що підтверджує ефективність обраної технології LoRa для організації СКД на середніх та великих відстанях.

4.4 Висновки до розділу 4

У межах розділу виконано проєктування апаратної частини системи, що включало розробку топології друкованих плат, 3Д-моделювання корпусів, а також фізичне виготовлення та тестування прототипу.

Проєктування друкованих плат виконано з урахуванням технологічних норм. Визначено габарити плат та обрано матеріал FR-4 із товщиною 1 мм. Товщина мідного шару 35 мкм з обох боків дозволяє витримувати необхідні струмові навантаження, а вибір параметрів 2 класу точності забезпечує сумісність із поширеними виробничими процесами.

Під час трасування друкованих плат сформовано полігони лінії GND, а високочастотні лінії SPI та I2C мінімізовані за довжиною. Зона під антенною модуля MFRC522 залишена вільною від суцільного мідного покриття та широких доріжок.

Наступним етапом стала розробка корпусів пристроїв у середовищі SolidWorks. Конструкція забезпечує надійну фіксацію друкованої плати та захист компонентів від механічного впливу. Геометрія корпусу узгоджена з габаритами плати. Усі роз'єми розташовано на краю плат та в корпусах зроблено відповідні отвори для зручного доступу до них.

Завершальним етапом стало виготовлення фізичного прототипу системи методом ЛПТ з подальшим монтажем компонентів та збіркою. Проведені випробування підтвердили його повну працездатність. Перевірено стабільний радіозв'язок на відстані до 107 метрів крізь перешкоди у вигляді цегляних стін та дерев.

5. РОЗРОБКА СТАРТАП ПРОЄКТУ

У сучасних умовах динамічного розвитку технологій та зростаючих вимог до безпеки доступу виникає необхідність створення інноваційних рішень, які б поєднували ефективність, зручність у використанні та економічну доцільність. Стартап, як форма започаткування нового бізнесу, орієнтований на швидке впровадження інноваційного продукту на ринок, має потенціал реалізувати сучасні високотехнологічні рішення, адаптовані до реальних потреб користувачів. Успішність стартапу базується на здатності запропонувати унікальний продукт, який відповідає актуальним викликам ринку, а також на гнучкості у розробці та швидкому масштабуванні.

З огляду на вищеописане, створення стартап-проєкту у сфері систем контролю доступу, заснованих на інтеграції технологій LoRa та RFID, є обґрунтованим напрямком. Такий проєкт може запропонувати оптимальне поєднання безпеки, зручності, а також можливостей локального та віддаленого керування, що відповідає сучасним тенденціям розвитку інтелектуальних систем доступу та Інтернету речей (IoT). Реалізація стартапу створить платформу для подальшого розвитку та комерціалізації високотехнологічних розробок, випереджаючи існуючі рішення за рівнем функціональності та економічної привабливості.

5.1 Опис ідеї проєкту

Ідея проєкту полягає у розробці системи контролю доступу, що базується на технологіях LoRa та RFID і реалізована у вигляді інтегрованого мікроконтролерного комплексу з можливістю локального збереження даних на зовнішньому носії та їх віддаленого моніторингу. Система передбачає зручне та надійне зчитування унікальних ідентифікаторів RFID-карток, обробку інформації за допомогою програмної архітектури з модульною структурою, а також взаємодію з периферійними блоками через радіозв'язок LoRa.

Актуальність ідеї зумовлена зростаючою потребою у гнучких рішеннях контролю доступу, які здатні забезпечувати високу безпеку та одночасно сприяти ефективному управлінню у різних сферах застосування, включно з інтелектуальними будівлями, виробничими комплексами, лабораторіями та іншими середовищами з різними умовами і вимогами до доступу. Запропонована концепція дозволяє подолати обмеження класичних систем, впроваджуючи інновації у форматі стартапу, що забезпечує конкурентні переваги на ринку.

У таблиці 5.1 приведено зміст ідеї стартап-проєкту, напрямки його застосування та вигоди, які отримує користувач.

Таблиця 5.1 – Опис ідеї стартап-проєкту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Створення системи контролю доступу на основі технологій LoRa та RFID	Контроль доступу у комерційних, виробничих, складських, навчальних або житлових приміщеннях	Надійна ідентифікація безконтактним способом із мінімізацією ризику несанкціонованого доступу. Гнучке керування налаштуваннями системи та базою даних. Відмова від необхідності з'єднувати дротами другорядні пристрої з головним.

Наступним етапом проведемо аналіз потенційних техніко-економічних переваг розробленої ідеї в порівнянні з існуючими ринковими пропозиціями. Для цього:

- сформуємо список основних техніко-економічних властивостей та характеристик проєкту;
- визначимо коло основних конкурентів, які вже представлені на ринку, і зберемо інформацію про відповідні техніко-економічні показники як для власної розробки, так і для конкурентів;
- проведемо порівняльний аналіз, розділивши показники на такі категорії: а) гірші за конкурентів (позначені як W — слабкі), б) на рівні конкурентів (N

— нейтральні), в) кращі від конкурентів (S — сильні), що представлено у таблиці 5.2.

Таблиця 5.2. Визначення слабких, нейтральних та сильних сторін ідеї проєкту

№ п/п	Техніко-економі- чні характе- ристики ідеї	(потенційні) товари/концепції кон- курентів				W (сла- бка сто- рона)	N (ней- тра- льна сто- рона)	S (си- льна сто- рона)
		Мій проєкт	Dahua Technol ogy	ATIS	Keenfin ity			
1.	Економічність	Висока	Середня	Сере- дня	Сере- дня			+
2.	Зручність вико- ристання	Висока	Середня	Висока	Висока			+
3.	Функціональ- ність	Сере- дня	Середня	Висока	Висока		+	
4.	Безпечність	Висока	Середня	Сере- дня	Висока			+

У підсумку, таблиця демонструє перелік ключових техніко-економічних показників та характеристик розробленої ідеї. Аналіз свідчить, що основними перевагами проєкту є висока економічність, зручність використання та безпечність.

5.2 Технічний аудит проєкту

Для ефективної реалізації стартап-проєкту необхідно провести аналіз технологічних рішень. Однією з головних задач є оцінка технологій, які лягають в основу програмної та апаратної архітектури. У таблиці 5.3 наведено перелік ключових ідей проєкту із зазначенням доступності та готовності до використання.

Таблиця 5.3. Технологічна здійсненність ідеї проєкту

№ п/п	Ідея проєкту	Технології її реалізації	Наявність техноло- гій	Доступність технологій
1.	Система контролю доступу на основі технологій LoRa та RFID	C++, Arduino Framework, ESP32, RFID, LoRa	Наявні	Доступні
2.	Локальне збереження подій на SD-карті	Файлова система CSV, SD-картка	Наявні	Доступні, зручні у використанні
3.	Обмін даними по радіомережі LoRa	LoRaWAN протокол, LoRa-модулі	Наявні	Доступні, недорогі
4.	Веб-інтерфейс для керування базою користувачів	HTML, CSS, JavaScript	Наявні	Доступні

Після проведення технічного аудиту бачимо, що для впровадження запропонованої системи використовуються вже існуючі та випробувані технології. Особливість реалізації полягає у поєднанні апаратних та програмних рішень, зокрема у роботі з мікроконтролером ESP32, що забезпечує гнучкість і масштабованість системи.

