Вінницький національний технічний університет
(повне найменування вищого навчального закладу)
Факультет інформаційних технологій та комп'ютерної інженерії
(повне найменування інституту, назва факультету (відділення))
Кафедра обчислювальної техніки
(повна назва кафедри (предметної, циклової комісії)

Пояснювальна записка

до комплексної магістерської кваліфікаційної роботи
магістр
(освітньо-кваліфікаційний рівень)

на тему: "Комплекс мобільного керування автоматикою пропуску. Частина 1. "Апаратна частина"

08-54.КМКР.007.00.000 ПЗ

Виконав: студент групи 2КІ-22м
спеціальності
123 – Комп'ютерна інженерія
(шифр і назва напряму підготовки, спеціальності)
Гуменюк В.В.
(прізвище та ініціали)
Керівник: к.т.н., доц. каф.ОТ
Городецька О.С.,
(прізвище та ініціали)
Опонент: к.т.н., доц.каф.МБІС
Карпінець В.В.
(прізвище та ініціали)

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.
10 06 2024 року

Вінниця ВНТУ – 2024 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітньо-кваліфікаційний рівень —магістр
Спеціальність 123 — «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
Азаров О. Д.
«12» 03 2024 року

З А В Д А Н Н Я
НА КОМПЛЕКСНУ МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Гуменюку Вадиму Васильовичу
(прізвище, ім'я, по батькові)

1 Тема роботи: "Комплекс мобільного керування автоматикою пропуску". Частина 1. Апаратна частина", керівник роботи: к.т.н., доцент кафедри ОТ Городецька О. С., затверджена наказом Вінницького національного технічного університету від 11.03.2024 року № 81.

2 Строк подання студентом роботи: 24.05.2024

3 Вихідні дані до роботи: системи контролю і управління доступом, комплекс дистанційного керування автоматикою пропуску з використанням мобільного застосунку на смартфоні, два канали керування, пристрій керування з технологіями Bluetooth, Wi-Fi, методика тестування й перевірки параметрів комплексу.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): огляд і аналіз систем контролю та керування пропуском; вибір технологій, методів і засобів розробки апаратної частини; розробка апаратних складових комплексу; дослідження й випробування комплексу; розрахунок економічних показників.

3

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Схеми структурна, функціональна пристрою керування, схеми та ілюстративний матеріал щодо розробки апаратної частини.

6 Консультанти розділів роботи наведені в таблиці 1.

Таблиця 1 — Консультанти роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1,2,3,4	Крупельницький Л. В., к.т.н., доцент каф. ОТ		
5	Небава М.І., к.е.н., професор каф. ЕПВМ		

7 Дата видачі завдання 01.03.2024

8 Календарний план виконання МКР наведено в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів дипломної магістерської роботи	Строк виконання етапів роботи	Примітка
1	Огляд і аналіз систем контролю та керування пропуском	30.03.2024	Виконано
2	Вибір технологій, методів і засобів розробки апаратної частини	20.04.2024	Виконано
3	Розробка апаратних складових комплексу;	10.05.2024	Виконано
4	Дослідження й випробування комплексу	20.05.24	Виконано
5	Економічна частина	24.05.2024	Виконано

Студент _____ Гуменюк В.В.
(підпис) (прізвище та ініціали)

Керівник магістерської кваліфікаційної роботи _____ Городецька О.С.
(підпис) (прізвище та ініціали)

Консультант з економічної частини _____ Небава М.І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

УДК 004.4

Гуменюк В.В. "Комплекс мобільного керування автоматикою пропуску". Частина 1. "Апаратна частина" Комплексна магістерська кваліфікаційна робота зі спеціальності 123 - Комп'ютерна Інженерія, Вінниця: ВНТУ, 2024, 103 с.

На укр. мові. Бібліогр.: 103 сторінки, 5 розділів, 32 рисунка, 22 таблиці, 42 дерел посилання.

У роботі розроблено систему віддаленого управління доступом за мобільним ідентифікатором, що надається віддалено через Інтернет. Проведено аналіз сучасних технологій управління доступом, розглянуті основні принципи побудови систем управління доступом, вибрано та проаналізовано аналоги, розглянуто принципи та технології віддаленого керування доступом, визначено підходи до побудови системи віддаленого керування доступом з розширеними функціональними можливостями, що забезпечує керування доступом при втраті зв'язку з Інтернет. Розроблено структурну та функціональні схеми контролера керування доступом.

Ключові слова: управління доступом, контролер управління доступом, мобільна ідентифікація, Bluetooth з'єднання, хмарний сервер.

.

ABSTRACT

Humeniuk, Vadym V. "Mobile Control System for Access Automation". Part 1. "Hardware Component" Comprehensive Master's Qualification Thesis in the specialty 123 - Computer Engineering, Vinnytsia: VNTU, 2024.

In Ukrainian. Bibliography: 103 pages, 5 sections, 32 figures, 22 tables, 42 sources listed in the references.

The work examines the principles of building a remote access control system using a mobile identifier provided remotely via the Internet. The analysis of modern access control technologies is conducted, the basic principles of access control systems are considered, and the principles and technologies of remote access control are reviewed. Approaches to developing software for a remote access control system with extended functionalities, which ensures access control in the event of Internet connection loss, are determined. Software for the web server, administrator application, and client application is developed. Testing and comprehensive verification of the developed system are conducted.

Keywords: access control, mobile identification, wireless connection, cloud server, web application.

ЗМІСТ

ВСТУП ……..… 8
1 ОГЛЯД І АНАЛІЗ СИСТЕМ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ І АВТОМАТИКОЮ ПРОПУСКУ ……..…. 10
1.1 Типові системи контролю доступу ……. 10
1.2 Принципи функціонування і основні складові СКУД …….. 11
1.3 Керування доступом як послуга - ACaaS …….....13
1.4 Порівняння контролерів керування пропуском – аналогів комплексу, що розробляється ….....16
2 ВИБІР ТЕХНОЛОГІЙ, МЕТОДІВ І ЗАСОБІВ ДЛЯ РОЗРОБКИ АПАРАТНОЇ ЧАСТИНИ КОМПЛЕКСУ ……..……21
2.1 Технології ідентифікації ……21
2.2 Технології мобільної ідентифікації NFC та BLE …… 26
2.3 Структурна схема та принцип дії комплексу керування пропуском ….....30
3 РОЗРОБКА АПАРАТНИХ СКЛАДОВИХ КОМПЛЕКСУ …...……..31
3.1 Аналіз можливої реалізації структурних блоків і вибір елементної бази .31
3.2 Розробка функціональної та принципової схем пристрою керування ……..48
4 Дослідження й випробування розробленого комплексу керування автоматикою пропуску LOKKYY…. 52
4.1 Установка, підготовка до роботи і початок роботи з комплеком…….....52
4.2 Вимоги до функціональних можливостей …….. 58
4.3 Основні показники призначення, що контролюються …….…….. 58
4.4 Програма випробування комплексу ……..…… 59
4.5 Основні методи контролювання ……..…….. 61

					08-54.КМКР.007.00.000 ПЗ		
Змн.	Лист	№ докум.	Підпис	Дата			
Розробив		Гуменюк В.В.			Комплекс мобільного керування автоматикою пропуску. Частина 1. Апаратна частина. Пояснювальна записка	Літ.	Аркуш 6 / Аркушів 103
Перевірив		Городецька О.С.					
Реценз.		Карпінець В.В				ВНТУ, гр. КІ-22мз	
Н. контр.		Швець С.І.					
Затвердж.		Азаров О.Д					

5 ЕКОНОМІЧНА ЧАСТИНА ……..….68
5.1 Комерційний та технологічний аудит науково-технічної розробки …….….68
5.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи ……..….. 71
5.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором …… 79
ВИСНОВКИ …….. 86
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ ……..……87
ДОДАТОК А Технічне завдання…… 92
ДОДАТОК Б Схема комплексу дистанційного керування доступом …… 97
ДОДАТОК В Структурна схема контролера керування доступом ……. 98
ДОДАТОК Г Функціональна схема контролера керування доступом …… 99
ДОДАТОК Д Блок-схема алгоритму роботи контролера доступу …..…….....100
ДОДАТОК Е Склад апаратної частини комплексу ……..… 101
ДОДАТОК Ж Основні технічні параметри ……..…. 102
ДОДАТОК И Протокол перевірки кваліфікаційної роботи на наявність текстових запозичень…….……... 103

ВСТУП

Система управління доступом включає в себе комплекс апаратно-програмних та організаційно-методичних засобів, спрямованих на забезпечення безпеки об'єктів шляхом контролю та обмеження доступу до них [1,2]. Сучасні системи управління доступом розв'язують широкий спектр завдань, таких як обмеження проникнення осіб та транспорту на територію об'єкта, ведення обліку робочого часу персоналу та контроль його руху протягом доби, а також обмеження доступу до конкретних зон.

Актуальність дослідження полягає в наростаючій потребі забезпечення безпечної експлуатації об'єктів бізнесу, житлових комплексів, промислових підприємств та об'єктів соціального призначення. Один з найефективніших і сучасних методів забезпечення комплексної безпеки різних типів об'єктів - це використання систем контролю та управління доступом. Ці системи дозволяють блокувати несанкціонований доступ на територію, в будівлю, на окремі поверхи та у приміщення.

Системи управління доступом постійно розвиваються, так само, як і інші електронні інформаційні системи. Завдяки розвитку мікроконтролерної бази, сенсорних елементів та різних технологій зв'язку, з'являються нові можливості управління доступом. Останні тенденції в цій сфері пов'язані з впровадженням IP-технологій. Більшість провідних виробників обладнання вже передбачають можливість підключення до мережі Ethernet, що дозволяє отримати додаткові можливості, такі як зручне використання обладнання, простота впровадження та невеликі витрати для систем з розвиненою IT-інфраструктурою. [3].

Об’єктом дослідження є процеси автоматизованого керування доступом до об’єктів.

Предметом дослідження є методи та засоби для дистанційного керування пропуском на об’єкти з обмеженим доступом.

Метою роботи є розширення функціональних можливостей комплексу мобільного керування доступом до об’єктів з автоматикою пропуску за рахунок

використання безпровідних технологій, інтегрованих з апаратно-програмним забезпеченням смартфонів та інтернет-мережі.

Для досягнення мети роботи потрібно розв′язати виконати такі **завдання**:

— здійснити аналіз сфер застосування систем керування доступом;

— класифікувати методи дистанційного керування автоматикою пропуску;

— запропонувати комбінований метод керування з використанням безпровідних технологій;

— розробити структуру апаратної частини комплексу;

— розробити мікропроцесорної пристрій керування;

— розробити методику випробувань апаратної частини комплексу;

— провести експериментальні дослідження та визначити технічні параметри комплексу.

В роботі мети використано такі **методи дослідження:**

— системний аналіз;

— методи структурного й схемотехнічного проектування;

— методи алгоритмічного проектування.

Новизна даного дослідження полягає в розширенні функціональних можливостей комплексу керування пропуском за рахунок застосування безпровідних технологій Bluetooth та Wi-Fi , сполучення апаратної частини з програмним забезпеченням смартфонів і використання інтернет-мережі.

Практичне значення розробленого апаратного забезпечення полягає в тому, що його функціональність дозволяє створювати сучасні системи умовного доступу на різноманітні об’єкти особистого, громадського та спеціалізованого призначення.

Апробація в доповіді та публікація тез за темою роботи [1]:

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС МОБІЛЬНОГО ДИСТАНЦІЙНОГО КЕРУВАННЯ ДОСТУПОМ / Гуменюк В.В., Зубринська Д. Л., Крупельницький Л.В., Городецька О.С // Міжнародна науково-практична Інтернет-конференція «Молодь в науці: дослідження, проблеми, перспективи (МН2024)» (15 жовтня

2023 р.- 20 травня 2024 р., Вінниця) : Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/21172/17557

1 ОГЛЯД І АНАЛІЗ СИСТЕМ КОНТРОЛЮ ТА КЕРУВАННЯ ДОСТУПОМ І АВТОМАТИКОЮ ПРОПУСКУ

1.1 Типові системи контролю доступу

Термін "контроль доступу" описує будь-які процеси, пов'язані з регулюванням проходу відвідувачів у будь-яку зону або з неї. По суті, стандартний замок, який відкривається за допомогою металевого ключа, можна розглядати як просту форму "системи контролю доступу". Проте, надійність такої системи може викликати певні сумніви, і тому з роками системи контролю доступу стають все складнішими. На сьогоднішній день термін "система контролю та управління доступом" найчастіше асоціюється з комп'ютерною електронною системою контролю доступу. Електронна система контролю доступу використовує спеціальну "пластикову картку з чіпом" замість металевого ключа, щоб надати доступ у захищену зону.

Мета системи контролю доступу полягає в тому, щоб надати швидкий та зручний доступ для авторизованих осіб, в той час як надійно обмежуються доступ для сторонніх осіб.

Система контролю та управління доступом (СКУД) складається з програмного та апаратного забезпечення, призначеного для забезпечення порядку, контролю та реєстрації руху осіб на контрольованій території. Функції такої системи включають обмеження доступу сторонніх осіб на контрольовану площу та контроль руху відвідувачів відповідно до їх прав доступу. На рисунку 1.1 зображена типова система СКУД, де через числа пояснюється послідовність її функціонування [2].

1.2 Принципи функціонування і основні складові СКУД

Системи контролю та управління доступом, які використовують безконтактні пластикові картки для пропуску, спрямовані на підвищення рівня безпеки та забезпечення дисципліни на підприємстві. Автоматизований пункт

пропуску, що базується на турнікетах-штативах і безконтактних картках, суттєво підвищує контроль доступу до об'єкта.

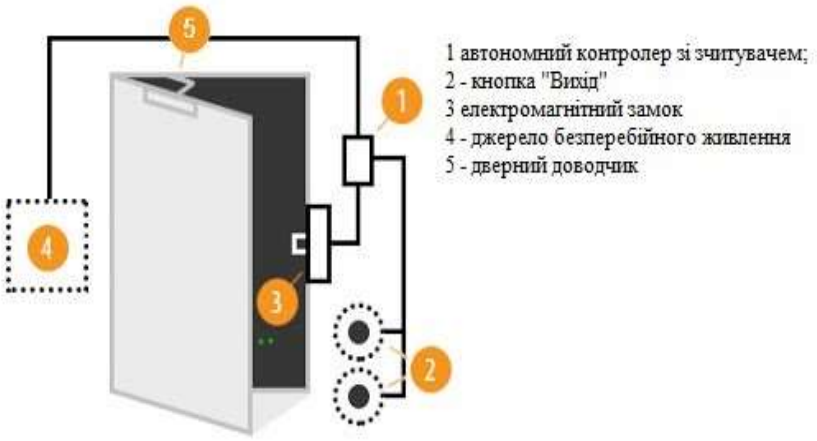


Рисунок 1.1 — Типова система контролю доступу

Система дозволяє вести облік працівників на території, ідентифікує їх за допомогою безконтактних електронних карток і фіксує час їх проходження. Крім того, вона моніторить події на точках доступу та повідомляє оператора про події тривоги, такі як злам замків або порушення режиму контролю доступу. Оператор може швидко управляти системними пристроями, блокуючи або відкриваючи замки дистанційно, наприклад, у випадку пожежі.

Системне програмне забезпечення дозволяє вести базу даних персоналу, включаючи ім'я, посаду, відділ, номер персоналу, режим роботи, фотографії, паспортні дані, інформацію про пропуск та права доступу. Крім того, воно підтримує використання безконтактних карток як ідентифікаторів (рис. 1.2).

Рисунок 1.2 — Пристрої для отримання доступу у приміщення

Системи контролю доступу можуть відрізнятися за типом та складністю. Проте більшість систем контролю доступу на базі карток мають щонайменше наступні основні компоненти [2].

Картка доступу. Картку доступу можна розглядати як електронний "ключ", який використовується особами для проникнення через двері, захищені системою контролю доступу. Кожна картка доступу має унікальне кодування. Більшість таких карток мають приблизно такий же розмір, як стандартна кредитна картка, і можуть легко поміщатися в гаманці або сумочці.

Картрідери (зчитувачі карток) — це пристрої, які використовуються для електронного "зчитування" інформації з карток доступу. Існують два типи зчитувачів: "вставні", які потребують вставки картки в пристрій, і "безконтактні", які зчитують інформацію з картки на невелику відстань, зазвичай від 3 до 6 см. Зчитувачі карток зазвичай розміщуються на зовнішній (неохороненій) стороні дверей, які вони контролюють.

Обладнання для електричних замків — це технічні засоби, які використовуються для електричного управління блокуванням та розблокуванням дверей, що контролюються системою контролю доступу. Це включає в себе різноманітні типи обладнання, такі як електричні замки, електромагнітні замки, електричні виходи та інші. Вибір конкретного типу та розташування такого обладнання для кожної двері залежить від конструкції дверей і їхніх функціональних вимог.

Серверний комп'ютер системи контролю доступу можна розглядати як головний центральний елемент системи, відповідальний за обробку та збереження всієї інформації. Цей комп'ютер виконує функції центральної бази даних та файлового менеджера, що забезпечує запис системної діяльності. Зазвичай використовується один серверний комп'ютер для управління багатьма дверима, які контролюються пристроями зчитування карток. Зазвичай для цієї ролі використовується звичайний комп'ютер, на якому встановлене спеціалізоване програмне забезпечення для системи контролю доступу.

Для дистанційного керування системою контролю та управління доступом є кілька можливих методів. По-перше, це встановлення програмного забезпечення "клієнтського" контролю доступу на інші комп'ютери компанії, які використовують мережу для зв'язку з сервером і виконання всіх системних функцій.

По-друге, багато систем дозволяють використовувати стандартний інтерфейс веб-браузера для підключення до сервера. Уповноважені користувачі можуть увійти в систему через будь-який комп'ютер за допомогою веб-браузера для виконання основних функцій.

Деякі системи контролю доступу пропонують мобільні додатки, які дозволяють керувати системою зі смартфона.

1.3 Керування доступом як послуга — ACaaS

Система контролю доступу запобігає несанкціонованому доступу та дозволяє керівництву компанії встановлювати обмеження на доступ персоналу до приміщень відповідно до їхніх ролей в організації. Цей принцип застосовується у всіх сферах діяльності, незалежно від того, чи йдеться про складські комплекси, банківські установи, автостоянки, гаражі, готелі, навчальні заклади чи бізнес-центри. Компоненти системи контролю доступу можуть включати турнікети, зчитувачі карток, відеодомофони та системи сигналізації [3-6].

За спостереженням розвитку цифрових технологій, підходи AcaaS виводять безпеку на новий рівень. AcaaS означає контроль доступу у формі послуги. Він використовує технологію "Програмне забезпечення як послугу" (SaaS) і, отже, є хмарним. Хоча обладнання для контролю доступу залишається на місці, програмне забезпечення та сервери видаляються з приміщень компанії і зберігаються в потужних віддалених центрах обробки даних. (рис.1.3).

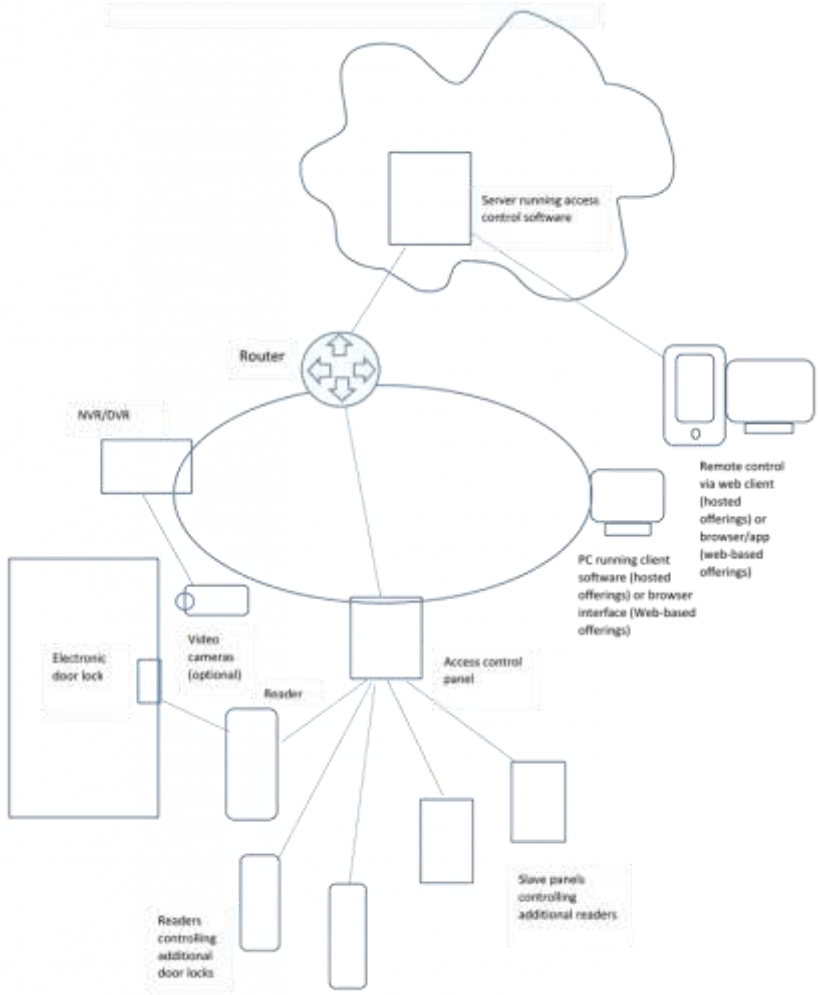


Рисунок 1.3 — Приклад інтегрованого контролю доступу як послуги

У порівнянні з традиційним контролем доступу, "контроль доступу як послуга" має ряд переваг:

1) оскільки вся інформація зберігається на віддалених серверах, немає необхідності встановлювати сервер в установі безпосередньо;

2) інформація, отримана з усіх об'єктів та всіх філій, зберігається в одному місці, і надається цілодобовий доступ до цієї інформації;

3) забезпечення доступності системи цілодобово підтримується технічним персоналом, малоймовірно, що який-небудь невеликий бізнес може похвалитися цілодобовою присутністю підтримки на місці в разі традиційного контролю доступу;

4) реалізація хмарної безпеки як послуги дозволяє змінювати конфігурацію контролю доступу за потреби, наприклад, можна додати більше

дверей або призначити власникам карток різні рівні доступу без необхідності заміни обладнання або придбання додаткового програмного забезпечення;

5) AcaaS використовує надійне шифрування, тому немає потреби хвилюватись про можливість злому системи контролю доступу;

6) деякі послуги AcaaS майже не потребують фізичного обладнання, співробітники можуть отримати доступ до певних приміщень, лише завантаживши мобільний додаток — це досягається за допомогою мобільних облікових даних, які відправляють сигнал контролеру дверей, дозволяючи співробітникам увійти в офіс лише там, де це дозволено;

7) контроль доступу як послуга дозволяє отримати і активувати комплексну безпеку у формі послуги — це означає, що можна інтегрувати систему сигналізації, відеоспостереження, виявлення вторгнень і інші компоненти безпеки.

