Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Перший (бакалаврський)
(рівень вищої освіти)

Розроблення системи автоматизації для контролю доступу до охоронюваної зони з використанням технологій IoT
(тема)

Виконав:
студент 4 курсу, групи АКТСІ -21-2
Маруніч Р.В.
(прізвище, ініціали)
Спеціальності 151 Автоматизація та комп`ютерно-інтегровані технології
(код і повна назва спеціальності)
Тип програми Освітньо-професійна
(освітньо–професійна або освітньо–наукова)
Освітня програма Системна інженерія
(повна назва освітньої програми)
Керівник доц. Сотник С.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри КІТАР _____ Невлюдов І. Ш.
(підпис) (прізвище, ініціали)

2025 р.

Я , Маруніч Ростислав Валерійович, як здобувач вищої освіти ХНУРЕ, розумію і підтримую політику закладу із академічної доброчесності. Я не надавав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Я не використовував штучний інтелект для підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на віповідне джерело.

"26" травня 2025 р  Маруніч Р.В.

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Факультет АКТ
Кафедра КІТАР
Рівень вищої освіти перший (бакалаврський)
Спеціальність 151 Автоматизація та комп'ютерно-інтегровані технології
Тип програми Освітньо-професійна
Освітня програма Системна інженерія
(шифр і назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«19» травня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Марунічу Ростиславу Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення системи автоматизації для контролю доступу до охоронюваної зони з використанням технологій IoT
Затверджена наказом по університету від 19.05.2025 р. №391 Ст
2. Термін подання студентом роботи до екзаменаційної комісії
3. Вихідні дані до роботи Площа охоронюваної зони (600 кв.м), кількість точок доступу/входів (1), максимальна кількість користувачів системи (50-100 осіб), рівні доступу, режими роботи, вимоги до часу відгуку системи (не більше 15 секунд)

4. Перелік питань, що потрібно опрацювати в роботі
4.1 Вступ
4.2 Аналіз предметної області
4.3 Архітектура та алгоритми симуляції IoT-Середовищ
4.4 Розроблення систем автоматизації для контролю доступу до охоронюваної зони з використанням технології IoT
4.5 Вибір апартної платформи
4.6 Розробка макетів Wokwi та Python веб-застосунку
4.7 Висновки та перелік джерел посилань

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

Демонстраційний матеріал, представлений у форматі презентації PowerPoint (*.ppt) – 12 с. формату А4

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Приміт–ка
1	Аналіз технічного завдання	16.11.2024	Виконано
2	Розробка класифікації IoT та охоронних засобів для системи	20.12.2024	Виконано
3	Опис етапів проектування системи автоматизации для охоронної системи з використанням технології IoT	05.02.2025	Виконано
4	Розробка структурної схеми системи	10.03.2025	Виконано
5	Вибір апаратної платформи та компонентів системи	13.04.2025	Виконано
6	Програмна реалізація системи	29.05.2025	Виконано
7	Оформлення пояснювальної записки	10.06.2025	Виконано

Дата видачі завдання 15.11.2024

Студент _____ Маруніч Р.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доц. Сотник С. В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить: 126 с., 6 табл., 47 рис., 6 дод., 16 джерел.

IOT, ESP32, WOKWI, NFC, БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ, СИСТЕМАКОНТРОЛЮ ДОСТУПУ, MICROPYTHON, ТЕЛЕГРАМ-БОТ, ОХОРОНЮВАНА ЗОНА.

Мета роботи – покращення ефективності управління безпекою за рахунок симуляційної моделі системи автоматизації контролю доступу до охоронюваної зони.

Об’єкт розробки – процес ідентифікації користувачів для надання або заборони доступу до охоронюваної зони.

Предмет розробки – система автоматизації контролю доступу з використанням апаратних і програмних засобів IoT.

У кваліфікаційній роботі бакалаврського рівня наведено аналіз сучасних IoT-технологій для реалізації автоматизованих систем доступу, обґрунтовано вибір архітектури, алгоритмів та апаратної платформи. Розглянуто можливості інтеграції системи з Telegram-ботом для віддаленого сповіщення про події. Описано процес створення симуляційної моделі у середовищі Wokwi та її тестування з використанням контролера ESP32, Arduino Uno, Raspberry Pi Pico W та MicroPython. Створено веб-додаток з API для інтеграції виявлення повітряної тривоги у регіоні.