5.3 Аналіз ринкових можливостей запуску стартап-проєкту

У підрозділі здійснюється комплексний аналіз ринкових можливостей і загроз, які можуть впливати на успішність стартап-проєкту. Для кращого розуміння ринку

виконаємо попередню характеристику потенційної аудиторії та умов, у яких планується впровадження розробки. Результати представлені у таблиці 5.4.

Таблиця 5.4. Попередня характеристика потенційного ринку

№ п/п	Показники стану ринку (найменування)	Характеристика
1.	Кількість головних гравців, од	>3
2.	Загальний обсяг продаж, грн/ум.од	4 000
3.	Динаміка ринку (якісна оцінка)	Зростає
4.	Наявність обмежень для входу (вказати характер обмежень)	Конкуренція серед перевірених компаній
5.	Специфічні вимоги до стандартизації та сертифікації	Відсутні
6.	Середня норма рентабельності в галузі (або по ринку), %	15-20

Наведена характеристика у таблиці 5.4 демонструє загальні показники ринку та його динаміку, що для розглянутої ніші має тенденцію до зростання. Водночас, наявність конкуренції серед існуючих компаній на ринку свідчить про складність виходу нових продуктів на внутрішній ринок, що може створювати певні бар'єри. Специфічні вимоги до продукту відсутні. Рентабельність у рамках 15-20 % відображає потенціал для отримання прибутку, хоча і з урахуванням конкуренції.

Наступним кроком є визначення потенційних груп клієнтів, їх ключових характеристик, а також формування орієнтовного переліку вимог до продукту з урахуванням потреб кожної групи. Результати цього аналізу представлені у таблиці 5.5.

Таблиця 5.5. Характеристика потенційних клієнтів стартап-проекту.

№ п/п	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці різних потенційних цільових груп	Вимоги споживачів до товару
1.	Потреба у бездротовому, недорогому та безпечному контролі доступу	Малі та середні підприємства, офіси, склади	Приватні користувачі цінують простоту. Бізнес цінує надійність і масштабованість.	Простота інтеграції, можливість розширення, безпека, віддалене керування

Таблиця відображає ключові потреби ринку і основні характеристики цільової аудиторії. Врахування відмінностей у поведінці користувачів дозволяє сформулювати вимоги до продукту, що відповідають їх очікуванням і умовам експлуатації.

Наступним етапом проаналізуємо фактори, які можуть заважати впровадженню розробленої системи на ринок (табл. 5.6).

Таблиця 5.6. Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1.	Конкуренція	Наявність відомих брендів з готовими рішеннями	Конкуренція за рахунок бездротовості та розробки нових функцій
2.	Відсутність маркетингового досвіду	Складність у просуванні продукту та залученні клієнтів	Залучення спеціалістів, онлайн-реклама

Продовження таблиці 5.6

3.	Програмне забезпечення	Поява більш зручних або функціональних рішень	Постійне вдосконалення власної прошивки
4.	Технічні несправності	Вихід з ладу окремих модулів пристрою	Модульна конструкція, можливість швидкого ремонту
5.	Фінансові обмеження	Недостатність коштів для старту виробництва	Поетапний розвиток, залучення інвесторів

Проведений аналіз факторів загроз показав, що найбільш суттєвий вплив на розвиток проєкту мають конкуренція на ринку та фінансові обмеження на початковому етапі. Водночас ризики пов'язані з програмним забезпеченням, технічними несправностями та відсутністю маркетингового досвіду, можуть бути мінімізовані завдяки постійному вдосконаленню продукту.

Наступним етапом розглянемо фактори можливостей, які наведено в таблиці 5.7.

Таблиця 5.7. Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1.	Зростання попиту на бездротові системи контролю доступу	Популярність бездротових технологій LoRa та RFID для організації контролю доступу у різних сферах	Розробка та впровадження нових продуктів з підтримкою LoRa і RFID для задоволення зростаючого попиту
2.	Попит на продукцію	Зростаюча потреба в системах контролю доступу	Збільшення виробництва, розширення асортименту

Продовження таблиці 5.7

3.	Зниження вартості комплектуючих	Розвиток ринку електронних компонентів	Оптимізація собівартості та зниження ціни для споживача
4.	Попит на підвищену безпеку	Актуальність захищених каналів зв'язку та шифрування	Впровадження нових алгоритмів захисту та оновлення прошивки

Проведений аналіз факторів можливостей показав, що розроблюваний пристрій має значний потенціал для розвитку завдяки зростанню попиту на бездротові системи, розвитку мобільних технологій та підвищенню вимог до інформаційної безпеки. Важливими є також можливості модернізації, зниження собівартості та виходу на нові ринки збуту.

Переходимо до аналізу ринку конкурентів, де у таблиці 5.8 приведено ступеневий аналіз конкуренції.

Таблиця 5.8. Ступеневий аналіз конкуренції на ринку

№ п/п	Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1.	Чиста конкуренція	На ринку представлено багато пристроїв із поєднанням бездротовості, шифрування та мобільного керування	Орієнтація на унікальні переваги продукту та швидкий вихід у свою нішу

Продовження таблиці 5.8

2.	Міжнародний характер конкуренції	На ринку присутні як локальні виробники, так і світові бренди	Необхідність підвищення якості та адаптації пристрою до різних ринків
3.	Міжгалузева конкуренція	Пристрій одночасно належить до сфер IoT, безпеки та автоматизації	Розвиток програмного забезпечення та інтеграції з іншими системами
4.	Цінова конкуренція	Ціна є важливим фактором вибору для малого та середнього бізнесу	Оптимізація собівартості та гнучка цінова політика
5.	Конкуренція за рівнем бренду	Покупці більше довіряють відомим торговим маркам	Формування іміджу, тестові впровадження, відгуки клієнтів

Можна зробити висновок, що конкурентне середовище для розроблюваного пристрою є динамічним і характеризується наявністю як локальних, так і міжнародних виробників. Конкуренція відбувається переважно в межах однієї товарної групи, а ключовими чинниками вибору для споживачів залишаються функціональність, рівень безпеки і ціна. Висока роль бренду та постійний технологічний розвиток впливають на регулярне оновлення продукту й активного просування на ринку.

Таблиця 5.9. Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари заміники
	ATIS, Keenfinity	Стартапи у сфері IoT та систем безпеки	Постачальники мікроконтролерів, RFID та LoRa модулів	Малі та середні підприємства, офіси, склади	WiFi замки, домофони, механічні замки

Продовження таблиці 5.9

Висновки:	Конкуренція є високою	Ринок є відкритим для нових рішень, але вимагає постійних інновацій	Залежність ціни товару від постачальників	Попит стабільний та орієнтований на недорогі й прості рішення	Важлива функціональна перевага та надійність
-----------	-----------------------	---	---	---	--

Аналіз показав, що ринок систем контролю доступу є конкурентним, з наявністю як сильних прямих конкурентів, так і значної кількості потенційних гравців та товарів-замінників. Разом із цим залежність від постачальників є, а попит з боку споживачів залишається стабільним. Це створює умови, за яких ключову роль відіграють унікальні характеристики виробу та рівень його конкурентних переваг.