Отже, СКУД — це система, що відстежує вхід і вихід в приміщення відвідувачів за допомогою ідентифікаторів. Основні компоненти системи включають загороджуючий пристрій (турнікет), ідентифікатор, зчитувач і контролер. В залежності від комплектуючих і функцій системи можна виділити три групи: автономні, мережеві і біометричні. Застосування комбінації цих трьох груп дозволяє підвищити рівень контролю доступу в приміщеннях систем безпеки.

1.4 Порівняння контролерів керування пропуском – аналогів комплексу, що розробляється

Один з аналогів засобів, що проєктуються - це універсальний IP контролер доступу NDC F18IP від компанії Forter (Україна), призначений для керування доступом у приміщення через двері у складі системи контролю та управління доступом, заснованої на мережі Ethernet. Пристрій підтримує автономний режим роботи — у разі відсутності зв'язку з сервером він продовжує виконувати завантаження у нього прав доступу. Ідентифікація доступу здійснюється за допомогою безконтактних карток, для роботи з якими контролер передбачає

підключення до 2 зчитувачів з інтерфейсом Wiegand. Основні характеристики контролера NDC F18IP наведені у табл. 1.1.

Таблиця 1.1 — Основні параметри контролера NDC F18IP

Параметр	Значення
Інтерфейс	Ethernet 100Mbit
Зчитувачі	2 порта Wiegand
Число підтримуваних ідентифікаторів	31 768 постійних і 1000 тимчасових карток відвідувачів
Записи в журналі подій	47000 записів
Зберігання в незалежній пам'яті	250 часових зон, 250 тижневих розкладів, 250 вихідних, підтримка плаваючих розкладів
Число входів	8, з контролем за струмом для підключення сенсорів, кнопок і т.д.
Число виходів управління зовнішніми пристроями	4 типу «сухий контакт»: два реле (C NO NC) 24В 5А, два реле (C NO) 24В 1А
Напруга живлення	12В
Мережеві налаштування	З використанням порта mini USB B вручну, або в процедурі автоконфігурації

Контролер NDC F18IP має свої переваги та недоліки. До переваг відносяться універсальність, підтримка різних типів зчитувачів карт, протоколу TCP/IP та висока кількість ідентифікаторів. Однак його недоліками є обмеженість у керуванні доступом лише за допомогою карт, що унеможливлює надання прав доступу дистанційно, та порівняно висока вартість, що становить близько 6,5 тис. гривень за один пункт пропуску.

Іншим аналогом є зчитувач-контролер SameKey Card Control від компанії SameKey. Цей пристрій призначений для використання в системах управління доступом, побудованих з використанням інтерфейсів Wi-Fi та

Ethernet. Доступ можна отримати за допомогою NFC-міток або мобільного додатка через Bluetooth. SameKey Card Control призначений для надання прав доступу, адміністрування доступу та відвідуваності в офісах, складських приміщеннях, бізнес-центрах та інших об'єктах з великою кількістю точок проходу. Пристрій працює через хмару, синхронізуючи дані в реальному часі. Контрольна панель зі статистикою також розташована у хмарі. Підключення до Інтернету здійснюється через мережний кабель Ethernet або бездротове з'єднання Wi-Fi [13].

Контролер SameKey, що входить до складу хмарної системи контролю доступу, має наступні особливості:

— підтримка підключення до Інтернету через Wi-Fi або Ethernet;

— можливість надання доступу різними способами: за допомогою NFC-міток, банківських карток, мобільного додатка через Bluetooth;

— наявність безкоштовних мобільних ідентифікаторів;

— підтримка підключення до електромагнітних і електромеханічних замків;

— адміністрування користувачів, пристроїв та прав доступу через веб-панель;

— синхронізація необмеженої кількості користувачів та пристроїв в одному акаунті;

— розмежування прав доступу:

— можливість надання гостьового доступу за посиланням з обмеженням за часом або кількістю використань:

— має пам'ять на 5 120 ключів і може зберігати до 16 384 події.

Основні параметри зчитувача-контролера SameKey представлені у табл. 1.2 [13].

Основними перевагами зчитувача-контролера SameKey є підтримка підключення до Інтернету через Wi-Fi або Ethernet, зручне масштабування для об'єктів з великою кількістю точок проходу і можливість організації дистанційного управління доступом.

З іншого боку, серед недоліків можна відзначити наявність лише

одного каналу керування навантаженням та неможливість реалізації зворотного зв'язку з виконавчими пристроями.

Таблиця 1.2 — Основні параметри контролера SameKey

Параметр	Значення
Тип	Автономний
Інтерфейс	Ethernet, Bluetooth, Wi-Fi
Призначення	Управління електричними замками
Ідентифікація	Картка NFC
Вбудована пам'ять карток	5 120
Вбудована пам'ять подій	16 384
Напруга живлення	Від 5В до 24 В
Діапазон температур	від мінус 20°С до + 70°С

Найбільш схожим до розглядуваних засобів є комплекс мобільного керування автоматикою пропуску LOKKYY [14], який призначений для використання з різноманітними автоматизованими системами контролю доступу і пропуску транспортних засобів та людей, такими як ворота, шлагбауми, ролети, тощо.

Комплекс LOKKYY застосовується на різних типах об'єктів, включаючи побутові, громадські, офісні, промислові, транспортні, телекомунікаційні, банківські, освітні та медичні, для контролю та обмеження пропуску на їх територію. Керування здійснюється через мережі Інтернет, Bluetooth та Wi-Fi за допомогою мобільного додатка LOKKYY APP, який встановлюється на смартфони користувачів. Це забезпечує: відсутність необхідності в апаратних ключах; відсутність додаткового апаратного сервера для централізованого керування; простоту надання як довготривалого, так і короткотермінованого доступу; оперативність у зміні ключів; розширену функціональність віддаленого керування й моніторингу. Основні параметрів комплексу LOKKYY наведені в таблиці 1.3 [14].

Таблиця 1.3 — Основні параметри комплекса LOKKYY

Параметр	Значення
Інтерфейс керування	Автономний
Інтерфейси підключення	Bluetooth SIG version 5.0, Wi-Fi 802.11 b/g
Число вихідних ліній керування навантаженням	4 (2 канали)
Виходи	Гальванічно розв’язані нормально розімкнені контакти реле
Максимальна комутована напруга навантаження	60 В
Максимальний струм комутації	1 А
Тип сенсорів контролю	Магнітні герконові, нормально розімкнені
Номінальна напруга живлення	24 В постійного або змінного струму частотою 50 Гц
Максимальний струм споживання	200 мА
Максимальна споживана потужність	6 Вт
Час спрацювання від подачі команди зі смартфона до перемикання реле	Від 0,1 с до 10 с

Комплекс LOKKYY дозволяє керувати через Інтернет, Bluetooth та Wi-Fi, не потребує апаратних ключів чи сервера, простий у використанні та зміні ключів. Але для його роботи потрібне стійке підключення до Інтернету.

З аналізу аналогів випливає, що розроблювані засоби мають підтримувати підключення через Bluetooth та Wi-Fi, мати не менше двох каналів керування навантаженням, а також підтримувати можливість зворотного зв'язку з виконавчими елементами.

2 ВИБІР ТЕХНОЛОГІЙ, МЕТОДІВ І ЗАСОБІВ ДЛЯ РОЗРОБКИ АПАРАТНОЇ ЧАСТИНИ КОМПЛЕКСУ

2.1 Технології ідентифікації

Системи управління доступом вирішують ряд завдань, однією з яких є ідентифікація відвідувачів за допомогою ідентифікаційних ознак. Ідентифікаційна ознака - це властивість, що характеризує суб'єкта доступу. Ідентифікатор - це унікальний набір значень ідентифікаційних ознак, який використовується для ідентифікації. Процедура ідентифікації полягає у порівнянні ідентифікатора, який пред'являється користувачем, з вмістом бази даних. Для цього створюється база даних образів ідентифікаторів.

При наданні доступу в сучасних системах управління доступом використовуються різні технології ідентифікації. Найбільш поширеними серед них є радіочастотна, мобільна та біометрична ідентифікація [4].

Радіочастотна ідентифікація (RFID) використовує безконтактні RFID картки, такі як EM-Marin та Mifare, для забезпечення доступу. Ці картки можуть бути зчитані на відстані від 5 до 90 см, навіть якщо зчитувач розташований за антивандальною неметалевою перегородкою. Це означає, що доступ до системи можна отримати швидко, не обмежуючи точного положення карти в просторі. Крім того, RFID-карти можуть працювати в агресивних середовищах, забезпечуючи ідентифікацію на значній відстані та маючи довгий термін служби.

Картки EM-Marin є Proximity-картками, які працюють на частоті 125 кГц і призначені лише для читання. Ці картки фактично є дистанційними електронними пропусками з вбудованим мікрочіпом, який має унікальний ідентифікаційний код. Вони широко використовуються в системах контролю як фізичного, так і логічного доступу під час безконтактної радіочастотної ідентифікації. Ці картки отримали значне поширення завдяки своїй зручності використання та відносно невеликій вартості.

Обмін інформацією між Proximity карткою та зчитувачем відбувається за відкритим протоколом, що робить їх вразливими для зловмисників. Крім того,

ці картки не захищені від копіювання, що може порушити безпеку системи доступу. Для уникнення несанкціонованого доступу через копію ідентифікатора часто використовуються додаткові засоби захисту, такі як введення PIN-коду в поєднанні з карткою, підтвердження доступу, використання двох карток тощо. Такі заходи дозволяють підвищити рівень безпеки системи доступу [4, 5].

Безконтактні високочастотні RIFD-картки, які працюють на частоті 13,56 МГц, є більш захищеними від копіювання порівняно з Proximity картками. Серед таких карток найбільше поширення отримали smart-картки у форматах Mifare та iCLASS. Протягом останніх кількох років їх вартість значно знизилася і вже майже дорівнює вартості карток у форматі EM-Marine. Такі карти надають більший рівень безпеки і забезпечують захист від копіювання, що робить їх привабливими для використання у системах контролю доступу.

Безконтактні високочастотні RIFD-картки, які працюють на частоті 13,56 МГц, дійсно дозволяють забезпечити більший рівень безпеки та швидкодії. Це зумовлено їхньою ширшою смугою пропускання, яка дозволяє ефективно передавати дані. Крім того, такі карти дозволяють використовувати різноманітні захисні механізми, такі як взаємна автентифікація між карткою та зчитувачем, а також алгоритми шифрування даних, що підвищує рівень безпеки в системах контролю доступу.

Високочастотні RIFD-картки мають значну перевагу завдяки наявності світового стандарту ISO14443. У порівнянні з низькочастотними картками доступу, які не підлягають стандартизації, це забезпечує їхню сумісність і взаємодію з різними пристроями та системами, що полегшує їх впровадження та ефективне використання в різних середовищах [4].

Чіпи високочастотних RIFD-карток, крім унікального серійного номера (UID), також мають пам'ять для багаторазового запису та читання. Доступ до цієї пам'яті захищений ключами, що практично унеможливлює копіювання таких карток або несанкціоноване зчитування інформації з них. Серійний номер чіпа завжди доступний для читання, його не можна змінити або приховати.

Тому для забезпечення високого рівня захисту від несанкціонованого доступу краще використовувати інформацію, що записана у пам'ять картки [5].

Використання вбудованої пам'яті в smart-картках та зростаюча її місткість дозволяють зберігати на них не лише ідентифікаційні ознаки, а й іншу корисну інформацію. За рахунок збільшення сумарного об'єму ідентифікаційної інформації повністю уникнута можливість збігу інформації в різних картах. Це суттєво розширює функціонал системи та сприяє зниженню вартості стаціонарного обладнання для системи контролю та управління доступом.

Для зчитування захищеної інформації унікальний ключ доступу до даних зберігається в самому зчитувачі. Це може здійснюється за допомогою двостороннього обміну інформацією між контролером і зчитувачем, або через запис ключів доступу до даних за допомогою спеціально підготовленої майстер-картки при її пред'явленні до зчитувача. Перше рішення є більш зручним, але потребує використання спеціальних зчитувачів і контролерів. Друге рішення дозволяє використовувати стандартні контролери з інтерфейсом Wiegand, але ускладнює настройку та модифікацію параметрів системи. При розподілі функціоналу між карткою і стаціонарним обладнанням найбільш перспективними є системи зі збереженням на карті ідентифікаційних ознак та централізованим зберіганням прав доступу і персональних даних користувачів [6].

Ультрависокочастотні картки доступу (Ultra High Frequency, UHF) працюють на частоті від 860 до 960 МГц і відрізняються значним збільшенням відстані зчитування. Зазвичай технології UHF використовуються для віддаленого зчитування RIFD-міток під час проїзду автотранспорту. Крім того, ультрависокочастотні картки доступу можуть бути використані в мультитехнологічних рішеннях для організації в'їзду на територію та входу до будівлі за допомогою однієї картки.

Мобільна ідентифікація використовує смартфон для отримання прав доступу і стає все більш популярною завдяки широкій поширеності смартфонів, їх універсальності та багатофункціональності. Використання смартфонів як ідентифікаторів усуває ризики клонування, втрати або передачі ідентифікатора

іншим особам. Це також уникне потреби у придбанні та персоналізації карт доступу, а впровадження здійснюється з мінімальними часовими витратами. На відміну від безконтактних карток, смартфони підтримують багатофакторну автентифікацію, біометричну ідентифікацію та інші функції безпеки [7, 8].

Для мобільного доступу за допомогою смартфона в основному використовуються дві технології: NFC (Near Field Communication) — для близької ідентифікації, та BLE (Bluetooth Low Energy) - для забезпечення низького енергоспоживання Bluetooth [8].

NFC є відносно новою стандартизованою технологією бездротового зв'язку малої дистанції дії, що є одним з найбільш популярних сучасних трендів у галузі використання мобільних пристроїв як ідентифікаторів. Серед основних особливостей цієї технології слід зазначити безконтактну передачу даних, можливість обміну інформацією з іншими пристроями або пасивними мітками, низьку вартість рішення та мале енергоспоживання. [8, 9].

Bluetooth Low Energy (BLE) є специфікацією популярної бездротової технології Bluetooth, а його найбільш важливими перевагами при використанні в системах управління доступом є надмале енергоспоживання, відсутність необхідності у попередньому сполученні пристроїв та використання алгоритму шифрування даних AES з ключем розміром 128 біт [8].

Ідентифікація за біометричними ознаками використовує різноманітні фізіологічні або поведінкові характеристики людини. Ці ознаки можуть бути як відкриті, такі як обличчя, долоні, відбитки пальців, рогівка ока, так і приховані, такі як розташування вен долоні, голос, унікальність будови внутрішніх органів, тощо [10].

Біометрична ідентифікація часто називається чистою або реальною через використання фактичної біометричної ознаки (ідентифікатора), пов'язаної з конкретною людиною. Одним із специфічних аспектів цього виду ідентифікації є необхідність великої бази даних біометричних зразків: кожен з цих зразків має бути порівняний з усіма записами в базі даних (порівняння 1: N або "один до багатьох"). Для ефективного використання у реальних умовах така система вимагає високої швидкості порівняння біометричних ознак [10].

В цілому, біометричні системи ідентифікації можна поділити на статичні та динамічні. При статичній ідентифікації використовуються фізіологічні характеристики:

— відбитки пальців або рисунок папілярних ліній;

— райдужна оболонка ока;

— сітківка ока;

— рисунок вен;

— лице;

— геометрія руки;

— ритм серцебиття;

— ДНК.

Динамічна ідентифікація можлива за поведінковими характеристиками людини, такими як:

— почерк чи динаміка підпису;

— серцевий ритм;

— голос та ритм мови;

— розпізнавання жестів

— особливості роботи на клавіатурі комп'ютера (або набору коду на панелі);

— особливості ходи [10, 11].

Біометрична ідентифікація має низку переваг, включаючи високий рівень надійності та точності у розпізнаванні, а також відсутність можливості передачі ідентифікаторів іншим особам. Системи розпізнавання обличчя здобувають все більше популярності як найбільш зручний і швидкий спосіб безконтактної ідентифікації. Проте їх використання обмежене через високу вартість, обмежену оперативність та значний обсяг машинної пам'яті, необхідний для їхньої ефективної роботи. Тому вони застосовуються переважно в установах з підвищеною секретністю [10].

Біометрична ідентифікація має низку переваг, включаючи високий рівень надійності та точності у розпізнаванні, а також відсутність можливості передачі ідентифікаторів іншим особам. Системи розпізнавання обличчя здобувають все

більше популярності як найбільш зручний і швидкий спосіб безконтактної ідентифікації. Проте їх використання обмежене через високу вартість, обмежену оперативність та значний обсяг машинної пам'яті, необхідний для їхньої ефективної роботи. Тому вони застосовуються переважно в установах з підвищеною секретністю [11].

З проведеного аналізу випливає, що з точки зору перспектив та більш широких можливостей використання найбільш привабливою є технологія мобільної ідентифікації. По-перше, вона базується на віртуальних ідентифікаторах, які є або безкоштовними, або майже безкоштовними у порівнянні з картками. По-друге, на одному смартфоні можна зберігати кілька ідентифікаторів. По-третє, вона забезпечує високий рівень захисту ідентифікаторів від несанкціонованого використання, оскільки смартфони підтримують різноманітні методи аутентифікації, що дозволяють визначати достовірність користувача за ідентифікаційними ознаками. Нарешті, лише мобільна ідентифікація дозволяє здійснювати дистанційне керування правами доступу через віддалене надання/відкликання ідентифікатора.

2.2 Технології мобільної ідентифікації NFC та BLE

Для досягнення максимальної автономності системи віддаленого керування доступом можна розглянути передачу ідентифікатора від мобільного пристрою до контролера керування доступом через NFC або Bluetooth. Для визначення оптимального вибору між цими двома технологіями, потрібно провести їх порівняльний аналіз.

Технологія обміну даними NFC, подібно до технології RIFD, ґрунтується на використанні індуктивного зв'язку між електронними пристроями, які перебувають у безпосередній близькості. Сьогодні NFC набула широкого поширення через популярність мобільних платежів та інших додатків. Головною особливістю NFC є простота використання та дуже малий час встановлення з'єднання [9], [19].

Технологія NFC використовує частоту 13,56 МГц та забезпечує передачу даних зі швидкістю до 424 кбіт/с на відстані приблизно до 10 сантиметрів. На

відміну від звичайних безконтактних технологій у даному частотному діапазоні, що дозволяють здійснювати тільки активно-пасивний зв'язок, обмін даними між NFC-пристроями може бути як активно-активним (одноранговим), так і активно-пасивним, тому в стандарті NFC простежуються тісний зв'язок з радіочастотною ідентифікацією RFID.

В технології NFC підтримуються три основні режими роботи пристроїв. Перший, найпоширеніший, - пасивний режим емуляції RFID картки, в якому NFC-пристрій працює як безконтактна картка. Цей режим використовується при здійсненні безконтактних банківських платежів.

Другий режим, який називають режимом peer-to-peer, є одноранговим і використовується для організації обміну інформацією між двома NFC-пристроями, кожний з яких працює в активному режимі.

Третій режим — це режим читання або запису, в якому NFC-пристрій є активним та обмінюється даними з пасивною RFID сумісною міткою [19].

Однією з ключових перешкод перед впровадженням мобільної ідентифікації за допомогою NFC для керування доступом є проблеми, що виникають при використанні мобільних пристроїв на базі операційної системи iOS. Це пояснюється тим, що доступ до NFC на пристроях від Apple для розробників сторонніх додатків був довго обмежений, і NFC використовувався головним чином лише для проведення безконтактних платежів через Apple Pay. Навіть на сьогоднішній день, починаючи з версії iOS 11, функціонал NFC доступний лише для читання, що ускладнює повноцінну взаємодію між мобільним додатком та зчитувачем для управління доступом [19].