Отримані результати можуть бути використані для підвищення безпеки промислових об’єктів, офісних приміщень, приватного житла та інших об'єктів, що потребують обмеження доступу сторонніх осіб.

ABSTRACT

The explanatory note contains: 126 pp., 6 tab., 47 fig., 6 app., 16 sources.

IOT, ESP32, WOKWI, NFC, BIOMETRIC IDENTIFICATION, ACCESS CONTROL SYSTEM, MICROPYTHON, TELEGRAM BOT, PROTECTED AREA.

The purpose of the study is to improve the efficiency of security management by means of a simulation model of the automation system for controlling access to a protected area.

Object of research – the process of identifying users to grant or deny access to a protected area.

The subject of development is an access control automation system using IoT hardware and software.

The bachelor's thesis provides an analysis of modern IoT technologies for the implementation of automated access systems, substantiates the choice of architecture, algorithms and hardware platform. The possibilities of integrating the system with a Telegram bot for remote event notification are considered. The process of creating a simulation model in the Wokwi environment and its testing using the ESP32 controller, Arduino Uno, Raspberry Pi Pico W, and MicroPython is described. A web application with an API was created to integrate airborne alarm detection in the region.

The results obtained can be used to improve the security of industrial facilities, office premises, private housing and other facilities that require restricted access by unauthorised persons.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AES – Advanced Encryption Standard;

AI – Artificial Intelligence;

AWS – Amazon Web Services;

BLE – Bluetooth Low Energy;

GPS – Global Positioning System;

IoT – Internet of Things;

LoRa – Long Range;

ML – Machine Learning;

NFC – Near Field Communication;

PIN – Personal Identification Number;

RFID – Radio Frequency Identification;

UI – User Interface;

Wi-Fi – Wireless Fidelity.

ВСТУП

Інтернет речей (IoT) – це революційна технологія, яка відкриває нові можливості для підвищення ефективності, автоматизації та безпеки в різних галузях. IoT базується на інтеграції сенсорів, обчислювальних пристроїв і мережевих технологій, що дозволяє у реальному часі здійснювати збір, обробку та аналіз даних. Така взаємодія забезпечує можливість створення систем, які автоматично реагують на зовнішні фактори, оптимізують процеси і приймають рішення без втручання людини.

Однією з ключових сфер застосування IoT є безпека. У сучасних умовах, коли ризики порушення безпеки значно зросли, важливість автоматизованих систем доступу є надзвичайно високою. IoT дозволяє створювати рішення, які забезпечують контроль над доступом до об'єктів, моніторинг територій та інтеграцію різних підсистем в єдине середовище. Наприклад, такі системи можуть включати інтелектуальні замки, камери з функцією розпізнавання облич, датчики руху та централізовані системи управління доступом.

Актуальність обраної теми пояснюється не лише швидким розвитком технологій IoT, а й їх значенням для покращення ефективності та безпеки у сучасному світі. Впровадження IoT у сферу охорони дозволяє знизити залежність від людського фактору, зменшити витрати та підвищити рівень контролю. Наприклад, автоматизовані системи можуть працювати безперервно 24/7, миттєво реагуючи на зміни ситуації та потенційні загрози.

Особливо важливо зазначити, що автоматизовані системи доступу, які базуються на IoT, мають широкий спектр застосувань. Вони можуть бути використані у приватних будинках, офісах, промислових підприємствах, державних установах та на стратегічно важливих об’єктах. Наприклад, у промисловості такі системи дозволяють обмежувати доступ до виробничих зон, забезпечуючи захист як обладнання, так і персоналу. В установах державного значення IoT-технології використовуються для моніторингу й аналізу потенційних загроз у реальному часі.

Однак впровадження IoT не позбавлене викликів. Серед основних проблем – забезпечення кібербезпеки, висока вартість обладнання та складність інтеграції з існуючими системами. Дані, які передаються через IoT-системи, є цінною інформацією, тому захист від несанкціонованого доступу є критично важливим аспектом. Крім того, питання енергоефективності пристроїв, які часто працюють у безперервному режимі, також потребує уваги.

Розробка систем на основі IoT не тільки відповідає потребам сьогодення, а й закладає фундамент для подальшого розвитку інноваційних рішень у сфері автоматизації та безпеки. Отримані результати можуть бути використані як у приватному секторі, так і в масштабних промислових або державних проектах.