З огляду на це переходимо до обґрунтування основних факторів конкурентоспроможності стартап-проєкту, що представлено у таблиці 5.10.

Таблиця 5.10. Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проєктів значущим)
1.	Бездротова передача даних	Відсутність кабелів спрощує монтаж та масштабованість
2.	Можливість оновлення прошивки	Дозволяє вдосконалювати функціонал без заміни апаратної частини
3.	Зручність налаштувань доступу	Можливість редагування бази даних та налаштувань системи з телефону
4.	Простота використання	Дозволяє швидко та інтуїтивно керувати системою
5.	Інноваційність технологій	Поєднання бездротового зв'язку, мобільного керування та локального зберігання даних

Після визначення та обґрунтування ключових факторів конкурентоспроможності стартап-проєкту переходимо до порівняльної оцінки його сильних і слабких сторін (табл. 5.11).

Таблиця 5.11. Порівняльний аналіз сильних та слабких сторін проєкту

№ п/п	Фактор конкуренто- спроможності	Бали 1- 20	Рейтинг товарів-конкурентів у порівнянні з стартап-проєктом						
			-3	-2	-1	0	+1	+2	+3
1.	Бездротова передача даних	19							+
2.	Можливість онов- лення прошивки	16					+		
3.	Зручність налашту- вань доступу	17						+	
4.	Простота викорис- тання	16				+			
5.	Інноваційність тех- нологій	18						+	

На основі отриманих оцінок у таблиці 5.11 можна зробити висновок, що стартап-проєкт є достатньо конкурентоспроможним й має виражені конкурентні переваги за бездротовою передачею даних, інноваційністю технологій та зручністю налаштування доступу.

Наступним етапом є складання SWOT-аналізу стартап-проєкту, результати якого наведено в таблиці 5.12.

Таблиця 5.12. SWOT-аналіз стартап-проєкту

Сильні сторони: 1. Бездротова архітектура 2. Високий рівень захисту даних. 3. Мобільне керування та зручне налаштування доступу. 4. Простота використання. 5. Інноваційність технологій. 6. Легка масштабованість.	Слабкі сторони: 1. Низька впізнаваність на початковому етапі. 2. Залежність від постачальників електронних компонентів. 3. Початкова обмеженість модельного ряду. 4. Обмежені фінансові ресурси.
Можливості: 1. Зростання попиту на бездротові IoT-рішення та системи контролю доступу. 2. Розширення ринків збуту. 3. Зниження вартості електронних компонентів. 4. Розширення функціоналу. 5. Інтеграція з іншими системами безпеки та «розумним будинком».	Загрози: 1. Висока конкуренція з боку відомих брендів 2. Поява нових технологій і продуктів-замінників 3. Фінансові ризики на старті виробництва 4. Швидке старіння технологій 5. Коливання цін на електронні компоненти

На основі виконаного SWOT-аналізу можна зробити висновок, що розроблюваний стартап-проєкт має суттєві сильні сторони, однак водночас стикається з ризиками, які необхідно враховувати при виході на ринок. Саме тому наступним кроком є розгляд можливих альтернатив ринкового впровадження стартап-проєкту, що дозволить обрати найбільш доцільний шлях розвитку (таблиця 5.13).

Таблиця 5.13. Альтернативи ринкового впровадження стартап-проєкту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1.	Орієнтація на ринок малого та середнього бізнесу з акцентом на бездротовість і простоту встановлення й використання	Висока	9 місяців
2.	Запуск із низькою стартовою ціною для швидкого залучення перших користувачів	Середня	6 місяців
3.	Залучення інвестицій або участь у грантових програмах	Ймовірна, за умови правильної презентації проєкту	3 місяці

Аналіз можливих альтернатив ринкового впровадження показує, що стартап-проєкт має кілька реалістичних шляхів виходу на ринок, основними з яких є орієнтація на малий бізнес, конкурентна цінова політика та залучення інвестицій.

5.4 Розробка ринкової стратегії стартап-проєкту

Для ефективного виходу стартап-проєкту на ринок необхідно чітко визначити основні напрями ринкової стратегії, що включають ідентифікацію цільових груп споживачів, вибір базової стратегії розвитку, визначення підходів до конкурентної боротьби та формування позиціонування продукту. Проаналізуємо потенційні цільові групи споживачів. Результати аналізу наведено в таблиці 5.14.

Таблиця 5.14 – Вибір цільових груп-потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Малі та середні підприємства	Висока	Високий	Висока	Середня
2.	Склади, офіси		Вище середнього		
Які цільові групи обрано: обрано малі та середні підприємства, а також склади й офіси, оскільки саме ці сегменти мають стабільний попит та високу готовність до впровадження систем контролю доступу.					

Отримані результати свідчать про доцільність орієнтації стартап-проекту на сегменти малих і середніх підприємств, а також складів та офісів, які характеризуються високою готовністю до впровадження продукту та стабільним попитом. Для ефективної роботи в обраному сегменті ринку необхідно визначити базову стратегію розвитку (табл. 5.15).

Таблиця 5.15 – Визначення базової стратегії розвитку

Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
Компенсація слабких сторін стартапу за рахунок ринкових можливостей (попит на системи контролю доступом)	Диференційований маркетинг	Бездротовість, низька собівартість, високий рівень захисту	Стратегія диференціації

Для розроблюваного стартап-проєкту обрано стратегію диференціації, оскільки продукт має чіткі унікальні переваги у вигляді бездротової архітектури, підвищеного рівня захисту даних та можливості мобільного керування, що дозволяє відрізнити його від більшості конкурентних рішень на ринку.

Наступним етапом проаналізуємо та оберемо стратегію конкурентної поведінки (табл. 5.16).

Таблиця 5.16. Визначення базової стратегії конкурентної поведінки

Чи є проєкт “першопрохідцем” на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки
Ні	Так	Повної копії не буде. Можливе запозичення принципів роботи, але покращене	Стратегія наслідування лідера

Аналіз показав, що розроблюваний проєкт не є першопрохідцем на ринку та орієнтується на активне залучення частини споживачів від існуючих конкурентів. При цьому обрана стратегія не передбачає прямого копіювання рішень, а ґрунтується на запозиченні базових принципів роботи з їх подальшим удосконаленням. Саме тому для проєкту обрано стратегію наслідування лідера, яка дозволяє використати перевірені ринком підходи, зменшити ризики впровадження та підвищити конкурентоспроможність за рахунок покращених технічних і функціональних характеристик. Для подальшого уточнення підходів опишемо вибір стратегії позиціонування (табл. 5.17).

Таблиця 5.17. Визначення стратегії позиціонування

Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проєкту	Вибір асоціацій, які мають сформувати комплексну позицію власного проєкту (три ключових)
Легке масштабування, безпека, доступна ціна, бездротовість	Стратегія диференціації	Бездротова передача даних (LoRa), шифрування AES-128, гнучке адміністрування, просте масштабування	Безпека Зручність Інноваційність

Для стартап-проєкту обрано стратегію диференціації, що дозволяє виділити продукт серед конкурентів за рахунок бездротовості, безпеки та зручності, а стратегія наслідування лідера зменшує ризики завдяки використанню перевірених ринком рішень. Сформоване позиціонування на основі асоціацій «безпека – зручність – інноваційність» відповідає очікуванням цільової аудиторії та підсилює конкурентні переваги проєкту.