Серед основних переваг технології NFC можна виділити низьке споживання енергії, швидке встановлення з'єднання, можливість з'єднання з об'єктами без електроживлення, простоту взаємодії з пристроями, відповідність промисловим стандартам та можливість взаємодії з існуючими безконтактними технологіями. Мінімальний радіус дії допомагає знизити потребу в захисті від несанкціонованого доступу до даних. Це робить технологію NFC потенційно важливою для сфери безпеки, де вона може

замінити більшість існуючих безконтактних технологій, таких як електронна ідентифікація особистості, контроль доступу до об'єктів та захист доступу до електронних пристроїв.

Технологія Bluetooth Low Energy (BLE) є економічною та раціональною альтернативою стандартній технології передачі даних Bluetooth із виходом специфікації Bluetooth 4.0. Вона широко використовується там, де потрібне низьке споживання енергії або при передачі обмежених обсягів даних з великими інтервалами між передачами. Інтеграція BLE в особисті електронні пристрої, яка підтримується більшістю виробників смартфонів та комп'ютерів, робить її привабливим вибором для недорогих та енергоефективних застосунків Інтернету речей. Стандарт передбачає швидкість передачі даних до 1 Мбіт/с при розмірі пакета даних від 8 до 27 байт. Дальність зв'язку може досягати до 300 м при потужності передавача 10 дБм [20].

Так само, як і в класичному Bluetooth, в технології BLE використовується ISM-діапазон (Industrial, Scientific, and Medical) від 2,4 ГГц до 2,4835 ГГц, і при встановленні з'єднання один з пристроїв виступає у ролі ведучого (master), а інший — у ролі веденого (slave). Один ведучий пристрій може підтримувати з'єднання з кількома веденими, тоді як ведений пристрій може мати лише одне підключення до ведучого. Це відрізняє BLE від класичного Bluetooth, де ведений пристрій міг також виступати в якості ведучого для інших пристроїв [20].

Для економії енергії ведений пристрій в стандарті BLE за замовчуванням перебуває в сплячому режимі, і періодично прокидається для перевірки наявності пакетів даних від ведучого. Ведучий пристрій визначає моменти часу, коли кожен з ведених пристроїв прокидається, регулюючи доступ пристроїв до каналу передачі за схемою поділу часу. Цей підхід дозволяє значно знизити активну споживану потужність в BLE у порівнянні з Bluetooth — до десяти разів.

У стандарті BLE, подібно до Bluetooth, використовується технологія адаптивної стрибкоподібної перебудови частоти (AFH). Сигнальна несуча

частота змінюється стрибкоподібно 1600 разів протягом однієї секунди між 40 частотними каналами шириною 2 МГц. Послідовність перемикання між цими частотними каналами відома лише ведучому та веденим пристроям, що забезпечує високу інтерференційну стійкість. Тому паралельно працюючі пристрої в одному просторі не заважають один одному. Цей підхід гарантує надійну передачу даних в умовах зашумленого ефіру [20].

Існують два основних типи каналів в стандарті BLE: канали оголошення та канали даних. Канали оголошення використовуються для виявлення пристроїв, установлення з'єднання та відправлення повідомлень широкого спектра. Кожен із каналів оголошення відповідає одній з трьох частотних хвиль, тоді як решта 37 каналів призначені для передачі даних між пристроями.

Порівнюючи технології NFC та BLE, важливо відзначити, що NFC має меншу швидкість передачі даних, але швидко встановлює з'єднання та має обмежений радіус дії. Цей обмежений радіус можна розглядати як недолік чи перевагу, з одного боку, він гарантує високий рівень безпеки, оскільки унеможливлює перехоплення даних на великій відстані. З іншого боку, NFC є сумісним з технологією RFID і може працювати, коли один з пристроїв не має живлення або вимкнений, що робить її вигідною у певних сценаріях, відмінно від Bluetooth.

Також важливо відзначити, що NFC не має чітких практичних сценаріїв використання або стандартних рішень. У відміну від Bluetooth, якого профілі чітко описують, як передати файли, підключити гарнітуру чи забезпечити мережний доступ, NFC є лише базою. Його безпосереднє використання залежить від додаткового програмного забезпечення, що працює через NFC. Це відкриває широкі можливості для розробників, але також може створити проблеми при забезпеченні взаємодії різних додатків та пристроїв.

Тому, через те, що технологія бездротового зв′язку Bluetooth підтримується як в пристроях, що використовують Android, так і в тих, що працюють на базі iOS, для передачі ідентифікатора від мобільного пристрою та контролера доступу доцільно використовувати Bluetooth.

2.3 Структурна схема та принцип дії комплексу керування пропуском

Наведемо структурну схема комплекса керування пропуском LOKKYY, що розробляється, пояснює під'єднання та взаємодію складових частин для одного керованого електроприводу, наведена на рис. 2.1

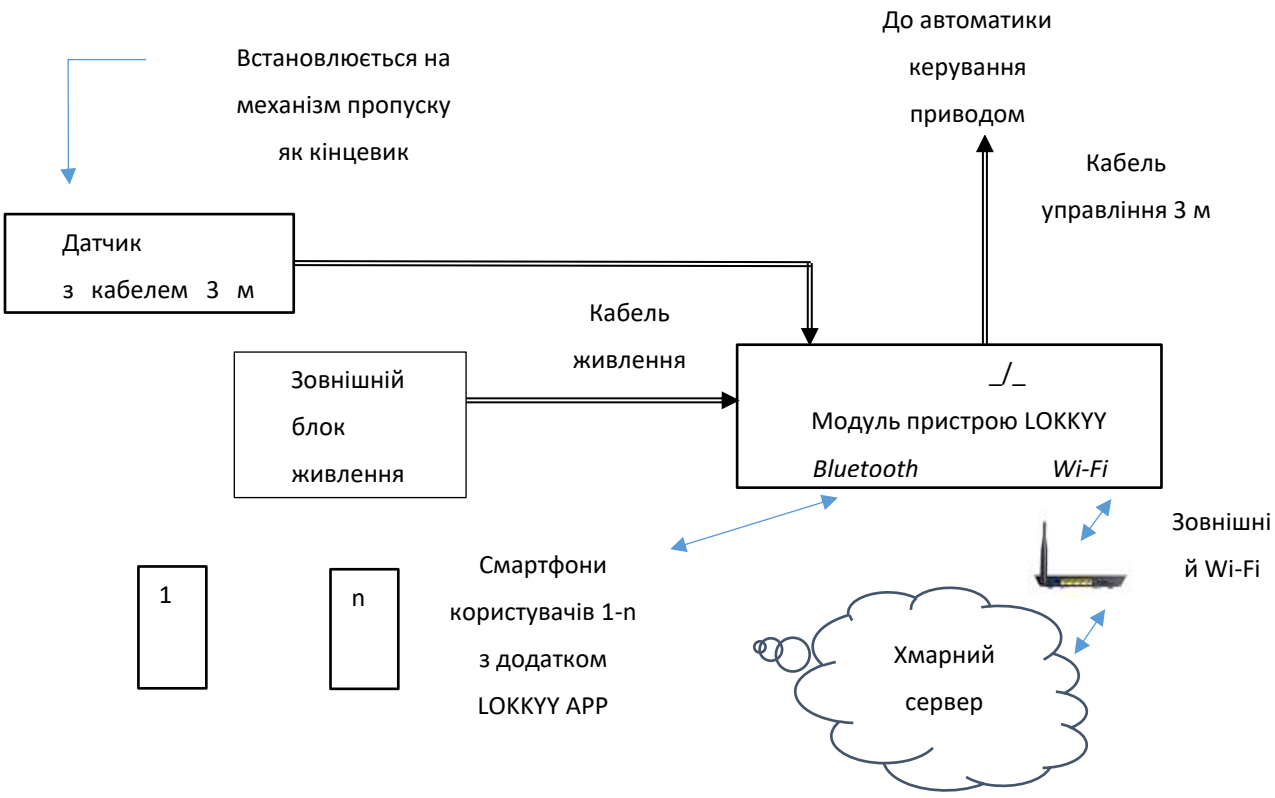


Рисунок 2.1 — Структурна схема комплекса LOKKYY

Пристрій LOKKYY працює за сигналом магнітного датчика, який визначає поточний стан керованого об'єкту пропуску – відкритий або закритий. За допомогою вбудованого реле він може керувати автоматикою приводу. Користувачі з додатком LOKKYY APP на своїх смартфонах можуть отримувати інформацію від пристрою LOKKYY через Інтернет та хмарний сервер, а також контролювати поточний стан і керувати пропуском.

Налаштування пристрою LOKKYY виконується через смартфон адміністратора за допомогою бездротової мережі Bluetooth. Доступ пристрою LOKKYY до Інтернету забезпечується через бездротову мережу Wi-Fi, яка присутня на об'єкті пропуску. У випадку відсутності доступу до Інтернету

зв'язок між смартфонами і пристроєм LOKKYY здійснюється за допомогою інтерфейсу Bluetooth.

3 РОЗРОБКА АПАРАТНИХ СКЛАДОВИХ КОМПЛЕКСУ

3.1 Аналіз можливої реалізації структурних блоків та вибір елементної бази

Основним елементом контролера керування доступом є мікроконтролер. На ринку існує широкий вибір моделей з різними архітектурами і від різних виробників. Найпопулярнішими серед них є RISC мікроконтролери з Гарвардською архітектурою. До недавнього часу найпоширенішими і доступнішими були два сімейства 8-бітних мікроконтролерів: AVR та PIC. Проте наразі все більшою популярністю користуються 32-бітні ARM мікроконтролери на основі ядра Cortex-M3. Зараз їх ціна настільки знизилася, що вони можуть конкурувати за цим показником з 8- та 16-бітними мікроконтролерами. При цьому ARM мікроконтролери відрізняються значною продуктивністю і розширеними функціональними можливостями..

Мікроконтролерне ядро ARM (Advanced RISC Machines) було розроблено британською компанією ARM Limited, що спеціалізується на створенні архітектури та засобів розробки, таких як компілятори та інтегровані середовища розробки (IDE), і не має власних виробничих потужностей для виготовлення мікроконтролерів. Тому вона продає ліцензії на свої технології іншим компаніям. Більш як 60 виробників напівпровідникової продукції є клієнтами ARM Limited, серед яких визначені гравці, такі як Altera, Analog Devices, Atmel, Cirrus Logic, Fujitsu, Intel, Motorola, National Semiconductor, Philips, ST Microelectronics та Texas Instruments [31].

Ядро Cortex-M3 від ARM вирізняється кількома особливостями, що роблять його привабливим для використання в мікроконтролера [32]:

— повністю 32-бітна архітектура: всі регістри 32-бітові, арифметичні операції є 32-бітними; операція множення виконується за один такт, ділення за 2-12 тактів;

— велика кількість (від 16) регістрів загального призначення, що характерно RISC-архітектури;

— хороша підтримка режимів енергозбереження; у режимі сну може перебувати як весь мікроконтролер, так і окремі системи;

— 24-бітний таймер SysTick, що має можливість задавати широкий інтервал спрацьовування для організації кінцевих автоматів і планувальника RTOS;

— повноцінна реалізація JTAG або SWD, що дає можливість встановлювати точки зупинки (breakpoints), контролювати вміст змінних та регістрів, виконувати програму покроково;

— контролер переривань NVIC з підтримкою до 240 переривань та до 256 пріоритетів;

— контролер прямого доступу до пам′яті DMA дозволяє периферії обмінюватися даними з оперативною пам′яттю без участі ядра;

— орієнтованість набору інструкцій на компілятори С, що забезпечує більш ефективну оптимізації коду компіляторами С, отже збільшує швидкодію.

Сімейство STM32 від компанії ST Microelectronics є одним з найпопулярніших серед ARM мікроконтролерів на ядрі Cortex-M3. Однією з ключових причин його світової популярності є максимальний комфорт для розробників. Універсальність ядра Cortex-M3 дозволяє змінювати виробника з мінімальними витратами на програмний код. Однак, ще більшою перевагою є "pin-to-pin сумісність" всередині сімейства STM32. Це означає, що незалежно від об'єму флеш-пам'яті, ОЗП або периферії, для одного розміру корпусу всі сигнали зберігаються на тих самих входах/виводах для різних варіантів мікроконтролерів сімейства. Це значно спрощує розробку, оскільки розробники можуть легко змінювати конфігурацію мікроконтролера без необхідності вносити зміни до друкованої плати.

Крім того, STM32 мають розгалужену периферію [32]:

— декілька швидкісних 12-бітних АЦП;

— двоканальний ЦАП, який має 8-ми або 12-бітнні режими роботи;

— 12-канальний контролер DMA, який обслуговує до 12 запитів, має 4 рівні пріоритетів, незалежні розміри блоків для прийому та передачі даних (8, 16 та 32 біти), підтримує кільцевий буфер, пересилання даних у режимах пам'ять-пам'ять, пам'ять-периферія, периферія-пам'ять та периферія-периферія;

— декілька 16-бітних таймерів з довільними дільниками з різноманітними режимами роботи;

— модуль RTC (Real-Time Clock) - годинник реального часу з функцією лічильника та будильника;

— декілька Watchdog-таймерів для збільшення надійності;

— FSMC — Flexible Static Memory Controller, який забезпечує прозорий доступ до декількох видів пам'яті: SRAM, ROM, NOR Flash, NAND Flash, PSRAM та 16-бітових PC Card- пристроїв;

— SDIO — Secure Digital I/O interface для читання/запису на карти MMC та SD, який надає можливість забезпечити підтримку FAT та повноцінно працювати з файлами на вказаних картках;

— контролер інтерфейсу USB, який забезпечує повну підтримку стандарту USB 2.0 Full-Speed, до 8 кінцевих точок та режим USB OTG (On-The-Go) для безпосереднього зв'язування USB-пристроїв;

— контролер Ethernet з підтримкою MAC-рівня та швидкості 10/100 Мбіт/с;

— шина I2S — шина для цифрових аудіо пристроїв;

— UART, SPI, I2C, CAN.

Ще одним фактором, що сприяє популяризації STM32, є наявність різноманітних інструментів розробки, як платних, так і безкоштовних. Крім того, великий вибір безкоштовних бібліотек із документацією сприяє ефективному використанню цих мікроконтролерів у різних проектах. Це робить STM32 зручним вибором для розробників, які шукають надійні та ефективні інструменти для реалізації своїх проектів [32].

Розглянувши вищезазначене, для нашого контролера керування доступом ми обираємо мікроконтролер з серії STM32 (рис. 3.1), який має вбудований контролер Ethernet. Наш пріоритет — готові модулі, які дозволять зменшити кількість компонентів та спростити фізичну реалізацію. Під час вибору оптимального варіанту ми керуватимемося габаритними розмірами та вартістю, щоб забезпечити ефективність та економічність нашого проекту.

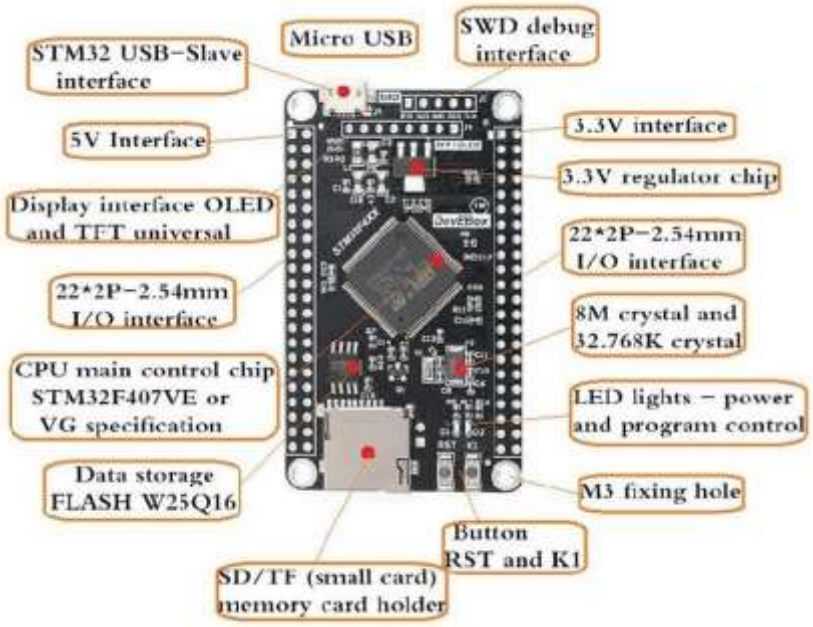


Рисунок 3.1 — Модуль STM32F407VET6-Mini

Отже, за вищезазначеними критеріями ми обираємо модуль STM32F407VET6-Mini, який ґрунтується на високопродуктивному мікроконтролері STM32F407VET6.

Модуль STM32F407VET6-Mini пропонує ряд переваг та функціональних можливостей. Робоча частота ядра становить 168 МГц, забезпечуючи високу продуктивність. Наявність додаткової FLASH пам'яті на 16Mbit дозволяє зберігати великі обсяги даних та програм.

Модуль також має роз'єм для підключення бездротового модуля зв'язку NRF24L01, що розширює можливості бездротового зв'язку. Наявність TFT LCD дисплея з FSMC інтерфейсом та підтримка SD карт

роблять його ідеальним для застосувань, що вимагають відображення графіки та роботи з файловою системою

Додатково, модуль має батарейний відсік для годинника реального часу, що забезпечує постійний доступ до часу та дати. Такі особливості роблять його відмінним вибором для проектів, що вимагають високої продуктивності, розширених можливостей зберігання та обробки даних, а також бездротового та графічного інтерфейсу (табл.3.1) [33].

Таблиця 3.1 — Параметри модуля STM32F407VET6-Mini

Параметр	Значення
Мікроконтролер	STM32F407VET6, ядро ARM Cotrex M4
Максимальна частота	168 МГц
Об'єм пам'яті програм (FLASH)	512 кБайт
Об'єм пам'яті даних (RAM)	192 кБайт
Зовнішня пам'ять	W25Q16/16Мбіт
Кварцові резонатори	HSE - 8МГц і RTC - 32.768Гц
Контролер DMA	16-потоковий з FIFO та пакетною підтримкою
Кількість доступних виводів	96 шт.
Таймери загального призначення	12 шт., 16 біт 2 шт., 32 біт
Розширений таймер з ШІМ керуванням двигунами	1 шт.
Генератор випадкових чисел	1 шт.
Системний таймер	1 шт.
Сторожові таймери	2 шт.
АЦП	3 шт., 12 біт
АЦП	2 шт., 12 біт
UART	4 шт.
SPI	3 шт.
I2S	3 шт.
I2C	2 шт.

FSMC	1 шт.
SDIO	1 шт.
CAN	2 шт.
USB	2 шт.
Ethernet	1 шт., 10/100 Мбіт/с
Роз'єм 32-pin підключення TFT LCD дисплея з інтерфейсом FSMC	1 шт.
Роз'єм 8-pin підключення бездротового модуля зв'язку NRF24L01	1 шт.
Роз'єм SD картки	1 шт.
JTAG/SWD debug	1 шт.
Модуль RTC з низьким енергоспоживанням	1 шт.
Кнопки користувача	3 шт.
DC-DC перетворювач	5В в 3.3В
Напруга живлення мікроконтролера	3,3 В
Напруга живлення плати	5 В
Розміри плати модуля	72 мм × 85 мм

На рис. 3.2 приведена схема з призначенням контактів модуля STM32F407VET6-Mini. Підключення контролера керування доступом до мережі Ethernet здійснюватиметься за допомогою вбудованого в мікроконтролер STM32F407VET6 Ethernet-модуля. Цей модуль відповідає стандарту IEEE802.3 і забезпечує передачу даних зі швидкостями 10 і 100 Мбіт/с через стандартний інтерфейс MII або скорочений інтерфейс RMII.

Важливо відзначити, що цей модуль також підтримує протокол IEEE1588 на апаратному рівні, що робить його ідеальним для застосувань, де важлива синхронізація часу. Крім того, він підтримує такі функції, як VLAN (віртуальна локальна мережа) і режими Half-duplex і Full-duplex на підрівні управління доступом до середовища (підрівень MAC). Ці

можливості дозволять забезпечити надійне та швидке з'єднання з локальною мережею Ethernet для контролера доступу [34].