Таким чином, обрана тема є актуальною, практично значущою та спрямованою на вирішення сучасних викликів, які постають перед суспільством у сфері безпеки.

Метою роботи – покращення ефективності управління безпекою за рахунок симуляційної моделі системи автоматизації контролю доступу до охоронюваної зони.

Об'єкт роботи – процес ідентифікації користувачів для надання або заборони доступу до охоронюваної зони.

Предмет роботи – система автоматизації контролю доступу з використанням апаратних і програмних засобів IoT.

Для досягнення мети було визначено наступні завдання:

– огляд можливостей застосування IoT;

– аналіз сучасних IoT-технології для створення систем автоматизації доступу;

– аналіз існуючих систем контролю доступу;

– оформити кваліфікаційну роботу згідно ДСТУ 3008:2015 [1], а також з методичними вказівками з підготовки й оформлення кваліфікаційної роботи здобувачами першого (бакалаврського) рівня вищої освіти спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» освітньої програми «Системна інженерія» [2] з дипломним проєктуванням для студентів усіх форм навчання .

Отримані результати роботи можна віднести до Цілі сталого розвитку 9 “Промисловість, інновації та інфраструктура”, а саме п. 9.4 “Сприяти прискореному розвитку високо- та середньо-високотехнологічних секторів переробної промисловості, які формуються на основі використання ланцюгів «освіта – наука – виробництво» та кластерного підходу за напрямами: розвиток інноваційної екосистеми”, індикатор 9.4.1.

За результатами роботи було опубліковано тези доповіді у збірнику університету [3-4] та наукову статтю у науково-технічному журналі [5].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз сучасних IoT-технології для створення систем автоматизації доступу

Сучасний розвиток Інтернету речей значно вплинув на сферу автоматизації доступу, змінюючи традиційні методи ідентифікації та контролю на сучасні високотехнологічні рішення. Завдяки IoT сьогоднішні автоматизовані системи доступу не лише підвищують безпеку, але й забезпечують зручність для користувачів, адаптуючись до їхніх потреб і вподобань. Інтеграція різних технологій у цій галузі, таких як RFID (Radio Frequency Identification), NFC (Near Field Communication), біометрія, штучний інтелект, блокчейн та хмарні сервіси, дозволяє створювати комплексні системи, здатні вирішувати задачі будь-якої складності [6].

Однією з ключових технологій, що лежать в основі автоматизованих систем доступу, є RFID. RFID-системи працюють на основі радіочастотного зв'язку між міткою та зчитувачем. Завдяки цій технології пристрої можуть ідентифікувати об’єкти та людей на відстані, що значно прискорює і спрощує процес доступу. Наприклад, на підприємствах RFID використовується для контролю доступу співробітників до виробничих зон, тоді як у логістичних центрах ця технологія забезпечує відстеження переміщення товарів. Сучасні RFID-системи інтегруються з IoT-платформами, що дозволяє в реальному часі моніторити всі дії та забезпечувати оперативний контроль.

NFC є еволюцією RFID і дозволяє обмінюватися даними на коротких відстанях (рис. 1.1). Ця технологія особливо популярна завдяки своїй інтеграції зі смартфонами. Наприклад, багато сучасних готелів впроваджують системи доступу на основі NFC, де гості можуть використовувати свої мобільні телефони як цифрові ключі. Це не лише полегшує процес реєстрації, але й підвищує безпеку, оскільки кожен ключ [7] прив'язується до конкретного користувача, і його неможливо втратити або вкрасти. У комерційних будівлях NFC-системи

використовуються для ідентифікації співробітників і надання їм доступу до різних зон офісу.

Рисунок 1.1 – NFC використання

Біометричні системи доступу є одним із найнадійніших методів ідентифікації, оскільки базуються на унікальних фізичних характеристиках людини. Технології розпізнавання обличь, відбитків пальців і навіть сітківки ока сьогодні активно впроваджуються в автоматизовані системи доступу. Наприклад, у банківських установах системи розпізнавання обличь використовуються для забезпечення доступу до сховищ, гарантуючи, що лише уповноважені особи можуть потрапити до критично важливих зон. Технологія розпізнавання обличь інтегрується зі штучним інтелектом, що дозволяє не лише ідентифікувати користувача, але й аналізувати його поведінку, виявляючи потенційні загрози.