5.5 Розробка маркетингової програми стартап-проєкту

На цьому етапі розроблення стартап-проєкту важливим є формування ефективної маркетингової програми, яка дозволить забезпечити впізнаваність продукту, зацікавленість потенційних клієнтів та стабільний попит на ринку. Основою такої програми є визначення ключових переваг концепції потенційного товару, які відрізняють його від конкурентних рішень та формують цінність для споживача. Ключові переваги концепції потенційного товару наведено в таблиці 5.18.

Таблиця 5.18. Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1.	Бездротова архітектура	Відсутність необхідності прокладання кабелів, швидкий монтаж, легке масштабування	Повністю бездротове з'єднання між пристроями
2.	Мобільне керування	Адміністрування доступу з телефону	Керування та редагування бази користувачів через мобільний додаток
3.	Безпека	Захист від клонування, перехоплення та підміни даних	Використання AES-128, CRC, локальне зберігання бази даних
4.	Ціна	Доступність для малого та середнього бізнесу	Нижча загальна вартість системи за рахунок впровадження сучасних технологій

Отже, проведений аналіз показав, що ключові потреби споживачів – це бездротовість, мобільне керування, безпека та доступна ціна, котрі повною мірою задовольняються розроблюваним товаром і формують його основні конкурентні переваги. Для розуміння структури цінності продукту розглянемо модель товару за трьома рівнями (табл. 5.19).

Таблиця 5.19. Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
I. Товар за задумом	Система контролю доступу на основі технологій LoRa та RFID		
II. Товар у реальному виконанні	Властивості / характеристики	М / Нм	Вр/Тх/Тл/Е/Ор
	1. Бездротовість	Нм	Тх
	2. Мобільне керування	Нм	Ор
	3. Безпека	М	Тх
	4. Ціна	М	Вр
	Якість: сертифікати якості ISO		
	Пакування: картонна коробка з інструкцією та комплектом для монтажу		
Марка: WirelessGate			
III. Товар із підкріпленням	До продажу: демонстрація можливостей, консультація щодо вибору та встановлення, технічна підтримка		
	Після продажу: гарантійне обслуговування, оновлення прошивки, сервісна підтримка		
За рахунок чого потенційний товар буде захищений від копіювання: патент, охоронні документи.			

Отже, розглянута модель товару за трьома рівнями показує, що розроблюваний пристрій поєднує в собі функціональну сутність сучасної бездротової системи доступу, реальні технічні та експлуатаційні характеристики, а також комплекс сервісної та правової підтримки, що підвищує його цінність для споживача.

Наступним кроком є визначення меж встановлення ціни (табл. 5.20).

Таблиця 5.20. Визначення меж встановлення ціни

Рівень цін на товари-замінники, грн	Рівень цін на товари-аналоги, грн	Рівень доходів цільової групи споживачів, грн	Верхня та нижня межі встановлення ціни на товар/послугу, грн
800-3000	3000-5000	40000-90000	800-2000

Наступним етапом є формування системи збуту (табл. 5.21).

Таблиця 5.21. Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Закупка в малій або середній кількості	Консультація клієнтів, продаж обладнання, постійна технічна підтримка	Прямий	Прямий

Проаналізувавши формування системи збуту бачимо, що для стартап-проєкту найбільш доцільною є коротка збутова мережа з орієнтацією на прямі продажі. Такий підхід відповідає специфіці закупівельної поведінки малих і середніх підприємств, складів та офісів та дозволяє зменшити витрати на посередників.

Для ефективної реалізації обраної системи збуту необхідно сформувати дієву концепцію маркетингових комунікацій (табл. 5.22).

Таблиця 5.22. Концепція маркетингових комунікацій

Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
Орієнтація на співвідношення ціна/функціонал	Соціальні мережі, вебсайт проєкту, онлайн маркетплейси	Бездротовість, безпека, простота використання, мобільне керування, економічність	Сформувати довіру до нового продукту, показати його практичну користь	Акцент на зручності та безпеці

5.6 Висновки до розділу 5

У розділі опрацьовано концепцію стартап-проєкту бездротової системи контролю доступу на основі технологій LoRa та RFID. Проведено аналіз цільової аудиторії, ринкового середовища, конкурентів, а також визначено ключові переваги розроблюваного продукту. Встановлено, що основними споживачами системи є малі та середні підприємства, склади й офіси, для яких вирішальними чинниками є бездротовість, безпека, простота встановлення, мобільне керування та доступна ціна.

На основі SWOT-аналізу, аналізу конкурентної поведінки та факторів конкурентоспроможності обґрунтовано вибір стратегії диференціації та стратегії наслідування лідера, що дозволяє поєднати перевірені ринкові підходи з власними інноваційними перевагами. Сформовано маркетингову програму, визначено систему збуту, ключові підходи до ціноутворення та концепцію маркетингових комунікацій.

Результати виконаного аналізу демонструють, що розроблюваний стартап-проєкт має реальні можливості для успішного виходу на ринок завдяки поєднанню

інноваційності, безпеки та зручності використання. Запропоновані маркетингові та конкурентні стратегії дозволяють знизити ризики на початковому етапі впровадження та забезпечити поступовий розвиток проєкту в обраному сегменті ринку.

ВИСНОВКИ

У першому розділі проведено аналіз існуючих СКД та технологій безконтактної ідентифікації. Визначено ключові властивості RFID-міток, принципи роботи зчитувачів, стандарти взаємодії та основні вразливості традиційних рішень. Особливу увагу приділено питанням інформаційної безпеки, де встановлено, що надійність системи значною мірою залежить від використання криптографічних алгоритмів, механізмів взаємної аутентифікації та контролю цілісності даних. Показано, що найбільш ефективним підходом є поєднання програмних та апаратних методів захисту, включно з використанням сучасних алгоритмів симетричного шифрування та апаратних механізмів зберігання даних.

У другому розділі сформовано повну апаратну структуру системи, що складається з головного та другорядного пристроїв. Виконано обґрунтований вибір елементної бази, розроблено структурні і електричні схеми. Для ГП обрано мікроконтролер ESP32, RFID-зчитувач MFRC522, радіомодуль LoRa SX1278, OLED-дисплей SSD1306, світлову та звукову індикацію, енкодер та карту пам'яті micro-SD. Для ДП реалізовано аналогічну структуру з акцентом на комутацію навантажень за допомогою реле та MOSFET-транзистора. Проведено тестування всіх компонентів окремо та у складі єдиної системи, що включало збирання апаратних модулів на макетній платі та випробування базових функцій. Даний етап підтвердив їх коректну взаємодію та стабільність передачі даних.

У третьому розділі розроблено програмну частину системи, яка реалізує логіку взаємодії головного й другорядного пристроїв. Це включало вибір мови програмування та середовища розробки, створення структурних схем програмної частини головного та другорядного пристроїв, а також реалізацію функціональних блоків у коді. Реалізовано блоки, такі як очікування й обробка пакетів, запит до бази даних, формування й відправка пакету, читання та обробка RFID-міток, оновлення індикації та дисплея, асинхронні дії у вигляді обробки органів керування та оновлення стану індикацій, а також зміна стану керуючих елементів. Створено локальний графічний інтерфейс та веб-інтерфейс, що забезпечують керування базою даних та параметрами системи.