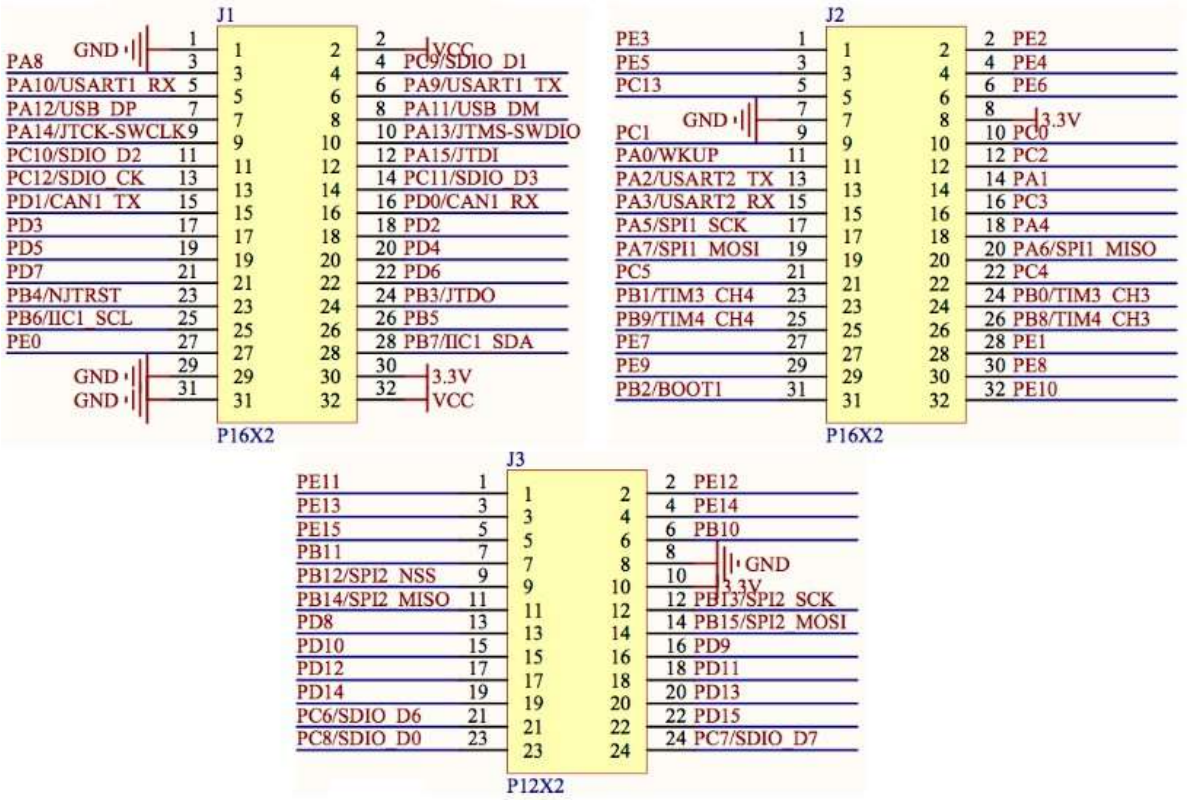


Рисунок 3.2 — Призначення контактів на роз′ємах модуля STM32F407VET6-Mini

Для полегшення розробки Ethernet-додатків, STMicroelectronics рекомендує використовувати lwIP TCP/IP- та NicheLiteTM TCP/IP-стеки, які дозволяють швидко та ефективно інтегрувати мережеві функції у додатки.

Для підключення до фізичної шини LAN мікроконтролер STM32F407xx вимагає зовнішнього фізичного інтерфейсного пристрою - трансивера фізичного рівня (PHY). Цей трансивер відповідає за кодування даних, переданих від Ethernet-модуля, для їх подальшої передачі у транспортне середовище, а також за синхронізацію переданих даних та їх прийом і декодування.

Підключення трансивера до мікроконтролера може бути здійснене через інтерфейси SMII, MII або RMII. Інтерфейс SMII створює службовий

канал, який використовується для доступу до регістрів управління або статусу трансивера.

Він використовує лише два сигнали:

— MDIO — послідовний двонаправлений канал даних для зв'язку з регістрами трансивера;

— MDC — послідовний тактовий сигнал каналу даних MDIO.

Інтерфейс MII (рис. 3.3), забезпечує взаємодію між підрівнем MAC, яке підтримується Ethernet-модулем та трансивером на швидкостях передачі даних 10 Мбіт/с або 100 Мбіт/с. Усі операції інтерфейсу MII виконуються в синхронному режимі [34].

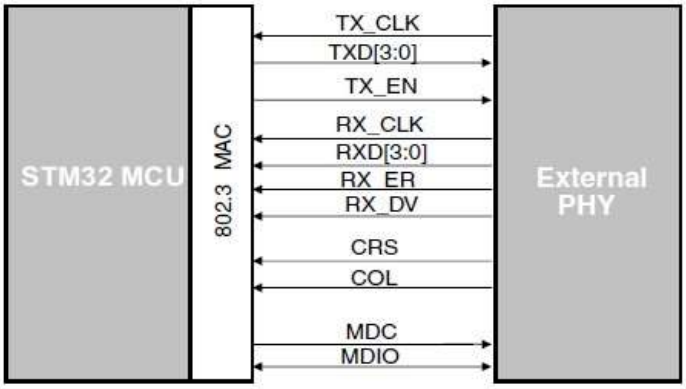


Рисунок 3.3 — Підключення трансивера за допомогою інтерфейсу MII

Канал передавання даних MII містить такі сигнали:

— MII_TXD (3..0) — група паралельних сигналів даних, що надходять в трансивер з MAC;

— MII_TX_CLK — тактовий сигнал передавання даних; який створюється трансивером і передається в MAC — 2,5 МГц для операцій 10 Мбіт/с, 25 МГц для операцій 100 Мбіт/с;

— MII_TX_EN — дозвіл на передавання; MAC встановлює цей сигнал, якщо встановлено достовірність даних для передавання;

— MII_CRS — опитування несівної; при напівдуплексних операціях трансивер генерує цей сигнал, якщо передає або приймає пакети даних; при дуплексних операціях CRS встановлюється при прийманні;

— MII_COL — детектування колізії; генерується трансивером, якщо виявлено колізію на лінії, є асинхронним і неактивним при дуплексних операціях;

— MII_RXD (3.0) — група паралельних сигналів даних, які видаються з трансивера в MAC-контроллер;

— MII_RX_CLK — тактовий сигнал для приймання даних; генерується в трансивері і передається в MAC: 2,5 МГц для операцій 10 Мбіт/с, 25 МГц для операцій 100 Мбіт/с;

— MII_RX_DV — достовірність прийнятих даних; встановлює трансивер, якщо він отримує достовірний пакет даних і коли видає достовірні дані на RXD;

— MII_RX_ER — помилка приймання генерується трансивером при виявленні помилки в даних, що приймаються [34].

Інтерфейс RMII (Reduced MII) — це "скорочений" варіант MII, де трансивер може працювати зі зменшеним набором сигналів інтерфейсу MII. У цьому режимі роботи розрядність шин RXD і TXD зменшується вдвоє, але відповідно збільшується частота синхронізації (рис. 3.4) [34].

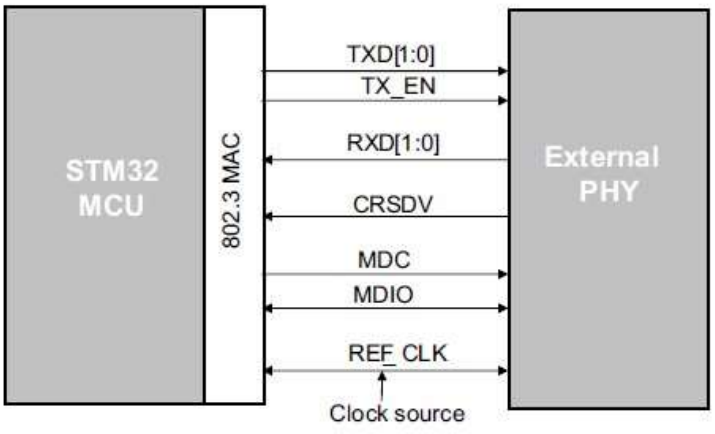


Рисунок 3.4 — Підключення трансивера за інтерфейсом RMII

Вибір способу підключення, MII чи RMII, здійснюється за допомогою 23-го біта (MII_RMII_SEL) в регістрі SYSCFG_PMC мікроконтролера. В табл. 3.2 наведено перелік ліній введення/виведення мікроконтролера

STM32F407VET6, які можуть використовуватися для сигналів інтерфейсів MII та RMII [34].

Таблиця 3.2 — Ліній портів вводу/виводу STM32F407VET6 (з альтернативними функціями MII та RMII)

Порт	Ethernet
PA0	WKUP ETH_MII_CRS
PA1	ETH_MII _RX_CLK / ETH_RMII _REF_CLK
PA2	ETH_MDIO
PA3	ETH_MII_COL
PA7	ETH_MII _RX_DV/ETH_RMII _CRS_DV
PB0	ETH_MII_RXD2
PB1	ETH_MII_RXD3
PB5	ETH_PPS_OUT
PB8	ETH_MII_TXD3
PB10	ETH_MII_RX_ER
PB11	ETH_MII_TX_EN/ETH_RMII_TX_EN
PB12	ETH _MII_TXD0/ETH_RMII_TXD0
PB13	ETH _MII_TXD1/ETH_RMII_TXD1
PC1	ETH_MDC
PC2	ETH_MII_TXD2
PC3	ETH_MII_TX_CLK
PC4	ETH_MII_RXD0/ETH_RMII_RXD0
PC5	ETH_MII_RXD1/ETH_RMII_RXD1
PE2	ETH_MII_TXD3
PG8	ETH_PPS_OUT
PG11	ETH_MII_TX_EN/ETH_RMII_TX_EN
PG13	ETH_MII_TXD0/ETH_RMII_TXD0
PG14	ETH_MII_TXD1/ETH_RMII_TXD1
PH2	ETH_MII_CRS
PH3	ETH_MII_COL
PH6	ETH_MII_RXD2
PH7	ETH_MII_RXD3
PI10	ETH_MII_RX_ER

Отже, обраним трансивером є модуль DP83848 Ethernet Board (рис. 3.5), який об'єднує в собі Ethernet-трансивер фізичного рівня DP83848, роз'єм RJ-45 та роз'єм керуючого інтерфейсу для підключення до мікроконтролерів з вбудованим Ethernet-модулем. Основні характеристики цього модуля наведені у табл. 3.3 [35].

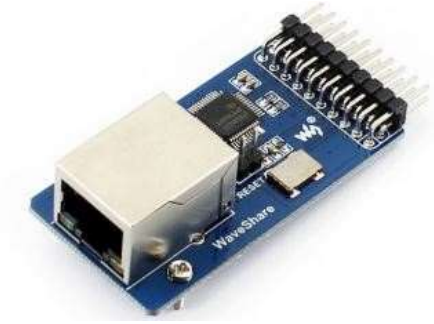


Рисунок 3.5 — Модуль трансивера DP83848 Ethernet Board

Таблиця 3.3 — Параметри модуля DP83848 Ethernet Board

Параметр	Значення
Підтримувані мережеві підключення	10/100МБіт
Стандарт	802.3u RMII
Напруга живлення	3.3 В
Споживана потужність	не більше 270 мВт

Для забезпечення підтримки бездротового з'єднання з мережею WiFi також планується використання готових рішень, що спрощує процес розробки завдяки підтримці сімейства протоколів TCP/IP. На сьогоднішній день одними з найбільш популярних є ESP модулі WiFi, що базуються на мікросхемі ESP8266.

Модулі виготовляються компанією Espressif Systems (Китай) і відзначаються найнижчою вартістю серед конкурентів при це вони мають достатньо значні можливості. Існують різні модифікації, що, в основному, різняться за обсягом флеш-пам'яті, типами роз'ємів та іншими характеристиками.

Модулі ESP складаються з мікросхеми ESP8266EX, мікросхеми SPI Flash-пам'яті об'ємом 2 Мбайт і вбудованої PCB-антени. Мікросхема ESP8266EX містить 32-бітний мікроконтролер Tensilica L106 з тактовою частотою 80 МГц та низьким енергоспоживанням, а також радіоінтерфейс. У режимі максимальної продуктивності тактова частота мікроконтролера Tensilica L106 може досягати 160 МГц. Мікросхема ESP8266EX підтримує IPv4, TCP/UDP/HTTP/FTP та різні режими Wi-Fi-з'єднання, такі як Wi-Fi-

клієнт, Wi-Fi-точка доступу та комбінований режим точки доступу та клієнта. Для забезпечення безпеки передачі даних по Wi-Fi (802.11b/g/n) використовуються технології WPA/WPA2, WEP/TKIP/AES [36], [37].

Згідно з даними виробника, підтримка Wi-Fi займає лише 20% процесорного часу модуля, що залишає значні ресурси для користувацьких додатків. Модуль використовує операційну систему RTOS, що спрощує інтеграцію користувацьких програм у програмне забезпечення модуля [36].

Серед різних варіантів модулів ESP обрано модель ESP-07, оскільки вона має керамічну антену та можливість підключення зовнішньої, що поліпшить відстань та якість зв'язку. Взаємодія з модулем відбувається за допомогою AT-команд. Зовнішній вигляд модуля ESP-07 можна побачити на рис. 3.6, а його основні технічні характеристики представлені у таблиці 3.4 [37].

Рисунок 3.6 —Wi-Fi модуль ESP-07

Для забезпечення комунікації між контролером керування доступом та смартфоном через Bluetooth ми використаємо готовий Bluetooth-модуль. З наявних моделей ми обрали модуль HC-05 (рис. 3.7), який є одним з найбільш популярних на ринку. Модуль HC-05 призначений для реалізації двостороннього зв'язку за протоколом Bluetooth і може працювати в режимах Master та Slave. Це дозволяє модулю самостійно виявляти Bluetooth-пристрої та налагоджувати зв'язок з ними.

Підключення модуля здійснюється через послідовний асинхронний TTL-сумісний інтерфейс UART.

Таблиця 3.4 — Параметри Wi-Fi модуля ESP-07

Процесорне ядро	Tensilica L106, 32 біт
Wi-Fi-протоколи	802.11 b/g/n
Діапазон частотн	Від 2.4 ГГц до 2.5 ГГц
Режими WiFi	Station / SoftAP / SoftAP + Station
Безпека	WPA/WPA2
Шифрування	WEP/TKIP/AES
Підтримувані мережеві протоколи	IPv4, TCP/UDP/HTTP/FTP
Протоколи	WiFi Direct (P2P), P2P Discovery, P2P GO (Group Owner) mode, GC (Group Client) mode, P2P Power Management.
Інтерфейс для підключення	UART
Напруга живлення	від 2.5 В до 3.6 В
Середній струм споживання	80 мА

Основною складовою модуля є мікросхема CSR BC417, яка підтримує Bluetooth версії 2.0. Швидкість передачі даних може сягати до 3 Мбіт/с. Взаємодія з модулем здійснюється за допомогою команд AT. Основні характеристики модуля HC-05 наведені в таблиці 3.5 [38].

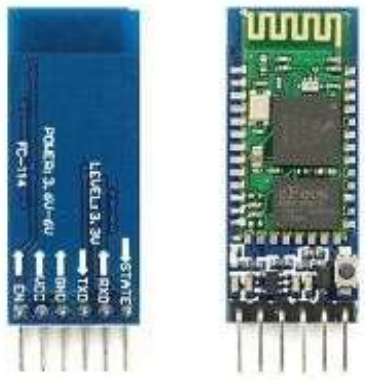


Рисунок 3.7 — Bluetooth-модуль HC-05

Таблиця 3.5 — Параметри Bluetooth-модуля HC-05

Параметр	Значення
Робоча напруга	+3,3 В або +5 В
Споживаний струм	50 мА
Основна частота	2,4 ГГц
Антена	Інтегрована
Потужність	≤ 4дБм, клас 2
Чутливість	≤ 84дБм, при 0,1%
Швидкість синхронної передачі даних	1 Мбіт/с
Швидкість асинхронної передачі даних	2,1 Мбіт/с
Захист	Авторизація та шифрування
Розміри (Д × Ш × В)	17 мм × 43 мм × 7,5 мм

Роз’єм модуля HC-05 має 6 контактів підключення (табл. 3.6).

Таблиця 3.6 — Призначення контактів модуля HC-05

Контакт	Символ	Призначення
1	EN	Вхід дозволу - активний рівень низький
2	VCC	Живлення
3	GND	Контакт «землі»
4	TXD	Вихід даних
5	RXD	Вхід даних
6	STATE	Вихід індикації стану: високий рівень - зв'язок встановлено, перемикання - встановлення зв′язку.

Керування виконавчим пристроєм, що регулює фізичний доступ, буде реалізоване за допомогою імпульсного (бістабільного) електромагнітного реле. Такі реле мають дві обмотки для імпульсного керування. Подача імпульсного струму до однієї з обмоток викликає замикання контактів реле, а до іншої - їх

розмикання. Для керування імпульсним реле використовуються два транзисторних ключі, що забезпечують формування імпульсів струму в обмотках (рис. 3.7).

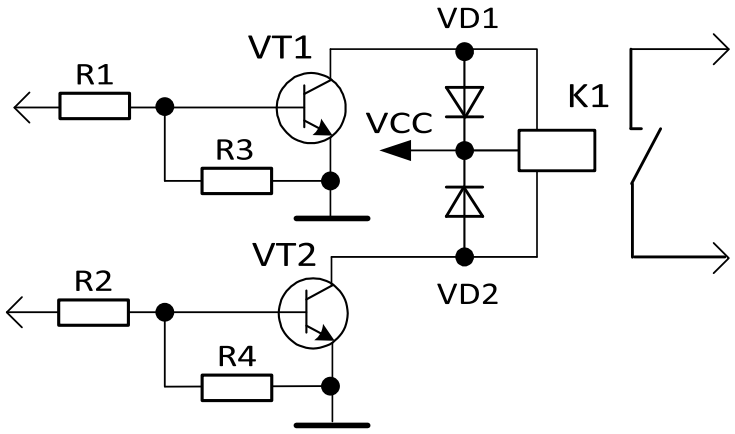


Рисунок 3.7 — Схема для керування імпульсним реле

Вибираючи реле, головними критеріями є комутована потужність не менше 2 кВт та напруга керування +5 В. Відповідно до цих вимог обрано реле G2RL145DC, яке має такі основні параметри, які наведені в табл. 3.7 [39].

Таблиця 3.7 — Основні параметри реле G2RL145DC

Параметр	Значення
Комутований струм	12 А, 250 В змінного струму 12 А, 24 В постійного струму
Напруга керування	5 В
Струм керування	80 мА
Кількість перемикань	20 млн.

Транзисторні ключові каскади побудуємо на транзисторах BC817-25, оскільки вони відповідають вимогам: максимальний струм колектора більший за струм керування реле (що складає 80 мА), а напруга колектор-емітер більша за 5 В. Основні параметри транзистора BC817-25 наведені в таблиці 3.8 [40].

Таблиця 3.8 — Основні параметри транзистора BC817-25

Параметр	Значення
Тип	n-p-n
Найбільший струм колектора	500 мА
Найбільша напруга колектор-база	50 В
Найбільша напруга колектор-емітер	45 В
Статичний коефіцієнт підсилення	не менше 160
Гранична частота	200 МГц

Транзистори BC817-25 також будуть використовуватися для керування світлодіодами, які відображатимуть стан елемента блокування пристрою. Стан пристрою загородження, відчинений чи зачинений, буде визначатися за допомогою датчиків, які виявлятимуть сигнали мікроконтролера.

Магнітно-контактний датчик буде використовуватися для фіксації перебування пристрою загородження у крайньому положенні. Він складається з двох частин: одна містить постійний магніт і розміщується на рухомому елементі, наприклад, на двері, а інша - герконовий елемент, що складається з двох електричних контактів і розміщується на нерухомому елементі, наприклад, на дверному рамі. При зачиненні дверей магніт утримує контакти геркона в замкнутому стані, а при відкритті дверей контакти геркона розмикаються.

Для захисту входів мікроконтролера від пробою підключення датчика ми будемо використовувати оптрони, такі як EL817 серії. Параметри оптрона EL817 наведено в табл. 3.9 [41].

Таблиця 3.9 — Основні параметри оптрона EL817

Параметр	Значення
Тип оптрона	транзисторний
Напруга ізоляції	5 кВ
Вхідний струм світлодіода	60 мА
Вхідна напруга на світлодіоді	1,2 В
Максимальний вихідний струм колектора	50 мА
Максимальна напруга колектор-емітер	35 В

Підключення герконового сенсора через оптрон здійснемо за схемою, що наведена на рис. 3.8.

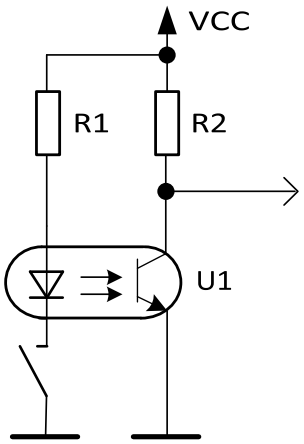


Рисунок 3.8 — Схема підключення герконового сенсора через оптрон

3.2 Розробка функціональної та принципової схем пристрою керування

З використанням відібраних компонентів та розглянутих схемних рішень була розроблена функціональна схема пристрою керування (контролера керування доступом), яка наведена у додатку Г. Контролер побудований на мікроконтролерному модулі STM32F407VET6-Mini DD2, який базується на 32-бітному високопродуктивному мікроконтролері STM32F407VET6. Модуль STM32F407VET6-Mini є самодостатнім функціональним блоком, оскільки, крім самого мікроконтролера, містить усі необхідні компоненти для підтримки його роботи. Цей модуль виконує такі завдання:

— обмін повідомленнями з хмарним Інтернет-сервером, використовуючи мережеве Ethernet або WiFi підключення;

— взаємодію зі смартфоном через з′єднання Bluetooth та визначення прав доступу;

— керування через виконавчі елементи загороджувальними пристроями для надання доступу.

Підключення до мережі Ethernet забезпечується за допомогою наявного у мікроконтролері STM32F407VET6 контролера Ethernet та модуля трансивера

фізичного рівня Ethernet DD1. Контролер Ethernet, що входить до складу мікроконтролера, забезпечує підтримку функцій підрівня MAC канального рівня згідно зі стандартом IEEE802.3. Модуль трансивера DD1 використовує мікросхему DP83848 для приймання та передачі даних по витій парі, а також для кодування та декодування даних.