Bluetooth Low Energy (BLE) також активно використовується у сучасних системах доступу. Ця технологія дозволяє створювати бездротові мережі з низьким енергоспоживанням, які ідеально підходять для роботи з мобільними пристроями. Наприклад, розумні замки з підтримкою BLE автоматично відкриваються, коли власник телефону з авторизованим додатком наближається

до дверей. Це забезпечує не лише зручність, але й додатковий рівень безпеки, оскільки доступ можливий лише через авторизований пристрій.

Хмарні платформи стали невіддільною частиною IoT-систем доступу, оскільки вони забезпечують централізоване управління та аналіз даних. Наприклад, хмарні рішення дозволяють адміністраторам великих бізнес-центрів у реальному часі відстежувати стан систем доступу, оновлювати права користувачів та аналізувати журнали доступу. У разі виникнення підозрілої активності хмарна система може автоматично заблокувати доступ і сповістити службу безпеки. Це значно підвищує рівень захищеності об’єктів і забезпечує гнучкість у керуванні системою.

Інтеграція блокчейн-технологій у системи доступу відкриває нові горизонти для забезпечення прозорості та безпеки. Завдяки блокчейну всі операції, пов'язані з доступом, реєструються в незмінному реєстрі, що унеможливлює фальсифікацію даних. Наприклад, у великих фінансових установах використання блокчейну дозволяє створювати журнал доступу до приміщень, де кожен запис зашифрований і зберігається у децентралізованій мережі. Це забезпечує високий рівень достовірності даних і виключає можливість їх підробки.

Штучний інтелект і машинне навчання додають інтелектуальності сучасним системам доступу. Завдяки цим технологіям системи можуть аналізувати поведінку користувачів і виявляти потенційні загрози. Наприклад, якщо користувач зазвичай входить до будівлі в певний час, але раптом починає намагатися отримати доступ у незвичайний період, система може вимагати додаткової авторизації або навіть заблокувати спробу доступу. Штучний інтелект також використовується для прогнозування загроз на основі аналізу історичних даних, що дозволяє запобігати порушенням ще до їхнього виникнення.

Інтеграція відеоаналітики з IoT-системами доступу є ще одним важливим напрямком розвитку цієї галузі. Камери, оснащені алгоритмами штучного інтелекту, можуть аналізувати поведінку людей і виявляти аномалії. Наприклад, якщо камера виявляє, що людина намагається потрапити до будівлі через вікно, система може автоматично активувати сигналізацію і заблокувати всі двері. Це

значно підвищує рівень безпеки і знижує необхідність у ручному моніторингу [8-12].

Протоколи зв’язку, такі як ZigBee і LoRa, забезпечують ефективну передачу даних у системах доступу, особливо на великих територіях. Наприклад, у великих сільськогосподарських комплексах ці протоколи використовуються для управління доступом до різних зон, таких як склади чи виробничі ділянки. Завдяки низькому енергоспоживанню ці протоколи ідеально підходять для пристроїв, які працюють від батарей, забезпечуючи надійну роботу навіть у віддалених районах.

Усі ці технології поєднуються у комплексних IoT-рішеннях, які забезпечують високу безпеку, зручність і гнучкість у використанні. Сучасні автоматизовані системи доступу активно впроваджуються не лише в комерційних об’єктах, але й у житлових будинках, транспортних вузлах та навіть у розумних містах. Це дозволяє створювати середовище, де безпека поєднується з комфортом і технологічною інноваційністю.

Таким чином, аналіз сучасних IoT-технологій для створення систем автоматизації доступу показав, що використання таких рішень, як RFID, NFC, біометричні сенсори, штучний інтелект та хмарні сервіси, дозволяє значно підвищити рівень безпеки, зручності та гнучкості систем доступу. Кожна з розглянутих технологій має свої переваги та сфери застосування, однак найбільш ефективними є саме інтегровані системи, що об’єднують кілька технологій одночасно. Це забезпечує можливість адаптації до різних умов експлуатації, масштабування системи та її модернізації в майбутньому. Таким чином, IoT-технології відкривають широкі перспективи для подальшого розвитку інтелектуальних систем контролю доступу.

1.2 Аналіз існуючих систем контролю доступу

Розвиток технологій IoT сприяв створенню низки ефективних рішень для автоматизації систем доступу, що використовуються у житлових, комерційних, промислових та стратегічних об’єктах. Ці системи демонструють

різноманітність підходів до інтеграції сенсорів, алгоритмів аналізу даних, хмарних платформ і засобів управління. У цьому розділі розглядаються найбільш відомі рішення, їхні особливості, технічні характеристики та приклади впровадження.