У четвертому розділі виконано проєктування апаратної частини системи. Здійснено проєктування друкованих плат, що включало визначення необхідних габаритів і форми плат, розрахунок ширини друкованих провідників та їх трасування. Спроектовано корпуси для головного та другорядного пристроїв. Завершальним етапом стало виготовлення прототипу та проведення випробувань, які підтвердили стабільну авторизацію користувачів та дальність зв'язку до 107 метрів з перешкодами.

У п'ятому розділі була проведена розробка стартап-проєкту. Проведено аналіз ринкового середовища, конкурентів та цільової аудиторії, визначено ключові переваги продукту та його позиціонування. На основі маркетингових досліджень визначено стратегії розвитку, каналів збуту та комунікацій, а також сформовано програму просування продукту на ринок. Аналіз показав, що запропонована система має комерційний потенціал завдяки поєднанню бездротовості, безпеки, простоти встановлення та низької вартості впровадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Система контролю і управління доступом. URL: <https://surl.li/zdwdlz> (дата звернення 26.10.2025).
2. Все, що потрібно знати про біометричні рішення контролю доступу. URL: <https://bezpeka.club/vse-shho-potribno-znaty-pro-biometrychni-rishennya-kontrolyu-dostupu> (дата звернення 26.10.2025).
3. Що таке СКУД? “Як влаштована і працює система контролю та управління доступом”. URL: <https://surl.li/espaxi> (дата звернення 03.11.2025).
4. Аутентифікація, авторизація та ідентифікація. URL: <https://training.qatestlab.com/blog/technical-articles/authentication-authorization-and-identification/> (дата звернення 26.10.2025).
5. RFID. Радіочастотна ідентифікація. URL: <https://surl.lu/eerxds> (дата звернення 28.10.2025).
6. Secure Access Control Solutions. HID Global. URL: <https://www.hidglobal.com/solutions/access-control-systems> (дата звернення 09.11.2025).
7. Dahua Technology. URL: <https://dahua-technology.com.ua/kontrol-dostupa/> (дата звернення 09.11.2025).
8. ATIS – передові технології безпеки. URL: <https://atis-security.com/ua/> (дата звернення 09.11.2025).
9. KEENFINITY: Access Control Systems. URL: <https://www.keenfinity-group.com/xc/en/solutions/access-control-systems/> (дата звернення 09.11.2025).
10. MIFARE cards: What are they, what are the different types available? URL: <https://www.usmartcards.co.uk/news-blog/mifare-cards-what-are-they-where-are-they-used-and-what-are-the-different-types-available#:~:text=MIFARE%20is%20a%20contactless%20smart,them%20highly%20efficient%20and%20secure>. (дата звернення 28.10.2025).
11. Стандарт ISO/IEC 14443. URL: https://ru.wikipedia.org/wiki/ISO/IEC_14443 (дата звернення 09.11.2025).

12. Стандарт ISO/IEC 15693. URL: https://ru.wikipedia.org/wiki/ISO/IEC_15693 (дата звернення 09.11.2025).
13. What is AES 128 Bit Encryption and How Secure AES 128-Bit is? URL: [https://cheapsslweb.com/blog/what-is-aes-128-bit-encryption/#:~:text=AES%20128%20is%20an%20example,permutation%20network%20\(SPN\)%20model](https://cheapsslweb.com/blog/what-is-aes-128-bit-encryption/#:~:text=AES%20128%20is%20an%20example,permutation%20network%20(SPN)%20model). (дата звернення 05.11.2025).
14. What is Radio Frequency Identification (RFID) Technology? URL: <https://electronicsntech.blogspot.com/2012/10/what-is-radio-frequency-identification.html> (дата звернення 16.11.2025).
15. Історія розвитку RFID технології. URL: <https://provotkin.com.ua/ru/blog-ru/istoriya-rozvytku-rfid-tehnologiyi> (дата звернення 16.11.2025).
16. Active vs. Passive RFID: Which Is Right for Your Use Case? URL: <https://redbeam.com/blog/resources/active-vs-passive-rfid#:~:text=Active%20RFID%20tags%20are%20radio,%2C%20tag%20size%2C%20a nd%20antenna>. (дата звернення 16.11.2025).
17. Як визначити тип картки доступу: види безконтактних карток RFID. URL: <https://secur.ua/news/iak-viznaciti-tip-kartki-dostupu-vidi-bezkontaktnix-kartok-rfid> (дата звернення 08.11.2025).
18. Why is ESP the most used IoT connectivity MCU. URL: <https://www.byte-lab.com/why-is-esp-the-most-used-iot-connectivity-mcu/> (дата звернення 17.11.2025).
19. LoRa. URL: <https://uk.wikipedia.org/wiki/LoRa> (дата звернення 09.11.2025).
20. Documentatin Espressif ESP32-WROOM-32E, ESP32-WROOM-32UE. URL: https://documentation.espressif.com/esp32-wroom-32e_esp32-wroom-32ue_datasheet_en.pdf (дата звернення 17.11.2025).
21. MFRC522 RFID Module. Specification. URL: https://mm.digikey.com/Volume0/opasdata/d220001/medias/docus/5531/4411_CN0090%20other%20related%20document%20%281%29.pdf (дата звернення 30.11.2025).
22. Модуль LoRa RA-02 SX1278. URL: <https://www.mini-tech.com.ua/lora-ra-02> (дата звернення 09.11.2025).
23. Що таке модуль LoRa. URL: <https://jooby.eu/uk/blog/sho-take-modul-lora/> (дата звернення 30.11.2025).

24. What is microSD card. Important FAQs. URL: <https://americas.lexar.com/microsd-card-guide/#:~:text=A%20microSD%20card%2C%20short%20for,to%20store%20and%20transfer%20data>. (дата звернення 01.11.2025).

25. Зінгер Я.Л., Адаменко Ю.Ф. Наскрізна розробка інтелектуальної техніки. Конспект лекцій [Електронний ресурс]: навч. посіб. для студентів спеціальності 172 «Електронні комунікації та радіотехніка». – Київ : КПІ ім. Ігоря Сікорського, 2023. – 45 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/f86043c1-c105-4f59-ba6b-25fbf12015b5/content> (дата звернення 28.11.2025).

26. PCB Trace Width Calculator. URL: https://www.pcbway.com/pcb_prototype/trace-width-calculator.html (дата звернення 22.11.2025).

ДОДАТОК А

Інв. № ориг.

Підп. і дата

Зам. інв. №

Інв. № дубл.

Підп. і дата

Перв. застосування

ЕЗ 1416.001.464.116.001

PI41P

USB TYPE-C

Лінійний стабілізатор 3.3В

RFID сканер

Карта пам'яті

Мікроконтролер

RGB світлодіод

Бuzzer, дисплей

Зм. №	№ докум.	Підп.	Дата	Система контролю доступу	Лт.	Маса	Масштаб
Розробив	Слободяний	М.І.		головний пристрій			
Перевірив	Піліпцев С.І.			Схема електрична принципова	Друкує 1	Друкує 1	
Н. контр.				Зав.			