Підключення трансивера DD1 до модуля DD2 (контролера Ethernet мікроконтролера STM32F407VET6) здійснюється за допомогою RMII інтерфейсу, сигнали якого виведені на роз'єми J2 та J3 модуля DD2. Фізичне підключення до кабелю Ethernet здійснюється через 8-контактний роз'єм RJ45, розташований на платі модуля DD1. Обмін даними з хмарним сервером через мережу Ethernet відбувається за допомогою стеку протоколів TCP/IP, який підтримується програмним забезпеченням мікроконтролера STM32F407VET6.

Підключення до мережі WiFi забезпечується за допомогою WiFi модуля DA1, який дозволяє обмін даними по радіоканалу відповідно до стандарту 802.11x. Модуль DA1 забезпечує підтримку стеку протоколу TCP/IP, що дозволяє реалізувати функції різних рівнів мережі. Взаємодія з хмарним сервером через WiFi підключення відбувається за допомогою простих AT команд, які передаються між мікроконтролерним модулем DD2 та WiFi модулем DA1 через послідовний асинхронний канал зв'язку, який формується лініями послідовних даних RxD та TxD з використанням вбудованого у мікроконтролер STM32F407VET6 універсального асинхронного передавача/приймача UART1.

Надання прав доступу відбувається за допомогою ідентифікатора, який передається зі смартфона в контролер керування доступом через Bluetooth з'єднання, встановлене за допомогою Bluetooth модуля DA2. Модуль DA2 забезпечує двосторонній зв'язок між смартфоном та мікроконтролерним модулем DD2 за протоколом Bluetooth. Підключення модуля до мікроконтролера STM32F407VET6 здійснюється через послідовний асинхронний інтерфейс, і мікроконтролер обмінюється даними з модулем за

допомогою асинхронного приймача/передавача UART2 через лінії послідовних даних Tx та Rx.

У контролері керування доступом передбачені два канали управління виконавчими пристроями, які вмикані/вимикані за допомогою імпульсних реле К1 та К2. Для кожного реле використовуються два імпульсні сигнали. Один імпульсний сигнал призводить до замикання контактів реле, а інший - до їх розмикання. У статичному стані, коли контакти реле залишаються замкненими або розімкненими, сигнал управління має рівень логічного нуля.

Управління реле здійснюється через лінії PD0…PD3 мікроконтролера STM32F407VET6, сигнали з яких подаються на ключі каскадів на транзисторах VT1…VT4. Сигнали на лініях PD0, PD1 забезпечують керування реле К1, на лініях PD2, PD3 - реле К2. Високий рівень сигналу забезпечує переведення підключеного до нього транзистора у відкритий стан. Це створює умови для протікання струму через обмотку реле, яка увімкнена у колекторне коло цього транзистора. Це, у свою чергу, призводить до зміни стану контактів реле. Діоди VD1…VD4 захищають транзистори VT1…VT4 від ЕРС самоіндукції, що виникає у котушці реле в момент перемикання транзистора у закритий стан. Резистори R5… R8 обмежують базові струми транзисторів VT1…VT4.

Резистори R11 та R14, що з'єднані між загальною шиною та базами транзисторів, забезпечують закритий стан транзисторів у момент вмикання живлення, коли лінії введення/виведення мікроконтролера перебувають у високоомному стані. Вихідні контакти реле вмикаються у розрив кола живлення виконавчого пристрою через роз'єми X3 або X4.

Індикація стану загороджувального пристрою забезпечується світлодіодами HL1 та HL2 червоного та зеленого кольорів. Світіння червоного світлодіода відповідає зачиненому стану, зеленого - відчиненому. Керування світлодіодами відбувається за допомогою ключових каскадів на транзисторах VT5 та VT6, які підключені до ліній PC10 та PC11 мікроконтролера. Вмикання світлодіода відбувається за сигналом високого логічного рівня на виході мікроконтролера STM32F407VET6, який

переводить транзистор у відкритий стан, створюючи умови для протікання струму через світлодіод, що увімкнений у його колекторне коло.

Резистори R9 та R10 обмежують базові струми транзисторів VT5 та VT6. Їх опір визначається за формулою (3.1), в яку вміщується значення струму керування реле IR. Замість цього значення слід використовувати значення робочого струму світлодіода ISD. Резистори R15 та R16 обмежують прямий струм світлодіода.

Для моніторингу положення загороджувального пристрою передбачено можливість приєднання двох герконових сенсорів. Контакти герконів активуються між виводами 2, 4 та 3, 4 роз'єму X1. Стан контактів визначається згідно зі сигналами на входах PB5 та PB6 мікроконтролера STM32F407VET6. Для захисту виводів мікроконтролера від можливих перевантажень підключення датчиків проводиться через транзисторні оптрони U1 та U2.

При вказаному з'єднанні герконів, вхідні схеми оптронів, створені за допомогою світлодіода, будуть активовані послідовно до їх контактів. При розімкненому стані контактів струм через світлодіод припиняється. Це призводить до закриття вихідного фототранзистора оптрона, що зумовлює напругу на його колекторі, що відповідає високому рівню логіки. У разі замкнених контактів герконів, вхідне коло оптрона замикатиметься, що призведе до протікання струму через світлодіод і його світіння. В цьому випадку фототранзистор буде відкритий, тому на його колекторі буде низький рівень напруги. Резистори R1 та R2 служать для обмеження прямого струму світлодіодів. Резистори R3 та R4 виступають як навантаження для фототранзисторів і мають опір, що обирається на рівні кількох кілоом.

Живлення розробленого пристрою керування здійснюється від місцевого джерела стабільної напруги +5В, яка виробляється під окремого DC-DC перетворювача 24 В – 5 В і підключається через роз'єм X2. Напруга живлення для Ethernet трансивера DD1 та WiFi модуля DA1 становить 3,3 В. Цю напругу постачає плата мікроконтролерного модуля DD2, що містить другий DC-DC перетворювач.

4 ДОСЛІДЖЕННЯ Й ВИПРОБУВАННЯ РОЗРОБЛЕНОГО КОМПЛЕКСУ КЕРУВАННЯ АВТОМАТИКОЮ ПРОПУСКУ LOKKYY

4.1 Установка, підготовка до роботи і початок роботи з комплеком

Розглянемо складові частини розробленого комплексу LOKKYY:

— апаратний мікроконтролерний пристрій керування LOKKYY з вбудованими безпровідними інтерфейсами та зовнішніми сенсорами й з'єднувальними кабелями (далі - пристрій LOKKYY);

— програмний мобільний застосунок LOKKYY APP, що має завантажуватис на смартфони користувачів їз сервісів Google Play Store та Apple App Store (далі застосунок LOKKYY APP).

Настанови з установки та налаштування пристрою LOKKYY далі викладемо покроково.

Крок 1— розпакування. Потрібно розпакувати пристрій з коробки та виймати її вміст. В типовому комплекті постачання на 1 канал керування має бути вміст, показаний на рис.4.1

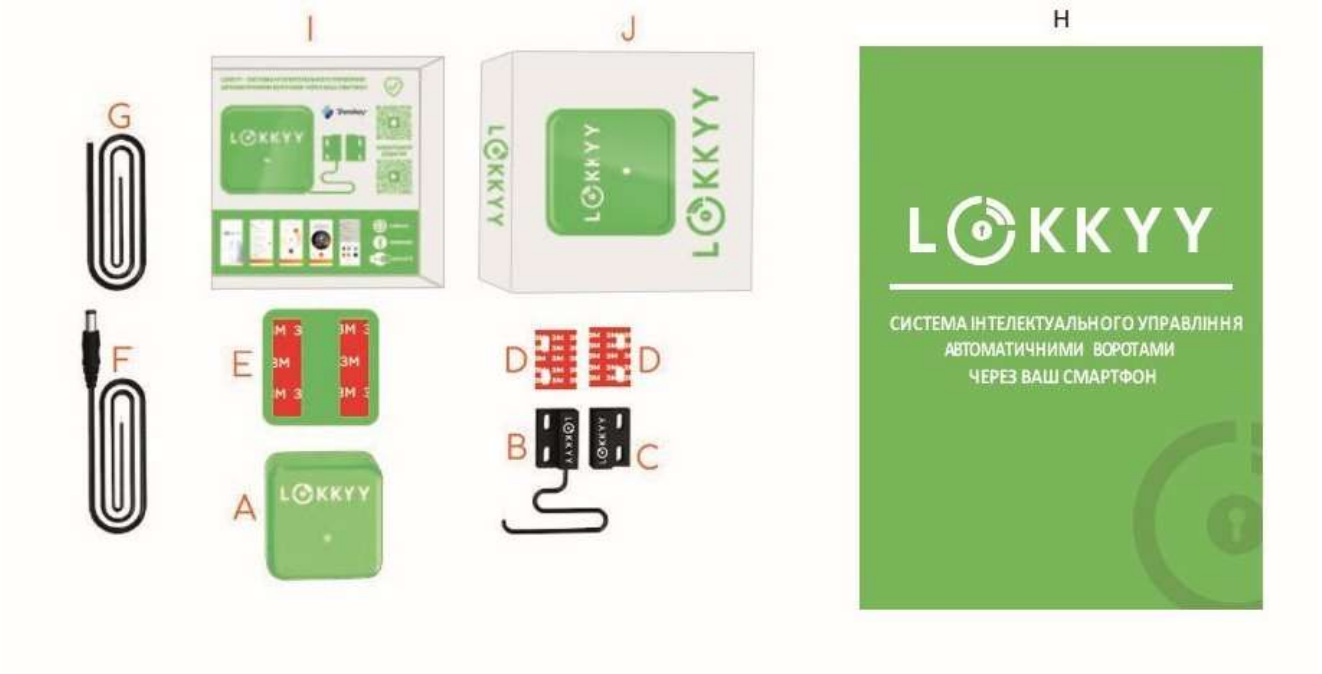


Рисунок 4.1 — Вміст типового комплекту пристрою LOKKYY

На рисунку:

A) — модуль пристрою керування LOKKYY;

B) — магнітний герконовий сенсор відкриття/закриття з кабелем 3 м;

C) — магнітний герконовий сенсор відкриття/закриття;

D) — скотч двосторонній для кріплення датчиків;

E) —скотч двосторонній для кріплення модуля пристрою LOKKYY;

F) —кабель живлення 1 м;

G) —кабель управління 3 м;

H) — експлуатаційна документація.

В двоканальному комплекті число поз. B, C, D подвоюється.

Крок 2.1 — встановлення двостороннього скотчу на модуль пристрою LOKKYY і на сенсори проілюстровано на рис. 4.2.

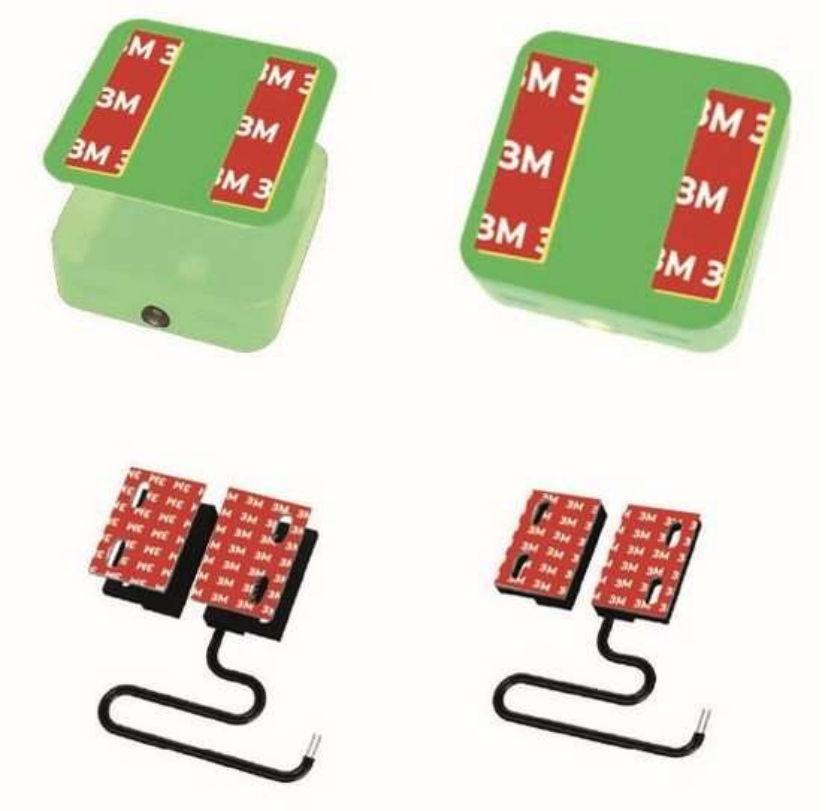


Рисунок 4.2 — Встановлення двостороннього скотчу

Слід видалити захисну плівку з одного боку наліпки E та розташувати наліпку на тильній частині модуля пристрою LOKKYY. Не видаляти захисну

плівку з іншого брку наліпки. Також видалити захисну плівку з одного боку наліпок D та розташувати наліпку на тильній частині датчиків B та C.

Крок 2.2 — відновлення налаштувань пристрою LOKKY, якщо активується новий смартфон телефон адміністратора або було видалено клієнтський застосунок LOKKYY APP зі смартфону адміністратора, ви можна скинути пристрій. Для цього на тильній частині пристрою слід скористатися кнопкою скидання до заводських налаштувань не менш, натиснувши її не менш ніж 10 с як показано на рис. 4.3.

Рисунок 4.3 – Апаратне скидання налаштувань

Після скидання пристрій керування LOKKYY може бути налаштований як новий пристрій з будь якого смартфону із Bluetooth, що знаходиться у радіусі покриття пристрою (детальніше див. Крок 8).

Також можна скинути пристроій LOKKYY зі смартфону, скористувавшись застосунком LOKKYY APP. Для цього, як показано на рис. 4.4 на домашній закладці застосунку слід натиснути кнопку та увійти в меню налаштувань.

Далі потрібно вибрати пункт меню «Скинути пристрій» та ввести код ідентифікації, який з'явиться на екрані. Після цього пристрій LOKKYY буде скинуто до заводських налаштувань. Всі ключі, які були згенеровані в застосунку LOKKYY APP також будуть дезактивовані.

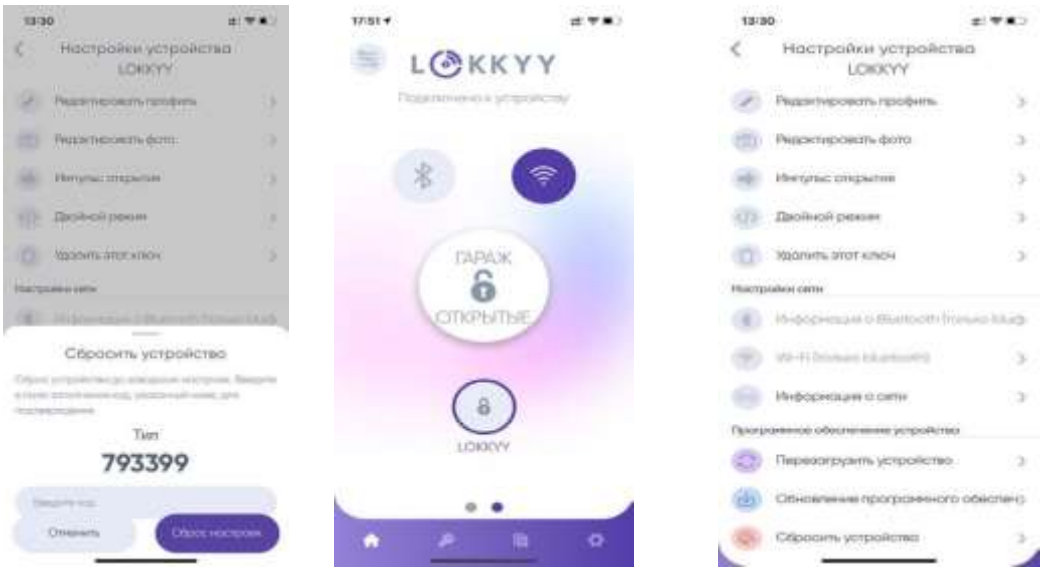


Рисунок 4.4 — Скидання налаштувань в застосунку LOKKYY APP

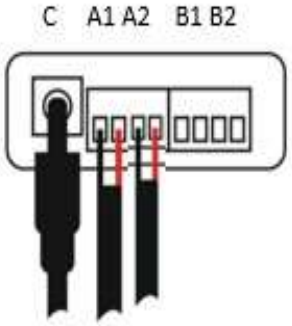
Крок 3 — підключення кабеля управління, слід скористатися кабелем G для підключення виходу A1 пристрою LOKKYY до вхідних контактів блоку керування електроприводом воріт/ролет . Такий блок матиме різні назви залежно від виробника та моделі приводу: "Кнопка ручного керування", "Імпульсний вхід", "PP", "Послідовний доступ", "Почати", "Ключ", "Настінний перемикач", а також "BTM" (кнопка) або "ЗВС".

Якщо немає впевнені в правильності підключення, слід вивчити настанову з експлуатації приводу або звернутися до сертифікованих партнерів, які інсталюють на налаштують пристрій LOKKYY.

Для прикладу на рис. 4.5 наведено підключення кабеля управління до приводу ролетних воріт типу Hormann ProMatic 2.

Крок 4 — підключення магнітних сенсорів відкриття / закриття — слід застосувати наявний магнітний сенсор (B) для під’єднання до виходу модуля пристрою керування LOKKYY (A2). Магнітний сенсор (B) закріплюють на корпусі чи направляючій приводу (залежно від типу воріт).

Друга частина сенсора (B) (без проводу) кріпиться на рухомій частині воріт в крайньому закритому положенні так, щоб в цьому положенні магніт знаходився навпроти магнітного сенсора (B), на відстані не більше 20 мм, як на рис. 4.6.



A1, B1 – вхід підключення кабеля управління (G)

A2, B2 – вхід для підключення сенсора відкриття/закриття (C)

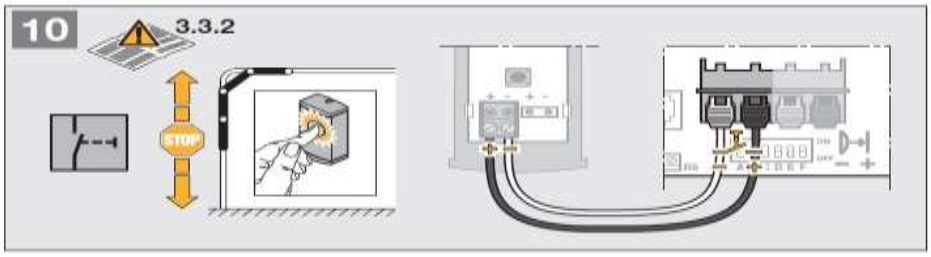


Рисунок 4.5 — Приклад позначення контактів модуля LOKKYY і підключення кабеля управління до приводу ролетних воріт Hormann ProMatic 2

Рисунок 4.6 — Кріплення магнітного сенсора як кінцевика

Крок 5 — підключення кабеля живлення, потрібно застосувати наявний кабель (F) для під’єднання виходу пристрою LOKKYY (C) до низьковольтного входу приводу.

Перед під’єднання кабеля живлення слід ознайомитись с настановами з монтажу, експлуатації та обслуговування потрібної моделі приводу, щоб упевнитись, що привід має необхідне значення напруги для живлення пристрою LOKKYY, а саме: 12/24 V AC/DC, полярність при цьому не важлива.

Далі слід увімкнути конектор в пристрій LOKKYY та увімкнути живлення приводу. Світлодіодний індикатор на пристрої LOKKYY повинен блимати білим кольором.

Для прикладу на рис. 4.7 наведено під’єднання кабеля живлення до приводу ролетних воріт Hormann ProMatic 2.

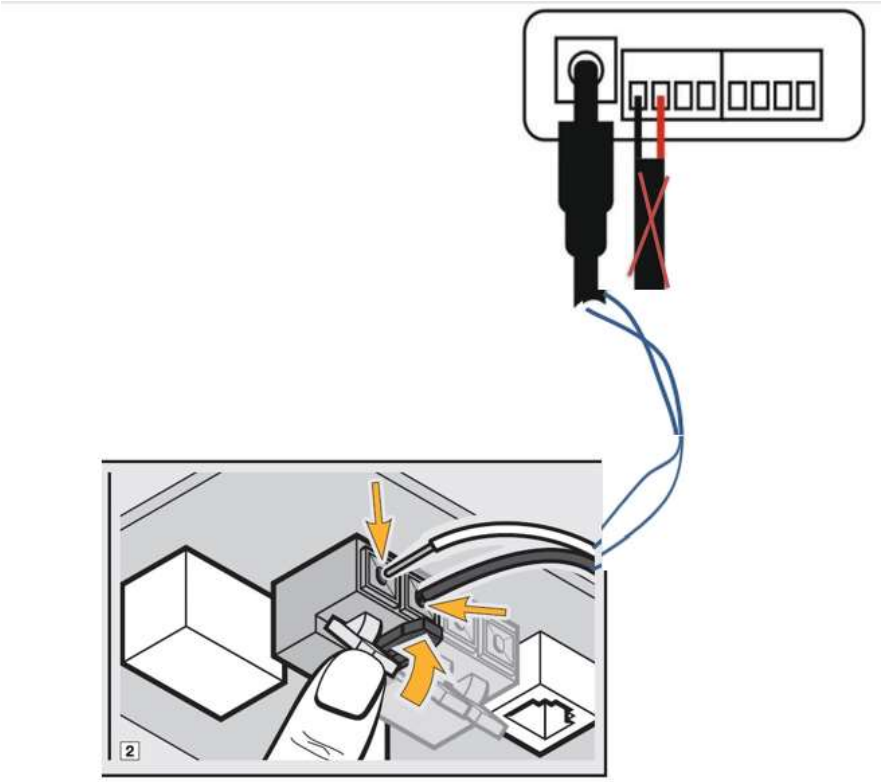


Рисунок 4.7 — Приклад під’єднання кабеля живлення до приводу ролетних воріт типу Hormann ProMatic 2

4.2 Вимоги до функціональних можливостей

Основні можливості комплексу LOKKYY включають:

— налаштування пристрою LOKKYY на об'єкті керування через бездротовий інтерфейс Bluetooth та підключення до Інтернету через доступну мережу Wi-Fi;

— визначення стану пропускної системи об'єкту (відкрито/закрито) за допомогою магнітних датчиків пристрою LOKKYY та передача цієї інформації в мобільний додаток LOKKYY APP на смартфоні користувача через бездротовий інтерфейс Bluetooth або мережу Wi-Fi та Інтернет;

— отримання зворотних команд керування для відкривання/закривання пропускної системи шляхом замикання/розмикання контактів вбудованого в пристрій LOKKYY реле;

— налаштування профілю користувача додатка LOKKYY APP;

— генерування та поширення постійного чи тимчасового ключа для керування пропуском на об'єкт іншим користувачам;

— перегляд поточного стану об'єктів та інформації про час та користувачів, які керували пропуском.