ДОДАТОК Б

Інв. № ориг.

Підп. і дата

Зам. інв. №

Інв. № дубл.

Підп. і дата

Перв. застосування

ЕЗ 200.0116.002 ЕЗ

PI-41MP.464116.002 ЕЗ

USB TYPE-C

Лінійний стабілізатор 3.3В

RFID сканер

Реле

Мікроконтролер

LORA

MOSFET, GPIO

RGB світлодіод, кнопка

Buzzer

Зм. Док. № док.м.	Підп.	Дата
Розробка	Сторожук М.П.	
Перевірив	Пічків С.В.	
Н.контр.		
Затв.		

Система контролю доступу

двухрядний пристрій

Схема електрична принципова

Лист

Маса

Масштаб

Архив 1

Архив 1

ДОДАТОК В

Блок коду «Запит до бази даних»

```

void writeFile(fs::FS &fs, const char *path, const char *message)
{
    Serial.printf("Writing file: %s\n", path);

    File file = fs.open(path, FILE_WRITE);
    if (!file)
    {
        Serial.println("Failed to open file for writing");
        return;
    }
    if (file.print(message))
    {
        Serial.println("File written");
    }
    else
    {
        Serial.println("Write failed");
    }
    file.close();
}

void listDir(fs::FS &fs, const char *dirname, uint8_t levels)
{
    Serial.printf("Listing directory: %s\n", dirname);

    File root = fs.open(dirname);
    if (!root)
    {
        Serial.println("Failed to open directory");
        return;
    }
    if (!root.isDirectory())
    {
        Serial.println("Not a directory");
        return;
    }

    File file = root.openNextFile();
    while (file)
    {
        if (file.isDirectory())
        {
            Serial.print("  DIR : ");
            Serial.println(file.name());
            logger.print("  DIR : ");
            logger.println(file.name());

            if (levels)
            {

```

```

        listDir(fs, file.name(), levels - 1);
    }
}
else
{
    Serial.print(" FILE: ");
    Serial.print(file.name());
    Serial.print(" SIZE: ");
    Serial.println(file.size());
    logger.print(" FILE: ");
    logger.print(file.name());
    logger.print(" SIZE: ");
    logger.println(file.size());
}
file = root.openNextFile();
}
}

```

```

void readFile(fs::FS &fs, const char *path, int linesPerChunk = 5)

```

```

{
    loggerSDcard.printf("Reading file: %s\n", path);

    File file = fs.open(path);
    if (!file)
    {
        loggerSDcard.println("Failed to open file for reading");
        return;
    }

    int lineCount = 0;
    String buffer = "";

    while (file.available())
    {
        String line = file.readStringUntil('\n');
        line.trim();

        buffer += line + "\n"; // Додаємо рядок в буфер
        lineCount++;

        if (lineCount >= linesPerChunk) // Якщо зібрали linesPerChunk рядків — виводимо
        {
            Serial.print(buffer);      // вивід на серійний монітор
            loggerSDcard.println(buffer); // вивід пачки

            buffer = ""; // очищаємо для наступних рядків
            lineCount = 0;
        }
    }

    if (lineCount > 0) // Якщо файл закінчився, а в буфері щось є
    {
        Serial.print(buffer);
    }
}

```

```

    loggerSDcard.println(buffer);
}

file.close();
}

bool deleteUserFromDB(String uid)
{
    File inFile = SD.open(DB_FILE_NAME, FILE_READ);
    if (!inFile)
        return false;

    File outFile = SD.open("/tmp.csv", FILE_WRITE); // Тимчасовий файл
    if (!outFile)
    {
        inFile.close();
        return false;
    }

    bool deleted = false;

    while (inFile.available())
    {
        String line = inFile.readStringUntil('\n');
        line.trim();
        if (line.length() == 0)
            continue;

        int c1 = line.indexOf(',');
        if (c1 == -1)
            continue;

        String uidField = line.substring(0, c1);

        if (uidField == uid) // Якщо UID співпав — пропускаємо (видаляємо)
        {
            deleted = true;
            continue; // НЕ записуємо рядок в новий файл
        }

        outFile.println(line); // Інакше — копіюємо рядок у новий файл
    }

    inFile.close();
    outFile.close();

    if (deleted) // Якщо запис видалено — замінюємо файл
    {
        SD.remove(DB_FILE_NAME); // видаляємо старий
        SD.rename("/tmp.csv", DB_FILE_NAME); // замінюємо новим
    }
    else
    {
        SD.remove("/tmp.csv"); // UID не знайдено — тимчасовий файл зайвий
    }
}

```

```

    }

    return deleted;
}

bool editUser(const String &uid, const String &newName, int newLevel)
{
    File f = SD.open(DB_FILE_NAME, FILE_READ);
    if (!f)
    {
        Serial.println("Error opening DB for edit");
        return false;
    }

    File tmp = SD.open("/tmp.csv", FILE_WRITE); // Тимчасовий файл
    if (!tmp)
    {
        Serial.println("Error creating temp file");
        f.close();
        return false;
    }

    bool replaced = false;

    while (f.available())
    {
        String line = f.readStringUntil('\n');
        line.trim();
        if (line.length() == 0)
        {
            continue;
        }

        if (line.startsWith("UID,") // Заголовок не чіпаємо
        {
            tmp.println(line);
            continue;
        }

        int c1 = line.indexOf(','); // Парсимо UID
        if (c1 == -1)
        {
            tmp.println(line);
            continue;
        }

        String uidField = line.substring(0, c1);

        if (uidField == uid) // Формуємо новий рядок
        {
            String newLine = uid + ",";
            newLine += newName + ",";
            newLine += String(newLevel) + ",";
            newLine += sett.rtc.toString(); // дата/час
        }
    }
}

```

```

        tmp.println(newLine);
        replaced = true;
    }
    else
    {
        tmp.println(line); // залишаємо як було
    }
}

f.close();
tmp.close();
SD.remove(DB_FILE_NAME); // Замінюємо старий файл новим
SD.rename("/tmp.csv", DB_FILE_NAME);

return replaced;
}

bool findUser(String uid, String &outName, int8_t &outLevel, String &outDateTime)
{
    File f = SD.open(DB_FILE_NAME);
    if (!f)
        return false;

    while (f.available())
    {
        String line = f.readStringUntil('\n');
        line.trim();
        if (line.length() == 0)
            continue;

        int c1 = line.indexOf(','); // Парсимо першу кому (UID)
        if (c1 == -1)
            continue;

        String uidField = line.substring(0, c1);

        if (uidField == uid)
        {
            int c2 = line.indexOf(',', c1 + 1); // Знайшли запис! Тепер парсимо інше
            int c3 = line.indexOf(',', c2 + 1);

            if (c2 == -1 || c3 == -1)
            {
                f.close();
                return false; // некоректний рядок
            }
            outName = line.substring(c1 + 1, c2);
            outLevel = line.substring(c2 + 1, c3).toInt();
            outDateTime = line.substring(c3 + 1);
            f.close();
            return true;
        }
    }
}

```

```

    f.close();
    return false; // UID не знайдено
}
bool uidExists(String uid)
{
    File f = SD.open(DB_FILE_NAME);
    if (!f)
        return false;

    while (f.available())
    {
        String line = f.readStringUntil('\n');
        int commaIndex = line.indexOf(',');
        if (commaIndex == -1)
            continue;
        String uidField = line.substring(0, commaIndex);

        if (uidField == uid)
        {
            f.close();
            return true;
        }
    }
    f.close();
    return false;
}

bool addRecord(String uid, String name, int level)
{
    String dt = sett.rtc.toString();

    File f = SD.open(DB_FILE_NAME, FILE_APPEND);
    if (!f)
    {
        Serial.println("DB open error");
        return false;
    }

    f.print(uid);
    f.print(",");
    f.print(name);
    f.print(",");
    f.print(level);
    f.print(",");
    f.println(dt);

    f.close();

    Serial.println("Запис зроблено:");
    Serial.println(uid + "," + name + "," + level + "," + dt);
    return true;
}

```

Блок коду «Формування й відправка пакету»

```

bool buildAndSend(uint8_t to, uint16_t msgId, uint8_t type,
                  const uint8_t *payload, uint8_t len)
{
    uint8_t raw[256];
    size_t r = 0;

    raw[r++] = 9;    // 0 access_level
    raw[r++] = HUB_ID;    // 1 from (хаб)
    raw[r++] = to;    // 2 to (кому)
    raw[r++] = (msgId >> 8) & 0xFF;    // 3 msgIdH
    raw[r++] = msgId & 0xFF;    // 4 msgIdL
    raw[r++] = type;    // 5 TYPE_ACK / CMD_OPEN / інше
    raw[r++] = len;    // 6 payload довжина

    if (len && payload)
    {
        memcpy(&raw[r], payload, len);
        r += len;
    }

    // --- ШИФРУЄМО ---
    uint8_t encrypted[256];
    uint16_t encLen = encryptBlock(raw, r, encrypted);

    // --- ПАКЕТ ---
    uint8_t buf[256];
    size_t idx = 0;

    buf[idx++] = PREAMBLE;
    memcpy(&buf[idx], encrypted, encLen);
    idx += encLen;

    uint8_t crc = crc8(&buf[1], encLen);
    buf[idx++] = crc;

    LoRa.beginPacket();
    LoRa.write(buf, idx);
    LoRa.endPacket();
    LoRa.receive();
    return true;
}

uint16_t encryptBlock(const uint8_t *input, uint16_t inLen, uint8_t *output)
{
    memcpy(iv_enc, aes_iv, 16);

    return aesLib.encrypt(
        (byte *)input,
        inLen,
        (byte *)output,
        aes_key,
        sizeof(aes_key),

```

```

    iv_enc);
}

uint8_t crc8(const uint8_t *data, size_t len) // ---- CRC8 ----
{
    uint8_t crc = 0x00; // Початкове значення CRC
    while (len--) // Проходимо всі байти масиву
    {
        uint8_t b = *data++; // Беремо наступний байт та зсуваємо вказівник
        for (uint8_t i = 0; i < 8; i++) // Обробляємо кожен з 8 бітів байта
        {
            uint8_t mix = (crc ^ b) & 0x01; // mix = XOR молодших бітів CRC і байта
            crc >>= 1; // Зсуваємо CRC праворуч
            if (mix) // Якщо mix = 1 – треба XOR з поліномом
                crc ^= 0x8C; // 0x8C — поліном CRC8 (Dallas/Maxim)
            b >>= 1; // Зсуваємо вхідний байт праворуч
        }
    }
    return crc; // Повертаємо обчислений CRC
}

```

ДОДАТОК Г

*Інформаційні технології та телекомунікаційні системи***СИСТЕМА АВТОРИЗАЦІЇ
З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ LoRa***Слободяник М. П.; Літвінцев С. М., к.т.н.**Національний технічний університет України**«Київський політехнічний інститут імені Ігоря Сікорського»,**м. Київ, Україна***Вступ**

Системи контролю доступу [1] відіграють ключову роль у забезпеченні безпеки будівель, виробничих та адміністративних приміщень. Із зростанням вимог до надійності та зручності експлуатації особливо актуальними стали безконтактні технології ідентифікації [2], серед яких RFID вирізняється швидкістю роботи, стійкістю до механічного зношення та простою інтеграції [3]. У різних галузях зростає попит на системи авторизації, що підтримують захищений обмін даними, стабільну ідентифікацію користувачів та гнучке розширення функцій.

На сьогодні існуючі системи вирізняються високою вартістю, оскільки використовують спеціальні протоколи для розширення системи. Автори пропонують використати для цього відомий протокол LoRa [4], який вирізняється не вибагливістю до ресурсів та великою відстанню бездротової роботи.

Мета проєкту

У рамках даної роботи авторами розроблено працюючий макет RFID-системи, що поєднує механізми захищеної передачі інформації, модульну побудову та можливість масштабування для використання в різних умовах. Проєкт спрямований на створення надійного рішення, здатного забезпечити ідентифікацію користувачів, зберігати історію подій та ефективно працювати в реальних умовах. Структурна схема системи представлена на рис. 1.

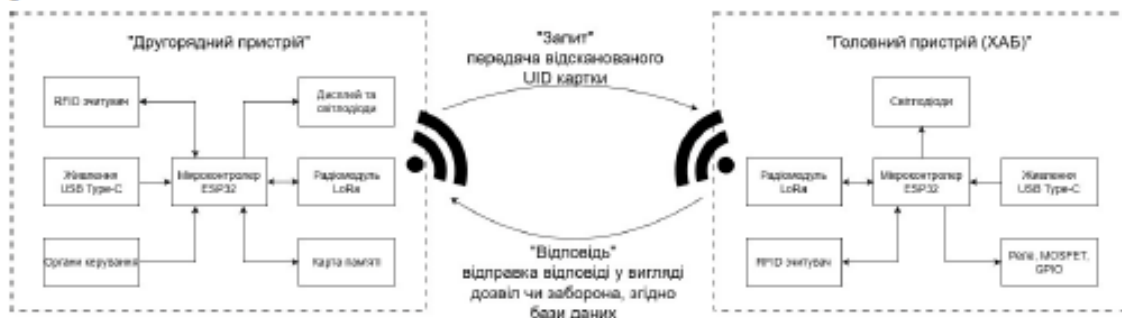


Рис. 1. Структурна схема запропонованої системи контролю доступу

Метою роботи було створення та експериментальне дослідження повністю функціонального прототипу системи контролю доступу з використанням технологій LoRa та RFID (рис. 2).