4.3 Основні показники призначення, що контролюються

4.3.1 Кількість вихідних ліній керування навантаженням – 4 (2 канали).

4.3.2 Тип виходів – гальванічно розв’язані нормально розімкнені контакти електромагнітного реле.

4.3.3 Максимальна комутована напруга навантаження — 60 В постійного струму.

4.3.4 Максимальний струм комутації в навантаженні — 1 А .

4.3.5 Кількість вхідних ліній контролю – 4 (2 канали).

4.3.6 Тип датчиків контролю – магнітні герконові, нормально розімкнені. Встановлюються як кінцевики закритого положення пропускного механізму.

4.3.7 Сигналу спрацювання на лініях контролю - замикання на «землю». Захист від перешкод на лініях контролю- є. Захист від «брязкання контактів»- є.

4.3.8 Загальний час спрацювання від подачі команди зі смартфона до спрацювання реле — від 0,1 с до 10 с.

4.3.9 Вимоги до інтерфейсів зв’язку

Безпровідні інтерфейси зв’язку, вмонтовані в пристрій LOKKYY– -

Bluetooth SIG version 5.0 (від 2,402 ГГц до 2,480 ГГц);

- Wi-Fi 802.11 b/g (від 2,4000 ГГц до 2,4835 ГГц).

4.3.10 Електроживлення пристрою LOKKYY повинно здійснюватися від зовнішнього джерела номінальною напругою 24 В постійного або змінного струму частотою 50 Гц. Робочий діапазон напруг від 9 В до 32 В.

Максимальний струм споживання пристрою LOKKYY при спрацюванні реле — 200 мА.

Споживана потужність пристрою LOKKYY в колі постійної вхідної напруги 12 В не більше 6 Вт.

4.3.11 Конструктивне виконання пристрою LOKKYY — електронний модуль в пластиковому корпусі, магнітні датчики, з’єднувальні кабелі, елементи кріплення (рис. 4.1). Габаритні розміри модуля не більше 50 мм х 50 мм х 25 мм. Вага модуля не більше 0.1 кГ.

4.4 Програма випробування комплексу

Для перевірки відповідності вимогам технічних умов, комплекс LOKKYY піддають таким випробуванням:

— приймально-здавальним;

— періодичним;

— випробуванням на надійність.

Випробування проводить відділ технічного контролю підприємства-виробника силами і засобами підприємства- виробника, або проведення випробувань здійснюється організаціями, що мають акредитацію на виконання відповідних випробувань.

Засоби випробувань, що використовуються, повинні бути повірені чи атестовані. Випробування обладнання , крім окремо обумовлених, проводять в нормальних кліматичних умовах.

Результати випробувань вважають позитивними, а комплекс LOKKYY таким, що пройшов випробування, якщо випробування проведені в повному обсязі і послідовності, встановленій в розділі 3 і виріб відповідає всім вказаним вимогам.

Результати випробувань вважають негативними, а комплекс LOKKYY таким, що не витримав випробування, якщо в результаті випробувань буде виявлено невідповідність виробу хоча б одному з вимог, встановлених цими ТУ для категорії випробувань, що проводяться.

На приймально-здавальні випробування (ПЗВ) представляють кожний виготовлений комплекс LOKKYY.

Обсяги й послідовність проведення ПЗВ наведено в таблиці 4.1. Результати випробувань оформлюють протоколом.

Прийнятим вважають комплекс LOKKYY, який витримав випробування, є укомплектованим і упакованим у відповідності до вимог цих ТУ, на який оформлено формуляр, що засвідчує його прийомку. Дефектний комплекс LOKKYY повертають у виробництво. Після усунення дефектів виріб повинен бути представлений на повторну перевірку.

Періодичні випробування (ПВ) проводять один раз в рік на одному з виробів, що пройшов приймально-здавальні випробування.

Відбір взірця для випробувань проводять випадковим способом з готових на даний момент виробів. По пункту невідповідності, що виявлена в процесі випробувань, випробування проводять на подвійній кількості виробів. Якщо і в цьому випадку результат випробувань незадовільний, то після аналізу і усунення дефектів повторні випробування проводять в повному обсязі на подвійній кількості виробів.

При отриманні незадовільних результатів випробувань приймання і поставку виготовлених виробів призупиняють до отримання додатних результатів випробувань та проводять дослідження причин, що привели до не задовільних результатів , з випуском висновку про необхідні заходи по усуненню виявлених недоліків.

Обсяги й послідовність проведення випробувань оформляють актом. До акту додаються протоколи всіх проведених випробувань, підписаних особами, що проводили ці випробування.

Таблиця 4.1 Перелік основних приймально-здавальних і періодичних випробувань комплекса LOKKYY

№ п/п	Назва випробування, перевірки	Обов'язковість при випробуваннях		
		ПЗВ	ПВ	ВН
1	Перевірка відповідності вимог до конструкції	+	+	-
2	Підключення і перевірка працездатності	+	+	+
3	Перевірка вимог до джерел живлення	+	+	-
4	Перевірка вимог до сигналізації і індикації	-	+	-
5	Перевірка показників призначення	+	+	+
6	Перевірка вимог до програмного забезпечення	-	+	-
7	Перевірка інтерфейсів зв'язку	+	_	-

4.5 Основні методи контролювання

Комплекс LOKKYY, засоби вимірювань, контролю і випробувань, допоміжні пристрої, що використовуються при випробуваннях, повинні бути підготовлені до роботи у відповідності з їх експлуатаційними документами.

Обладнання, до якого підключається пристрій LOKKYY повинно бути надійно заземлено перед підключенням до мережі напруги живлення.

При всіх видах випробувань перед відключенням заземлення необхідно відключити відповідне обладнання від мережі живлення.

Всі підключення до пристрою LOKKYY повинні відбуватися після відключення виробів від мережі живлення.

Для контролю працездатності й перевірки параметрів комплексу LOKKYY під час приймально-здавальних і періодичних випробувань необхідно на базі виробника слід використовувати спеціальний випробувальний стенд КМКА 001.03.00.000 ПС, що імітує об'єкт пропуску. Стенд виготовлено на основі електроприводу поширених ролетних воріт типу Hormann ProMatic (Німеччина) . В якості джерела живлення для пристрою LOKKYY під час випробувань

використовують промисловий нестабілізований лінійний знижуючий трансформатор напруги змінного струму з 220 В на 24 В - ОСМ-0,063 220/24 (ELTIZ, Україна) або аналогічний з 220 В на 12 В і 24 В - S21 C12K 00 (Cetinkaya Pano, Турція).

В якості смартфонів користувачів під час випробувань використовують актуальні моделі від iPhone 5S (IOS 11) і вище та на базі ОС Android 6.0 і вище.

Для комплексної перевірки працездатності комплекса LOKKYY необхідно налаштувати його зв'язок з мережею Інтернет через Wi-Fi роутер, доступний у випробувальній лабораторії.

Перелік обладнання і засобів вимірювань, необхідних для контролю і випробувань наведений у табл.4.2. Обладнання і прилади, наведені в переліку, можуть бути замінені аналогічними, які забезпечують потрібні режими випробувань і точність вимірювань.

Перевірку відповідності вимог до зовнішніх джерел живлення виконують з використанням регульованого лабораторного блоку живлення постійної напруги типу Unit UTP3303 0-32V 0-3A з вмонтованими амперметрами чи з використанням іншого лабораторного аналогічного блоку живлення з вмонтованими чи окремими вольтметрами і амперметрами постійного струму (з використанням 2-х мультиметрів універсальних DT9207), як показано на рисунку 4.8.

Таблиця 4.2 Перелік обладнання і засобів вимірювань, необхідних для контролю і випробувань

№ п/п	Назва обладнання і основні параметри
1	Стенд спеціальний випробувальний на основі електроприводу ролетних воріт Hormann ProMatic – 1 шт.
2	Трансформатор напруги змінного струму з 220 В/50 Гц в +24 В ± 5 % в, 2А ОСМ-0,063 220/24 – 1 шт.
3	Смартфон Apple з ОС не нижче IOS 11 – 1 шт.
4	Смартфон з ОС Android 6.0 – 1 шт.
5	Wi-Fi роутер з підтримкою стандарта 802.11 b/g

6	Штангенциркуль ШЦ-111-400-0,1. Діапазон вимірювань (0-400)мм. Похибка вимірювань ±0,1мм.
7	Ваги KERN EHA 3000-0 Границя вимірювань від 10 до 3000 г. Похибка вимірювань ±2 г.
8	Рулетка 5 м
9	Установка пробійна УПУ-10. Границя встановлення випробувальної напруги 1,3,10 кВ. Номінальне значення частоти змінної напруги 50 Гц. Потужність 1кВА. - 1 шт.
10	Вимірювач параметрів безпеки електрообладнання GPI-745A. Границя встановлення випробувальної напруги 5 кВ змінного струму, 6 кВ постійного струму. Вимірювання опору ізоляції і заземлення, контроль опорів з'єднань, детектор струмів витікання. Потужність 200 ВА, - 1 шт.
11	Мегаомметр М4100/3 Діапазон вимірювань від 0 до 100 МОм. Клас точності 1,0. Номінальна напруга 500 В.
12	Блок живлення лабораторний Unit UTP3303 0-32V 0-3A. Вихідна напруга від 0 до +32 В, вихідний струм від 0 до 3 А. Похибки вимірювання напруги 1%, струму 2% - 1 шт.
13	Цифровий мультиметр універсальний DT9207. Границі вимірювання напруги 0.2 – 1000 В, струму 0,02 – 20 А, активного опору – 0,1 – 10 000 Ом– 2 шт.
14	Автотрансформатор змінної напруги лабораторний ЛАТР 220 /0-240 В, 50 Гц – 1 шт.
15	Реостат лабораторний BXS-150 100 Om – 1 шт.

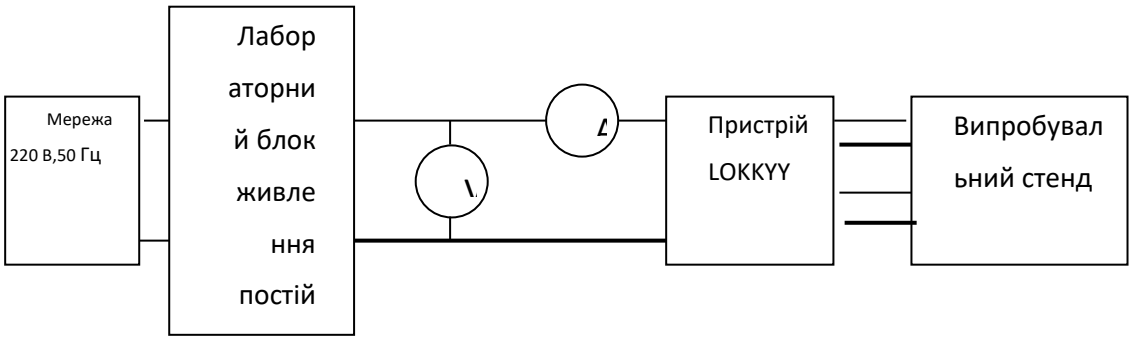


Рисунок 4.8 — Схема перевірки вимог до джерел живлення постійним струмом

Перевірку відповідності вимог до зовнішніх джерел живлення виконують з використанням регульованого лабораторного автотрансформатора ЛАТР 220 / 0-240 В, 50 Гц з окремими вольтметрами і амперметрами змінного струму, як показано на рисунку 4.9.

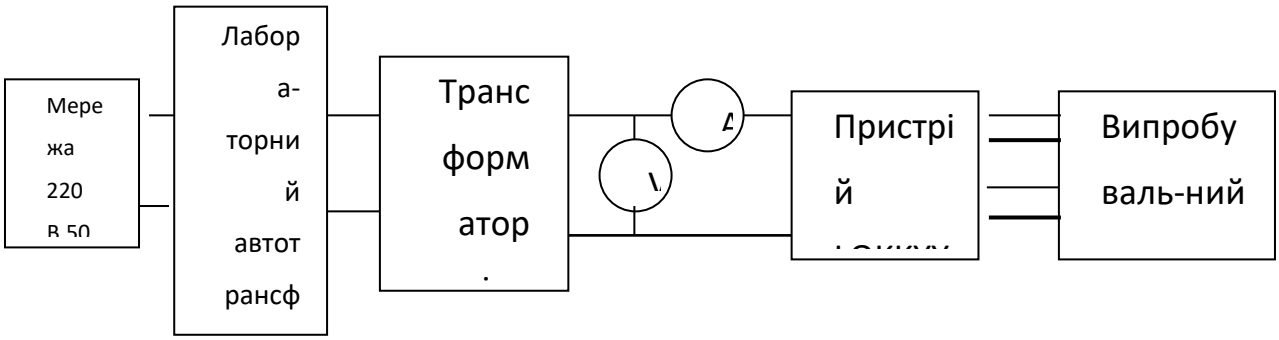


Рисунок 4.9 – Схема перевірки вимог до джерел живлення змінним струмом

Перевірку пристрою LOKKYY виконують послідовно при номінальному та крайніх значеннях напруги живлення 24 В, 9 В, 32 В в режимах спрацювання реле (відкривання). Фіксують значення відповідних напруги V (В) , струму споживання А (А), та обчислюють споживану потужність за формулою P=V*A (Вт).

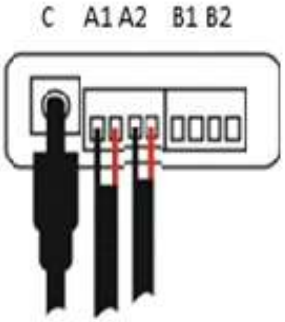
Пристрій LOKKYY вважають таким, що витримав випробування, якщо він виявився працездатним, а його струм споживання і споживана потужність відповідають технічним вимогам, при всіх значеннях напруги живлення.

Індикацією правильного функціонування модуля пристрою LOKKYY є поодиноко блимання вмонтованого світлодіодного індикатора білого кольору після підключення живлення й самоперевірки.

Скидання пристрою LOKKYY в початковий стан проводять шляхом натискання не менш ніж на 10 с кнопку перезавантаження на тильній частині модуля. При цьому, всі налаштування й паролі скидаються і пристрій LOKKYY повинен бути повторно налаштований по інтерфейсу Bluetooth зі смартфону з додатком LOKKYY APP у відповідності до підрозділу «Налаштування додатка LOKKYY APP» паспорта КМКА 001.00.00.000 ПС.

Перевірку функції керування й індикації стану комплексу LOKKYY проводять шляхом перевірки роботи додатка LOKKYY APP у відповідності до п.9.3 «Робота комплекса LOKKYY» паспорта КМКА 001.00.00.000 ПС.

Перевірку кількості та типу вихідних та вхідних ліній керування навантаженням проводять шляхом послідовного керування електроприводом випробувального стенду по першому та другому каналам керування. Для перевірки першого каналу А кабель датчика підключають до двопровідної лінії А1, а кабель управління електроприводом – до двопровідної лінії А2, як показано на рисунку 4.10.



A1, B1 – вхід для підключення кабеля управління (G)

A2, B2 – вхід для підключення датчика відкриття/закриття (C)

Рисунок 4.10 — Під’єднання вхідних і вихідних ліній каналів А і В

Для перевірки другого каналу В кабель магнітного сенсора підключають до двопровідної лінії В1, а кабель управління електроприводом – до двопровідної лінії В2.

При подачі команд керування з додатку LOKKYY APP обидва канали керування повинні правильно взаємодіяти з випробувальним стендом.

Стан контактів сенсора й контактів вихідного реле в початковому стані повинен бути розімкнений, а при спрацюванні – замкнений. Перевірка здійснюється шляхом вимірювання опору за допомогою цифрового мультиметра DT9207 чи аналогічного приладу.

Перевірку максимальної напруги й струму комутації проводять за допомогою штучного навантаження в колах керування за схемою рис. 4.9. Опір лабораторного реостата BXS-150 100 Om чи аналогічного встановлюють в значення (60+-1) Ом. Напругу на виході автотрансформатора ЛАТР 220 /0-

240 В, 50 Гц встановлюють в значення (60+-1) В, яке контролюють вольтметром V.

Значення стуму в колі навантаження при замнених контактах реле повинно складати (1,0 +- 0,01) А (при необхідності регулюють зміною опору реостата. В якості вольтметра V та амперметра А може послідовно використовуватись мультиметр DT9207, або окремі вольтметр і амперметр змінного струму.

Перевірку проводять почергово для вихідних каналів А і В. Замикання контактів реле фіксують по зростанню струму в навантаженні до 1 А.

Пристрій LOKKYY вважають таким, що пройшов перевірку, якщо у всіх з 10-ти послідовних перемикань навантаження тривалістю по 3-10 с було зафіксовано збоїв при перемиканні контактів реле.

Перевірка загального часу спрацювання комплексу LOKKYY проводиться шляхом вимірювання часу від подачі команди зі смартфона до спрацювання реле в схемі по рис. 4.9.

Для випробувань використовують два смартфони – перший з операційною системою IOS, другий - на Android. На одному зі смартфонів в додатку LOKKYY APP подаються команди керування відкриттям/закриттям пропуску, а на іншому в ці ж моменти часу запускають секундомір в системному додатку. Зупинку секундоміра й відлік часу проходження команди керування визначають за моментом реакції амперметра на спрацювання реле в схемі по рис. 4.9. Далі функції смартфонів змінють.

Для кожного смартфону і для варіантів керування за мережами Bluetooth і Інтернет через Wi-Fi проводять по 10 спроб керування.

Комплекс LOKKYY вважають таким, що пройшов перевірку загального часу спрацювання, якщо у всіх спробах для чотирьох варіантів керування час від подачі команди зі смартфона до спрацювання реле не перевищив 10 с.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Комерційний та технологічний аудит науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному випадку нового виробу, а саме комплексу мобільного керування автоматикою пропуску. Особливістю виробу є універсальність і мобільність завдяки функцірнальним можливостям контролю й керуванням через мережі Інтернет, Bluethooth, Wi-Fi за допомогою відповідного мобільного додатка. Цим забезпечується: відсутність будь-яких апаратних ключів, відсутність додаткового апаратного сервера (пристрою централізованого керування), простота надання довготривалого й короткотермінованого доступу, оперативність зміни ключів, розширена функціональність віддаленого керування й моніторингу.

Аналогом розробки є система контролю та управління доступом Evertech – 100 000 грн

Для проведення комерційного та технологічного аудиту залучають не менше 3-х незалежних експертів. Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням п’ятибальної системи оцінювання за 12-ма критеріями, у відповідності із табл. 5.1.

Таблиця 5.1 — Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Кри те-	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не	Концепція підтверджена	Концепція підтверджена	Концепція перевірена	Перевірено роботозда

Продовження табл. 5.1

Ринкові переваги					
2	Багато аналогів на малому ринку	Ринкові п Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві

Продовження табл. 5.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в таблиці 5.2

Таблиця 5.2 – Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	3	4	3
Наявність аналогів на ринку	3	4	3
Цінова політика	4	3	3
Технічні та споживчі властивості виробу	3	4	4
Експлуатаційні витрати	4	3	3
Ринок збуту	3	4	4
Конкурентоспроможність	4	3	3
Фахівці з технічної і комерційної реалізації	3	4	4
Фінансування	4	3	4
Матеріально-технічна база	3	3	3
Термін реалізації ідеї	3	3	4
Супровідна документація	3	4	3
Сума	40	42	41
Середньоарифметична сума балів	(40+42+41) / 3 = 41		

За даними таблиці 5.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці 5.3.

Таблиця 5.3 — Рівні комерційного потенціалу розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків	Рівень комерційного потенціалу розробки
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового виробу є є високим, що досягається за рахунок того, що універсальність і мобільність завдяки функцірнальним можливостям контролю й керуванням через мережі Інтернет, Bluethooth, Wi-Fi за допомогою відповідного мобільного додатка. Цим забезпечується відсутність будь-яких апаратних ключів, відсутність додаткового апаратного сервера (пристрою централізованого керування), простота надання довготривалого й короткотермінованого доступу, оперативність зміни ключів, розширена функціональність віддаленого керування й моніторингу.

5.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи

5.2.1 Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t \,, \tag{5.1}$$

де М — місячний посадовий оклад конкретного розробника, грн.;

$Т_р$ — число робочих днів в місяці, 23 днів;

t — число днів роботи розробника (дослідника).

Результати розрахунків зведемо до таблиці 5.1.

Таблиця 5.1 — Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	25000	1086,96	30	32608,696
Інженер	22000	956,52	30	28695,652
Всього				61304,35

5.2.2 Витрати на основну заробітну плату робітників ($З_р$) розраховуються на основі норм часу, які необхідні для виконання даної роботи, розраховуються за формулою:

$$З_р = \sum_{1}^{n} t_i \cdot С_i \cdot К_с , \qquad (5.2)$$

де t_i — норма часу (трудомісткість) на виконання конкретної роботи, годин;

n — число робіт по видах та розрядах;

$К_с$ — коефіцієнт співвідношень, який установлений в даний час Генеральною тарифною угодою між Урядом України і профспілками;

Сі — погодинна тарифна ставка робітника відповідного розряду, який виконує відповідну роботу, грн./год.

$С_i$ визначається за формулою:

$$С_i = \frac{М_м \cdot К_i}{Т_р \cdot Т_{зм}}, \qquad (5.3)$$

де $М_н$ — мінімальна місячна оплата праці, грн., 8000 грн. у 2024 р.

$К_i$ — тарифний коефіцієнт робітника відповідного розряду;

$T_р$ — число робочих днів в місяці, $T_р$ = 23 дні;

$T_{зм}$ — тривалість зміни, $T_{зм}$ = 8 годин.

Погодинна тарифна ставка згідно чинного законодавства у грудні 2024 року = 48 грн./год.

Розрахунки заносимо до табл. 5.5.

Таблиця 5.5 — Витрати на основну заробітну плату робітників

Найменування робіт	Трудомісткість, год.	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн.	Величина оплати робітника
Заготівельні	6	3	1,35	54,621	327,726
Слюсарно-	22	3	1,35	54,621	1201,662
Налагоджувальні	3,5	5	1,7	68,782	240,737
Всього					1476,00

5.2.2 Додаткова заробітна плата розробників, які приймали участь в розробці обладнання.

Додаткова заробітна плата прийнято розраховувати як 10% від основної заробітної плати розробників та робітників:

$$З_д = (З_{о.роз} + З_{о.роб}) \cdot 10\% /100\% \quad (5.2)$$

$$З_д = (61304,35 + 1476,00) \cdot 10\%/100\% = 6278,03 \text{ (грн.)}$$

5.2.3 Нарахування на заробітну плату розробників.

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_{о.роз} + З_{о.роб} + З_{д.}) \cdot 22\%/100\% \quad (5.3)$$

$$Н_з = (61304,35 + 1476,00 + 6278,03) \cdot 22\%/100\ \% = 14868,12\ (грн.)$$

5.2.4. Оскільки для розроблювального програмного продукту не потрібно витрачати матеріали та комплектуючи, то витрати на матеріали і комплектуючі дорівнюють нулю.

5.2.5 Амортизація обладнання, яке використовувалось для проведення розробки.

Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді амортизація обладнання, що використовувалась для розробки розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12}\ \text{[грн.]}. \qquad (5.4)$$

де Ц — балансова вартість обладнання, грн.;

Т — термін корисного використання обладнання згідно податкового законодавства, років

$t_{вик}$ — термін використання під час розробки, місяців.

Розрахуємо, для прикладу, амортизаційні витрати на комп’ютер балансова вартість якого становить 30000 грн., термін його корисного використання згідно податкового законодавства – 2 роки, а термін його фактичного використання – 1,304 міс.

$$A_{обл} = \frac{30000}{2} \times \frac{1,304}{12} = 1630,435\ грн.$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до таблиці 5.6.

Таблиця 5.6 — Амортизаційні відрахування матеріальних і нематеріальних ресурсів для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна периферія	30000	2	1,304	1630,435
Офісне обладнення (меблі)	20000	4	1,304	543,478
Приміщення	750000	20	1,304	4449,728
Всього				6623,64

Амортизація обладнання, що використовувалось робітниками, розраховується аналогічно, результати розрахунків зведено в таблицю 5.7 і враховуються при розрахунку виробничої собівартості виробу.

Таблиця 5.7 — Амортизаційні відрахування матеріальних і нематеріальних ресурсів для робітників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання		Амортизаційні відрахування, грн.
			го д.	міс.	
Комп'ютер	30000	2	3	0,0163	20,3804
Спеціалізоване обладнання (меблі)	20000	4	3	0,0163	6,7935
Приміщення	750000	20	22	0,1196	373,6413
Всього					400,8152

Так як вартість ліцензійної ОС та спеціалізованих ліцензійних нематеріальних ресурсів, а також спеціалізованого обладнання менше 20000 грн (операційна система – безкоштовно, осцилограф – 8000 грн., мультиметр

– 380грн.), то даний нематеріальний актив не амортизується, а його вартість включається у вартість розробки повністю, $B_{спец.\ обл..}$ = 11000 грн.

5.2.6. Витрати на комплектуючі

Витрати на комплектуючі, що були використані на виготовлення розраховуються за формулою

$$K = \sum_{i=1}^{n} H_i \cdot Ц_i \cdot K_i , \qquad (5.5)$$

де H_i — кількість комплектуючих i-го виду, шт.,

$Ц_i$ — роздрібна ціна комплектуючих i-го виду, грн.,

K_i — коефіцієнт транспортних витрат, K_i=1,1,

n — кількість видів матеріалів.

Проведені розрахунки зводимо до таблиці 5.8 без врахування транспортних витрат.

Таблиця 5.8 – Витрати на комплектуючі

Найменування комплектуючих	Кількість	Ціна за штуку, грн.
Мікроконтролерний модуль	1	300
Модуль Wi-FI	1	240
Модуль Bluethooth	1	160
Реле	2	40
Магнітний сенсор-кінцевик.	2	35
Кабелі	3	20
Всього		***910,00***

Витрати на комплектуючі, що були використані на розробку з врахуванням транспортних втрат:

$$H = 910 \cdot 1,1 = 1001,00 \text{ (грн.)}$$

5.2.7 Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників (енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1-й або 2-й клас). Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (5.6)$$

де В — вартість 1 кВт-години електроенергії для 1 класу підприємства з ПДВ в 2024 році для Вінницької області за даними Енера-Вінниця, В = (5635,47/1000)*1,2 = 6,76 грн./кВт;

П — встановлена середня потужність обладнання, кВт. П = 0,4 кВт;

Ф — фактична кількість годин роботи обладнання, годин.

$К_п$ — коефіцієнт використання потужності, $К_п$ = 0,8.

$$В_е = 0,8 \cdot 0,4 \cdot 8 \cdot 30 \cdot 6,76 + 0,8 \cdot 0,4 \cdot 6,0 \cdot 6,76 = 519,168 + 12,979 = $$
$$= 532,15 \text{ (грн.)}$$

5.2.8 Інші витрати та загальновиробничі витрати.

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.6)$$

де $Н_{ів}$ — норма нарахування за статтею «Інші витрати».

$$І_в = (61304,35 + 782,28) \cdot 53\% / 100\% = 33273,58 \text{ (грн.)}$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.7)$$

де $Н_{нзв}$ — норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$Н_{нзв} = (61304,35 + 1476,00) \cdot 120\% / 100\ \% = 75336 \text{ (грн.)}$$

5.2.9 Витрати на проведення науково-дослідної роботи.

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи:

$$В_{заг} = 61304,35+1476,00+6278,03+14868,12+6623,64+ 400,8152+11000+$$
$$+1001,00+532,15+33273,58+75336 = 212094,11 \text{ грн.}$$

5.2.11 Розрахунок загальних витрат на науково-дослідну (науково-технічну) роботу та оформлення її результатів.

Загальні витрати на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються *ЗВ*, визначається за формулою:

$$ЗВ = \frac{В_{заг}}{\eta} \text{ (грн)}, \quad (5.8)$$

де η — коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Так, якщо науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

$$ЗВ = 212094{,}11 / 0{,}5 = 424188 \text{ грн.}$$

5.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

В ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розробки необхідно:

а) вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

б) зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3-х років після її впровадження);

в) кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основних суб’єктів (зацікавлених осіб) цього попиту;

г) визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов’язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

— абсолютного економічного ефекту (чистого дисконтованого доходу);

— внутрішньої економічної дохідності (внутрішньої норми дохідності);

— терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором можна об’єднати, враховуючи визначені ситуації з відповідними умовами.

5.3.1 Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим споживачем.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (5.9)$$

де $\pm \Delta Ц_o$ — зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

N — кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки;

$Ц_o$ — основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_o = Ц_б \pm \Delta Ц_o$;

$Цб$ — вартість програмного продукту у році до впровадження результатів розробки;

ΔN — збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ — коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$.

p — коефіцієнт, який враховує рентабельність продукту;

ϑ — ставка податку на прибуток, у 2024 році ϑ =18%.

Припустимо, що при прогнозованій ціні *20000* грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти її ціну на *1000* грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року – на 1000 шт., протягом другого року – на 1300 шт., протягом третього року на 1500 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

$\Delta П_1$ = (0*1000 + (20000 + 1000)*1000)* 0,8333* 0,13) * (1 - 0,18) = 1776666,596 грн.

$\Delta П_2$ = (0*1000 + (20000 + 1000)*(1000+1300)* 0,8333* 0,13) * (1 - 0,18) = 4290649,828 грн.

$\Delta П_3$ = (0*1000 + (20000 + 1000)*(1000+1300+1500)* 0,8333* 0,13) * (1 - 0,18) = 7088899,716 грн.

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 13156216,14 грн.

5.3.2 Розрахунок ефективності вкладених інвестицій та періоду їх окупності.

Розраховуємо приведену вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (5.10)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т – період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0,05...0,15$;

t – період часу (в роках).

Збільшення прибутку ми отримаємо починаючи з першого року:

ПП = (1776666,596/(1+0,1)^1)+(4290649,828/(1+0,1)^2)+(7088899,716/(1+0,1)^3) = 1615151,45 + 3545991,59 + 5325995,28 = 10487138,32 грн.

Далі розраховують величину початкових інвестицій *PV*, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (5.11)$$

де $k_{інв}$ — коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;

ЗВ — загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

PV = 2 * 424188 = грн.

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід *(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \quad (5.12)$$

$$E_{абс} = 10487138,32 - 424188 = 10062950,10 \text{ грн.}$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність або показник внутрішньої норми дохідності (IRR, Internal Rate of Return) вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну

внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{5.13}$$

де $T_ж$ – життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{(1 + 10062950{,}10/\ 424188} - 1 = 1{,}913$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{5.14}$$

де d — середньозважена ставка за депозитними операціями в комерційних банках; в 2024 році в Україні d = (0,09…0,14);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{\min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{5.15}$$

$$T_{ок} = 1 / 1{,}913 = 0{,}52 \text{ р.}$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 0,52 роки, то фінансування даної наукової розробки є доцільним.

Висновки до розділу: економічна частина даної роботи містить розрахунок витрат на розробку продукту, сума яких складає 424188 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення, розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,52 роки.

ВИСНОВКИ

В комплексній магістерській кваліфікаційній роботі в апаратній її частині виконано такі завдання:

— здійснено аналіз сфер застосування систем керування доступом;

— виконано класифікацію методів дистанційного керування автоматикою пропуску;

— запропоновано комбінований метод керування з використанням безпровідних технологій;

— розроблено структурну та функціональні схеми апаратної частини комплексу;

— розроблено мікропроцесорний пристрій керування;

— розроблено методику випробувань апаратної частини комплексу;

— проведено експериментальні дослідження та визначити технічні параметри комплексу.

Розроблений пристрій керування доступом дає можливість визначати права доступу віддалено через підключення до хмарного сервера за допомогою Ethernet або Wi-Fi. Він також забезпечує доступ в офлайн-режимі за ідентифікатором, який передається зі смартфона через Bluetooth.

За матеріалами досліджень опубліковано тези доповіді [1].

Отже, всі поставлені в роботі завдання виконано, а мету роботи, яка полягає в розширенні функціональних можливостей комплексу мобільного керування доступом до об’єктів з автоматикою пропуску – досягнуто.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС МОБІЛЬНОГО ДИСТАНЦІЙНОГО КЕРУВАННЯ ДОСТУПОМ / Гуменюк В.В., Зубринська Д. Л., Крупельницький Л.В., Городецька О.С // Міжнародна науково-практична Інтернет-конференція «Молодь в науці: дослідження, проблеми, перспективи (МН2024)» (15 жовтня 2023 р.- 20 травня 2024 р., Вінниця) : Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/21172/17557

2. Системи контролю та управління доступом. [Електронний ресурс]. Режим доступу: https://evertech.ua/access-controll-systems/.

3. Технічні системи безпеки на об’єктах. [Електронний ресурс]. Режим доступу: https://karabiner.ua/ua/stati/tehnicheskie-sistemy-bezopasnosti-na-obektah/

4. Системи контролю і управління доступом від А до Я. [Електронний ресурс]. Режим доступу: https://deps.ua/ua/knowegable-base/referenceinformation/7824.html.

5. Системи контролю та управління доступом. [Електронний ресурс]. Режим доступу https://www.rim2000.com/equipment/networks/access-control/.

6. СКУД - система контролю та управління доступом. [Електронний ресурс]. Режим доступу: http://www.centrebespek.com/articles/ELEMENT_ID_14787/.

7. Gean Davis Breda New Era of Mobile Access Control System / Gean Davis Breda, Raul Mariano Cardoso, Felipe André Cordeiro Pirotta // International Journal of Computer Science and Network Security, VOL.15, No.8, 2015, P. 6 – 15.

8. Rajashree S. Bluetooth and NFC Enabled Contactless Access Control System / S.Rajashree, S. Kaushik, K. Varman // ScieXplore: International Journal of Research in Science, 2015, № 2, P. 1 - 32.

9. NFC: розумні мітки. [Електронний ресурс]. Режим доступу:https://itc.ua/articles/nfc_umnye_metki_53544/.

10. Бідюк П. Сучасні методи біометричної ідентифікації / Петро Бідюк, Володимир Бондарчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2009. Випуск 1(18). С. 137 - 146.

11. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних закладів] / Р.Ю. Царьов, Т. М. Лемеха. - Одеса: ОНАЗ ім. О.С. Попова, 2016. - 140 с.

12. Контролер доступу NDC F18IP(U-Prox IP400). [Електронний ресурс].
Режим доступу: https://www.forter.com.ua/kontrollery-dostupa/u-prox-ip-400/.

13. Зчитувач-контролер SameKey Card Control. [Електронний ресурс]. Режим доступу: https://secur.ua/kontroller-schityvatel-samekey-card-control.html.

14. Комплекс мобільного керування автоматикою пропуску LOKKYY [Електронний ресурс]. Режим доступу: https://lokkyy.com/#about.

15. GSM. [Електронний ресурс]. Режим доступу: http://www.smartphone.ua/w_gsm.html.

16. GSM-модуль RC-25 - пристрій для управління автоматикою воріт і шлагбаумів з мобільного телефону. [Електронний ресурс]. Режим доступу: https://novi-vorota.com.ua/ua/avtomatika-gsm-module.html.

17. Дистанційне управління зі смартфона з WI-FI, Bluetooth, LTE, GSM. [Електронний ресурс]. Режим доступу: https://dtb.com.ua/ua/g91671568upravlenie-smartfona-kanalam.

18. Протокол передачs гіпертекста. [Електронний ресурс]. Режим доступу: https://developer.mozilla.org/ua/docs/Web/HTTP/Overview.

19. Що таке NFC в смартфоні? Для чого потрібна функція NFC і як цим користуватися? [Електронний ресурс]. Режим доступу: https://mixfin.com/ua/blog/shcho-take-nfc

20. Bluetooth Technology Overview. [Електронний ресурс]. Режим доступу:https://www.bluetooth.com/learn-about-bluetooth/tech-overview/.

21. Створення безпечної аутентифікації користувачів у веб-додатках. [Електронний ресурс]. Режим доступу: https://redstone.media/stvorennya-bezpechnoyi-autentifikaciyi-koristuvachiv-u-veb-dodatkah

22. Ідентифікація, автентифікація та авторизація — як не передати керування доступами зловмисникам. [Електронний ресурс]. Режим доступу: https://thekernel.ua/identyfikatsiia-avtentyfikatsiia-ta-avtoryzatsiia/

23. Організація бездротових мереж. [Електронний ресурс]. Режим доступу: https://sez.net.ua/organizaciya-komp-yuternyh-setej-38-2.html

24. Комп’ютерні мережі : підручник / Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.. − Вінниця : ВНТУ, 2020, 378 с.

25. Огляд технології Ethernet. [Електронний ресурс]. Режим доступу: https://bg.net.ua/content/obzor-tekhnologii-ethernet.

26. Wi-Fi технології: основи, принципи роботи та сучасні тенденції розвитку [Електронний ресурс]. Режим доступу: https://cudy.com.ua/wi-fi-istoriya-tehnologiya-ta-perspektyvy-rozvytku/

27. . В. Паровишник Wi-Fi - розвиток і основні принципи найпоширенішого стандарту бездротових мереж [Електронний ресурс]. https://ua.gecid.com/netlan/wi-fi_-_razvitie_i_osnovnyee_prinjipye_samogo_rasprostranennogo_standarta_bespro

vodnyeh_seteyi/ Режим доступу: https://www.lessons-tva.info/articles/net/003.html.

28. М. Потужна Все, що потрібно знати про бездротові мережі WLAN: побудова, безпека та керування [Електронний ресурс]. Режим https://netwave.ua/vse-shcho-potribno-znaty-pro-bezdrotovi-merezhi-wlan-pobudova-bezpeka-ta-keruvannya/

29. Лящук О. М. Безпровідні мережі. Стандарт ZigBee. / О. М. Лящук // Вісник Національного технічного університету України «КПІ», №44, 2011, С. 157 – 163.

30. Види і призначення електромагнітного реле, пристрій і принцип роботи, переваги і недоліки. [Електронний ресурс]. Режим доступу: https://sitemasters.com.ua/elektroobladnannja/vidi-i-priznachennja-elektromagnitnogorele/

31. Рожненко Ж. Г. Використання мікропроцесорів на базі arm cortex в електромеханіці / Ж. Г. Рожненко, О. К. Данилейко, Г.В. Коломіц, А. В. Ятчук // Гірничий вісник, вип. 109, 2021, С. 98 – 106.

32. STM32: Епоха 32-бітних мікроконтролерів настала. [Електронний ресурс]. Режим доступу: http://www.kosmodrom.com.ua/data/stm32/stm32new.php.

33. Наладжувальна плата STM32F407VET6-Mini. [Електронний ресурс]. Режим доступу: http://www.kosmodrom.com.ua/el.php?name=STM32F407VET6-Mini.

34. STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced Arm-based 32-bit MCUs. [Електронний ресурс]. Режим доступу: https://www.st.com/resource/en/reference_manual/dm00031020-stm32f405-415stm32f407-417-stm32f427-437-and-stm32f429-439-advanced-arm-based-32-bit-mcusstmicroelectronics.pdf.

35. Ethernet модуль DP83848 Waveshare. [Електронний ресурс]. Режим доступу: https://miniboard.com.ua/modules/764-ethernet-modul-dp83848waveshare.html.

36. ESP8266: мікросхема Wi-Fi. [Електронний ресурс]. Режим доступу: http://microsin.net/adminstuff/hardware/esp8266-wifi-ic.htm.

37. Wi-Fi модуль ESP8266 версія ESP-07. [Електронний ресурс]. Режим доступу: https://arduino.ua/prod1444-wi-fi-modyl-esp8266-versiya-esp-07.

38. Модуль Bluetooth HC-05. [Електронний ресурс]. Режим доступу: https://foton.ua/catalog/arduino/modul-bluetooth-hc-05.html

39. PCB Relay G2RL. . [Електронний ресурс]. Режим доступу: http://www.kosmodrom.com.ua/pdf/G2RL.pdf.

40. BC817 45 V, 500 mA NPN general-purpose transistors. [Електронний ресурс]. Режим доступу: https://assets.nexperia.com/documents/datasheet/BC817_SER.pdf.

41. 4 PIN DIP PHOTOTRANSISTOR PHOTOCOUPLER Everlight Electronics Co., Ltd. 1 http://www.everlight.com Document No : DPC-0000046 Rev.10 April, 21 2010 EL817 Series

42. React Native init VS Expo [Електронний ресурс]. Режим доступу: https://habr.com/ru/post/480258/

ДОДАТОК А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

проф., д.т.н.. Азаров О.Д.

" ____ " _____ 2024 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання комплексної магістерської кваліфікаційної роботи

"Комплекс мобільного керування автоматикою пропуску".

Частина 1. "Апаратна частина"

08-54.КМКР.007.00.000 ТЗ

Науковий керівник: доцент к.т.н.

_____ Городецька О.С.

Виконав: студент групи КІ-22мз

_____ Гуменюк В.В..

ВНТУ 2024

1 Підстава для виконання магістерської кваліфікаційної роботи (МКР) - наказ по ВНТУ № 81 від 11.03.2024 р.

1.1 Необхідність побудови гнучкої та легко впроваджувальної системи віддаленого керування правами доступу з підтримкою можливості надання доступу в автономному режимі з використанням технологій мобільної ідентифікації.

1.2 Наказ про затвердження теми МКР.