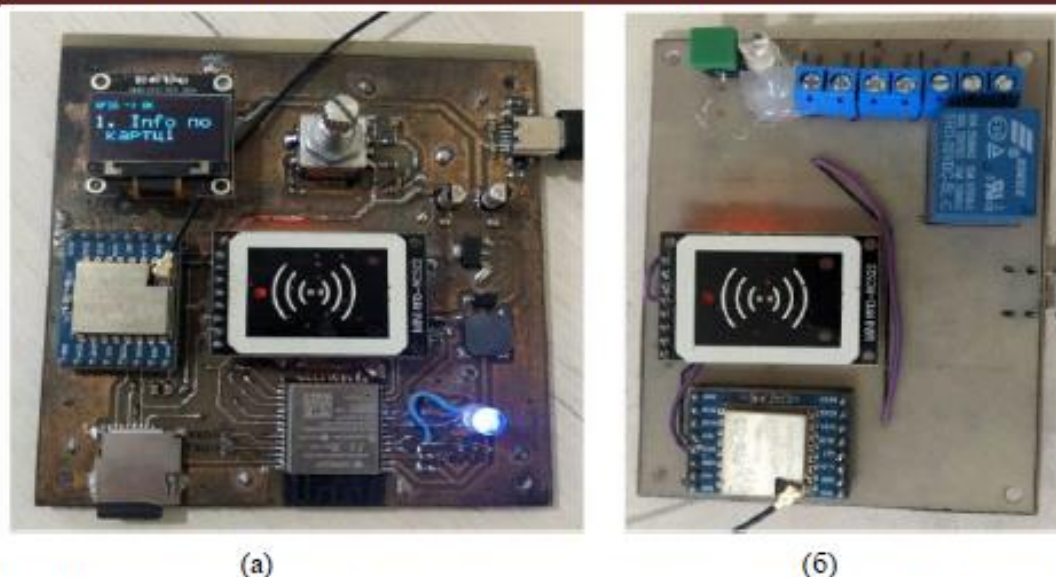


Рис. 2. Фото прототипа елементів системи контролю доступу: а -- головний пристрій, б -- другорядний пристрій

Методи і технічні рішення

Розробка системи базувалася на поєднанні теоретичного аналізу RFID-технологій і практичного конструювання. У рамках проекту розроблено апаратну частину на основі мікроконтролера ESP32 [5], створено логіку обробки UID-кодів, реалізовано захист даних та механізм збереження інформації на SD-картці.

Робота також включає проектування електричної схеми та створення програмного забезпечення. Мікроконтролер забезпечує роботу RFID-зчитувача, SD-карти і модуля LoRa у межах єдиної системи [6]. Програмна реалізація виконана мовою C++ та передбачає обробку UID-кодів, ведення журналу подій і взаємодію з периферією в режимі реального часу. В алгоритмах системи передбачено захист даних, що запобігає доступу неавторизованих карток та сторонньому втручання.

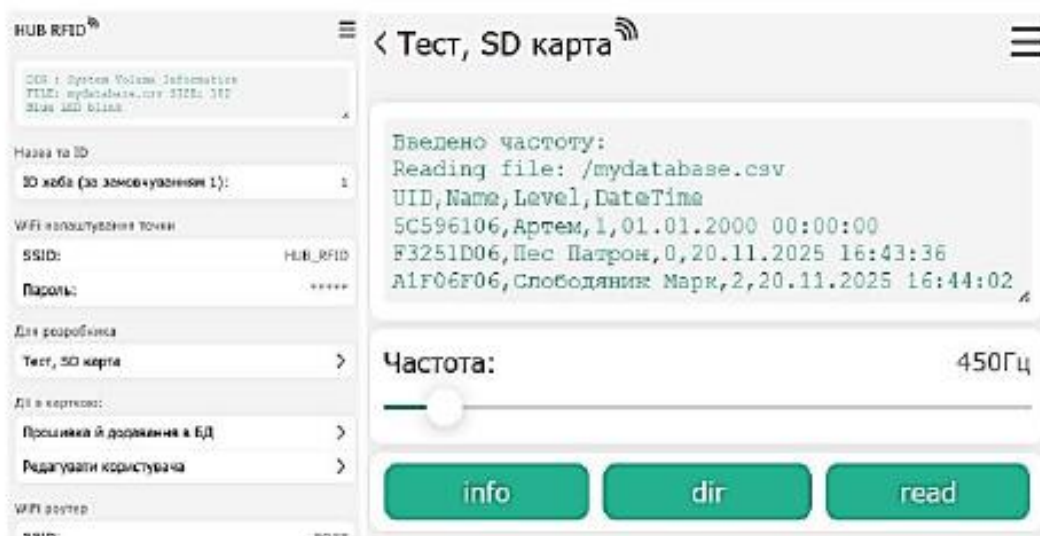


Рис. 3. Вигляд веб-сторінки налаштувань головного пристрою

Для зручного налаштування системи та керування даними розроблено веб-інтерфейс (рис. 3), доступ до якого надається по локальній WiFi мережі. Комплекс технічних рішень дозволив сформувати стабільну платформу для авторизації [7] користувачів у системі.

Висновки

Розроблений прототип системи авторизації з використанням технологій LoRa та RFID довів ефективність комплексного підходу, який об'єднує апаратні та програмні рішення для досягнення високої надійності та безпеки. Реалізовані алгоритми ідентифікації і захисту інформації забезпечують коректну роботу системи та стійкість до несанкціонованих дій. Практичні випробування підтвердили працездатність апаратного макета та його готовність до подальшого використання або розширення.

Перелік посилань

1. Система контролю і управління доступом [Електронний ресурс] — Режим доступу до ресурсу: <https://surl.li/edvzyv>
2. Радіочастотна ідентифікація [Електронний ресурс] — Режим доступу до ресурсу: <https://surl.li/lfcfgr>
3. RFID-технологія [Електронний ресурс] — Режим доступу до ресурсу: <https://www.imena.ua/blog/rfid-technology/>
4. LoRa [Електронний ресурс] — Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/LoRa>
5. Datasheet ESP32_WROOM_32E [Електронний ресурс] — Режим доступу до ресурсу: <https://fcc.report/FCC-ID/2AC7Z-ESP32WROOM32E/4684794.pdf>
6. Module LoRa [Електронний ресурс] — Режим доступу до ресурсу: <https://jooby.eu/uk/blog/sho-take-modul-lora/>
7. Авторизація [Електронний ресурс] — Режим доступу до ресурсу: <https://training.gatestlab.com/blog/technical-articles/authentication-authorization-and-identification/>

Анотація

У роботі представлено розробку апаратно-програмного комплексу системи авторизації з використанням технології LoRa (Long Range). Проєкт включає аналіз сучасних методів контролю доступу, побудову апаратної частини на базі мікроконтролера ESP32, реалізацію програмного забезпечення для обробки UID-кодів RFID-карток, організацію локального зберігання даних на SD-карті та створення розподіленої структури вузлів з використанням радіоканалу LoRa.

Розроблена система забезпечує надійну ідентифікацію користувачів, гнучкість конфігурації та можливість інтеграції з іншими пристроями. Наведено результати тестування, що підтверджують працездатність та ефективність запропонованого рішення.

Ключові слова: RFID, авторизація, ESP32, LoRa, контроль доступу, ідентифікація.

Abstract

This paper presents the development of a hardware–software authorization system based on Long Range (LoRa) technology. The project includes an analysis of modern access control methods, the implementation of a hardware module based on the ESP32 microcontroller, software for processing RFID card UIDs, local data storage on an SD card, and a distributed node structure using LoRa communication.

The designed system provides reliable user identification, flexible configuration, and the possibility of integration with other devices. Testing results confirm the functionality and efficiency of the proposed solution.

Keywords: RFID, authorization, ESP32, LoRa, access control, identification.