2 Мета МКР і призначення розробки

2.1 Мета робота — розширення функціональних можливостей системи віддаленого керування доступом через веб-інтерфейс за рахунок підтримки можливості роботи в офлайн режимі;

2.1 Призначення розробки — визначення підходів до побудови апаратних та програмних засобів системи віддаленого керування доступом через вебінтерфейс.

3 Вихідні дані для виконання МКР

3.1 Функціональне призначення — віддалене керування доступом з використанням хмарних та мобільних технологій;

3.2 Організація доступу - за ідентифікатором, що надсилається зі смартфону або планшету;

3.3 Реєстрація в системі — відділена через веб-інтерфейс;

3.4 Інтерфейси - Ethernet, WI-FI та Bluetooth;

3.5 Протоколи - TCP/IP, HTTP, Bluetooth;

3.6 Вихід контролера — 2 комутовані канали потужністю до 4 КВт;

3.7 Вхід контролера — 2 оптично розв′язані канали;

3.8 Живлення контролера — джерело постійної напруги +5 В потужністю до 3 Вт.

4 Вимоги до виконання МКР

4.1 Провести обґрунтування доцільності розробки;

4.2 Провести аналіз сучасних технологій управління доступом;

4.3 Визначити підходи до реалізації апаратних та програмних засобів системи віддаленого керування доступом через веб-інтерфейс з підтримкою можливості роботи в режимі офлайн;

Оцінити комерційний потенціал розробки.

5 Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз сучасних сучасних технологій управління доступом	15.03.2024	20.03.2024	Вступ Розділ 1
2	Огляд принципів та технологій віддаленого керування доступом	21.03.2024	28.03.2024	Розділ 2
3	Розробка структурної схеми	01.04.2024	18.04.2024	Розділ 3.1,
4	Аналіз технологій можливої реалізації	19.04.2024	27.04.2024	Розділ 3.2
5	Розробка і тестування системи та її компонентів. Розробка схеми	18.05.2024	27.05.2024	Розділ 3,4 Блок схеми пристрою додатки

	електричної принципової			
6	Оцінка комерційного потенціалу розробки	28.05.2024	30.05.2024	Розділ 5
7	Оформлення пояснювальної записки, графічного матеріалу і презентації	01.06.2024	04.06.2024	Пояснювальна записка, графічний матеріал, презентація

6 Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами, довідка про відповідність оформлення МКР діючим вимогам.

7 Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання МКР

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення т правила складання»;

— Методичні вказівки до виконання магістерських кваліфікаційних робіт студентами спеціальності 123 «Комп'ютерна інженерія». / Укладачі О.Д. Азаров, О.В. Дудник, С.І. Швець − Вінниця : ВНТУ, 2023. − 57 с.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21».

ДОДАТОК Б

Схема комплексу дистанційного керування доступом

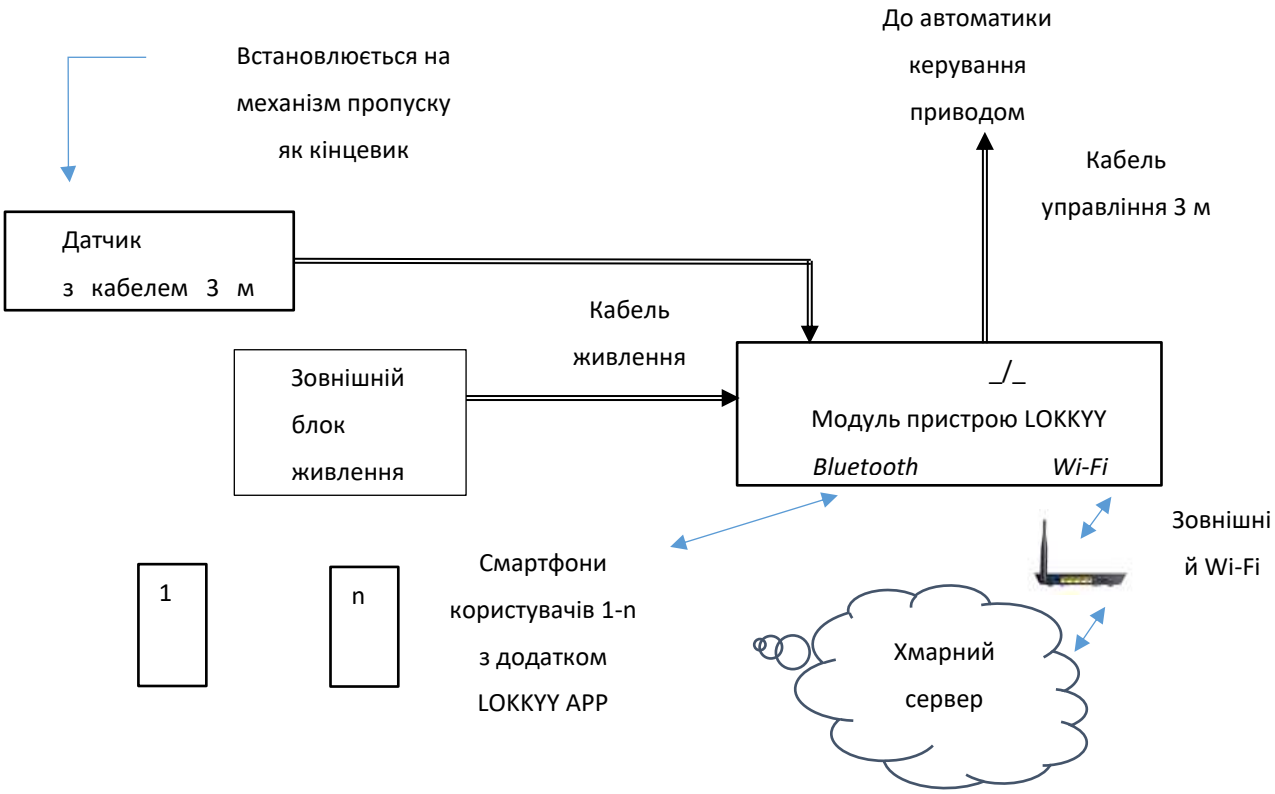


Рисунок Б.1 — Схема керування доступом

ДОДАТОК В

Структурна схема контролера керування доступом

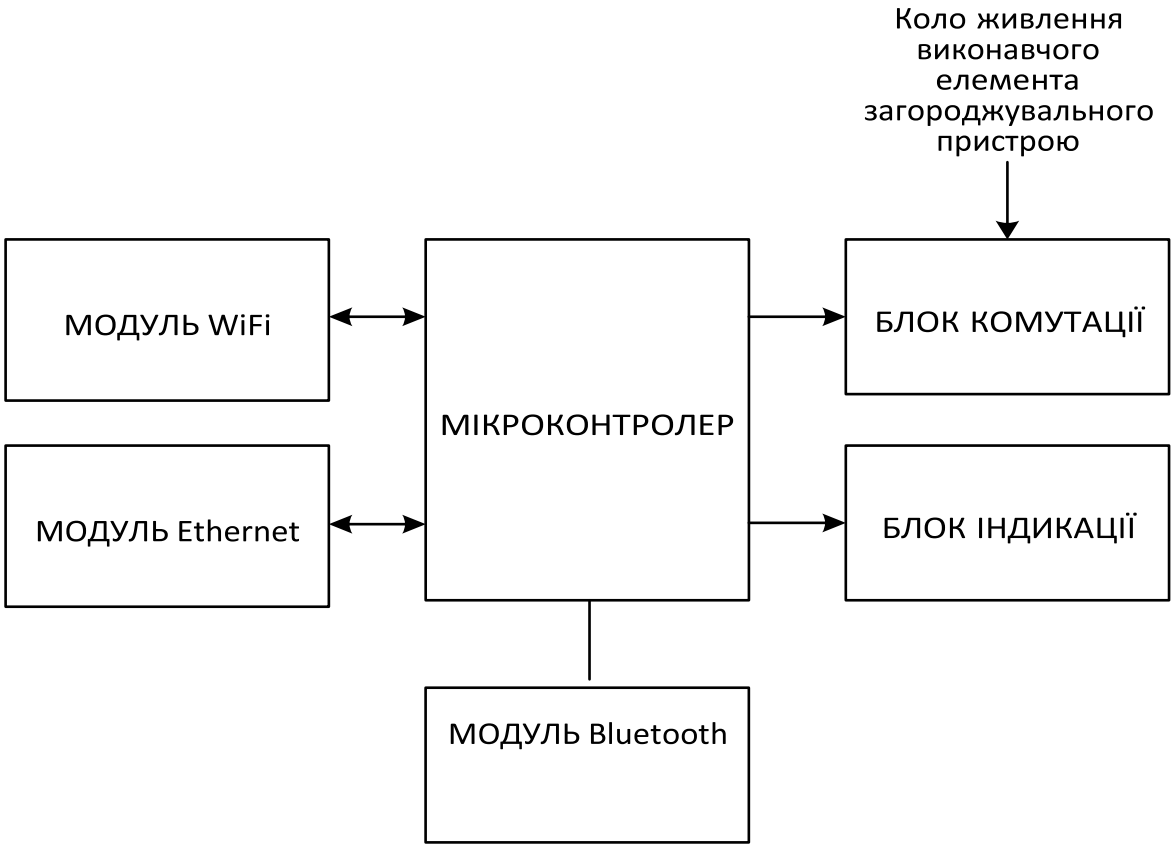


Рисунок В.1 — Структурна схема контролера керування доступом

ДОДАТОК Г

Функціональна схема контролера керування доступом

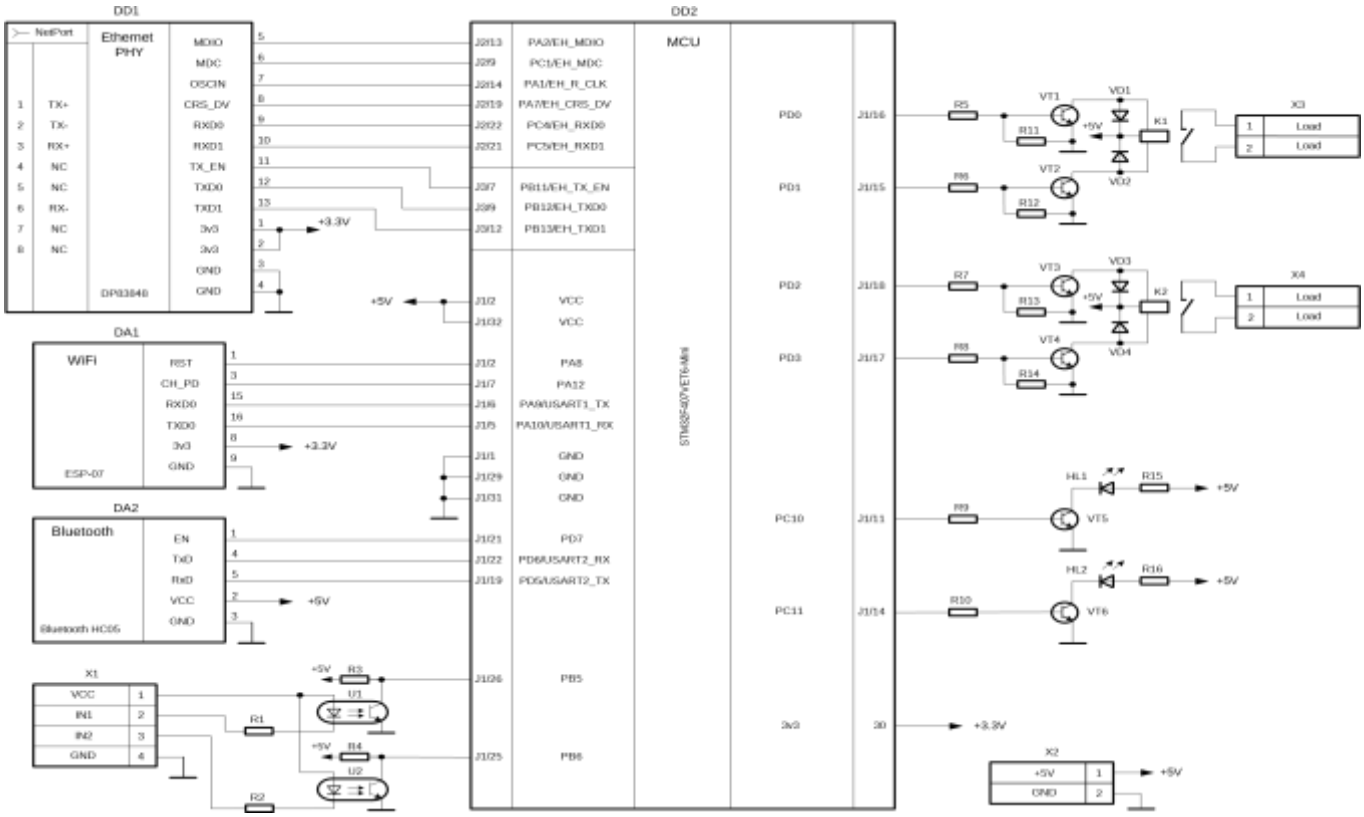


Рисунок Г.1 — Функціональна схема контролера керування доступом

ДОДАТОК Д

Блок-схема алгоритму роботи контролера доступу

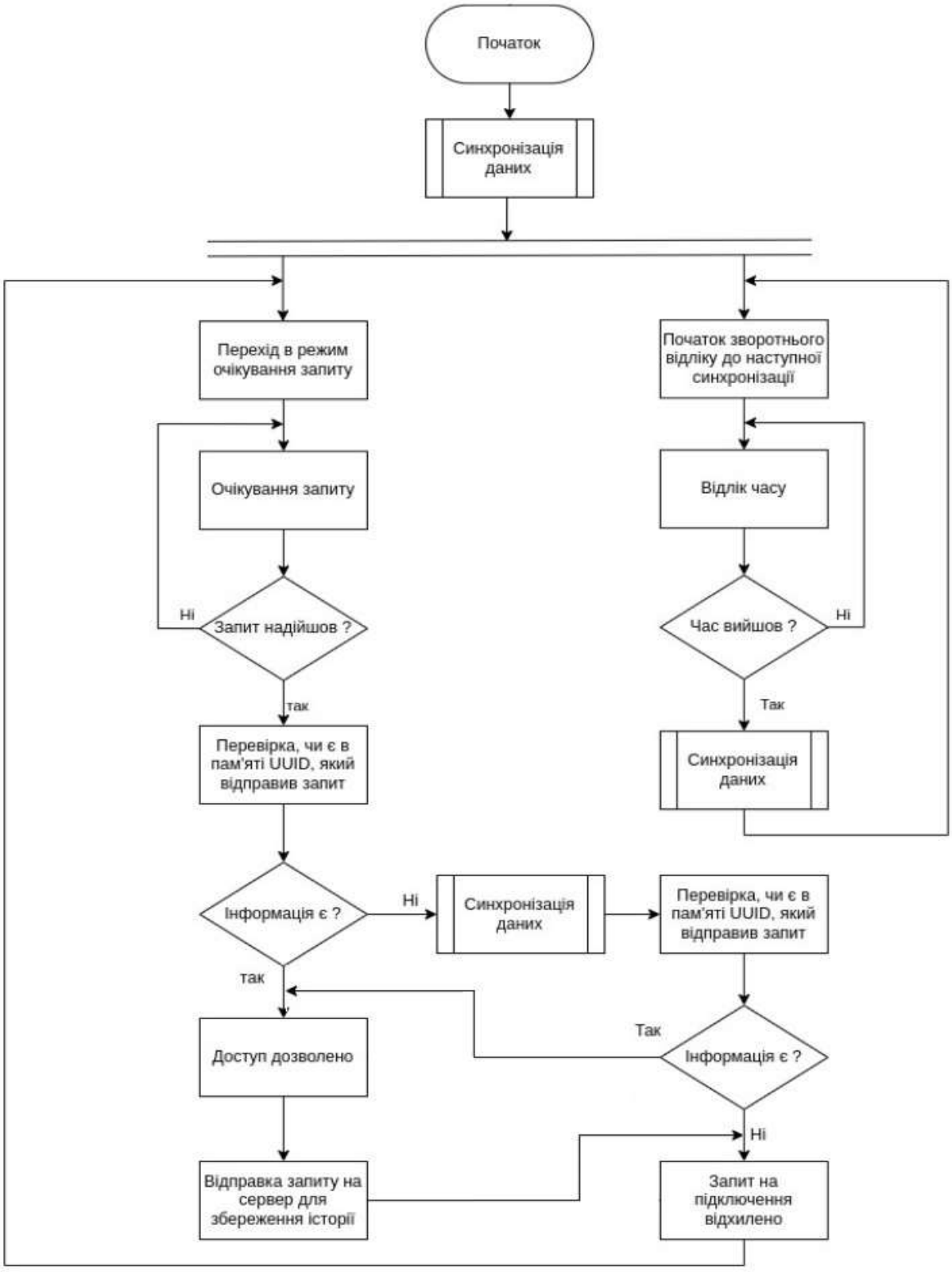


Рисунок Д.1 — Блок-схема алгоритму роботи контролера доступу

ДОДАТОК Е

Склад апаратної частини комплексу

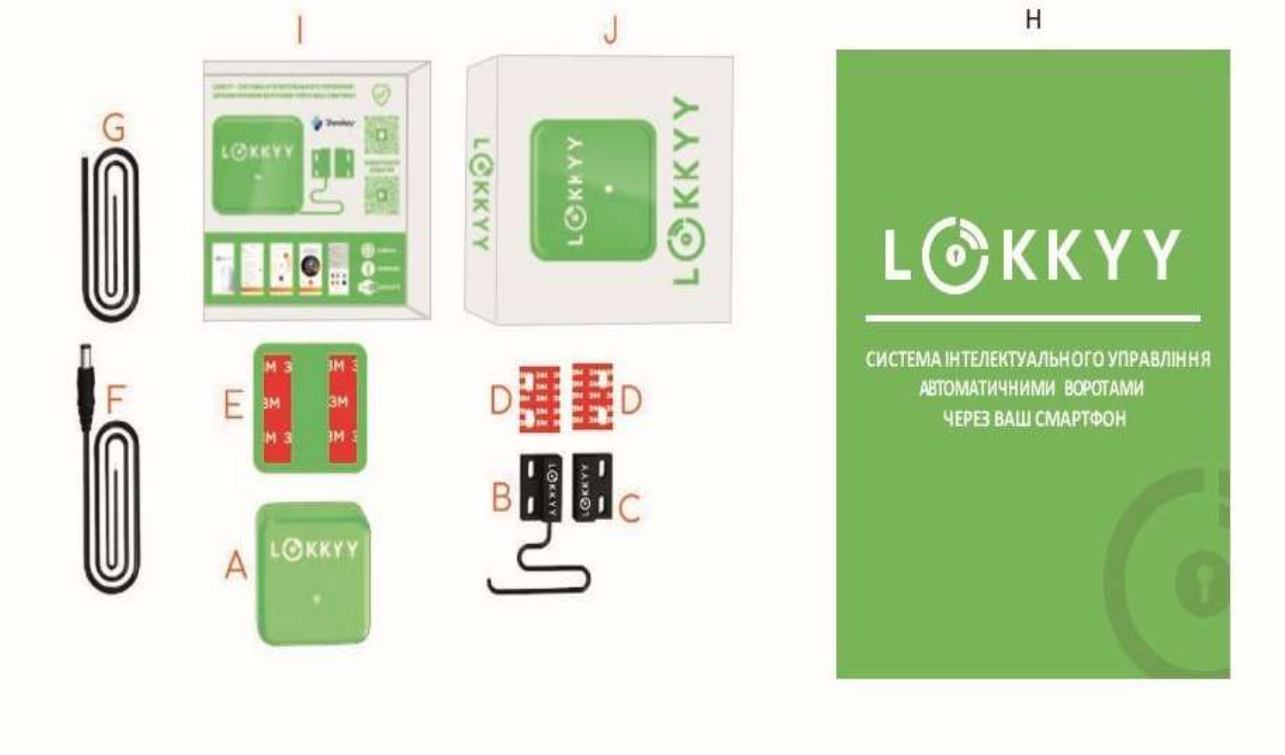


Рисунок Е1. Склад апаратної частини комплексу

ДОДАТОК Ж

Основні технічні параметри

1) кількість вихідних ліній керування навантаженням — 4 (2 канали);

2) тип виходів — гальванічно розв’язані нормально розімкнені контакти електромагнітного реле;

3) кількість вхідних ліній контролю — 4 (2 канали).

4) тип сенсорів контролю – магнітні герконові, нормально розімкнені, встановлюються як кінцевики закритого положення пропускного механізму;

5) сигнал спрацювання на лініях контролю — замикання на «землю». Захист від перешкод на лініях контролю і від «брязкання контактів».

6) загальний час спрацювання від подачі команди зі смартфона до спрацювання реле — від 0,1 с до 10 с;

7) в пристрій КМКАП вмонтовані безпровідні інтерфейси зв’язку — Bluetooth SIG version 5.0 (від 2,402 ГГц до 2,480 ГГц); Wi-Fi 802.11 b/g (від 2,4000 ГГц до 2,4835 ГГц);

8) номінальна напруга живлення — 24 В, струм споживання — до 0.1 А.

ДОДАТОК И

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: ____Комплекс мобільного керування автоматикою пропуску". Частина 1. "Апаратна частина_____

Тип роботи: комплексна магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 88.7% Схожість 11.3 %

Аналіз звіту подібності (відмітити потрібне):

✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.

□ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи Гуменюк В.В.
(підпис) (прізвище, ініціали)

Керівник роботи Городецька О.С.
(підпис) (прізвище, ініціали)