Для початку розглянемо Honeywell Security Suite (HSS). HSS є передовою системою управління доступом і безпекою, яка зарекомендувала себе як надійне рішення для різних типів об’єктів – від невеликих офісних приміщень до масштабних промислових комплексів та стратегічних об’єктів. Завдяки своїй модульній архітектурі система може бути адаптована до конкретних вимог замовника, забезпечуючи високу гнучкість і ефективність. Це робить HSS популярним вибором у всьому світі для організації інтегрованих безпекових систем.

Однією з ключових особливостей HSS є її масштабованість. Це дозволяє використовувати систему в різних умовах: як для управління доступом у невеликій будівлі з кількома дверима, так і для забезпечення безпеки на великих промислових об’єктах або в аеропортах.

Завдяки модульній структурі можна легко додавати нові компоненти, пристрої чи користувачів без необхідності заміни основних елементів системи. Наприклад, підприємство, що планує розширення, може поступово інтегрувати додаткові модулі системи, такі як нові точки доступу, камери спостереження або датчики руху.

Інтеграція з відеоспостереженням є ще однією важливою особливістю HSS. Система дозволяє підключати камери відеоспостереження, які автоматично аналізують потоки даних у реальному часі. Алгоритми відеоаналітики забезпечують ідентифікацію осіб, розпізнавання номерних знаків або моніторинг поведінки у визначених зонах.

Наприклад, якщо камера фіксує підозрілу поведінку, система може автоматично надсилати сповіщення оператору та блокувати доступ до певної зони. Це особливо корисно для стратегічних об’єктів, таких як аеропорти, де контроль за великими територіями має критичне значення.

Хмарна платформа, що є невіддільною частиною HSS, дозволяє адміністраторам системи віддалено здійснювати управління та моніторинг. Використовуючи веб-інтерфейс або мобільний додаток, адміністратори можуть переглядати журнали доступу, змінювати права користувачів або отримувати сповіщення про потенційні загрози незалежно від їхнього місцезнаходження. Наприклад, якщо на об’єкті відбувається несанкціонована спроба доступу, адміністратор отримає повідомлення на смартфон із деталями інциденту. Це забезпечує високий рівень оперативності та дозволяє швидко реагувати на можливі загрози.

З технічної точки зору HSS підтримує широкий спектр пристроїв і технологій, що робить її універсальним рішенням для різних умов. Наприклад, система сумісна з RFID-картками, що є зручним інструментом для ідентифікації користувачів.

Біометричні пристрої, такі як сканери відбитків пальців або розпізнавання обличь, додають додатковий рівень безпеки, оскільки доступ можливий лише за наявності унікальних біометричних даних. Крім того, HSS інтегрується з популярними IoT-протоколами, такими як ZigBee та LoRa, що забезпечує зручний зв’язок між пристроями навіть на великих відстанях.

Захищеність даних є ще одним важливим аспектом HSS. Для цього система використовує передове AES-256 шифрування, яке гарантує, що передані дані залишаються конфіденційними. Це особливо важливо для великих корпорацій і державних установ, де витік інформації може призвести до значних втрат. Наприклад, журнали доступу, біометричні дані користувачів та інші критичні записи зберігаються в зашифрованому вигляді, що виключає можливість їх перехоплення або несанкціонованого доступу.

У реальних умовах система Honeywell показала свою ефективність на численних об’єктах по всьому світу.

Одним із найяскравіших прикладів є міжнародний аеропорт Лондона. На цьому об’єкті HSS використовується для управління доступом до технічних зон, розпізнавання облич персоналу та динамічного налаштування доступу залежно від рівня авторизації.

Наприклад, технічний персонал має доступ лише до зон, де вони виконують свої обов’язки, тоді як керівники мають ширші права. Усі дії фіксуються в системі, що дозволяє адміністраторам аналізувати поведінку користувачів і оперативно реагувати на аномальні події.

HSS також забезпечує зручність для кінцевих користувачів.

Наприклад, співробітники можуть отримувати тимчасові коди доступу через мобільний додаток або використовувати біометрію для швидкого входу. Це дозволяє уникнути втрати ключів чи карток і підвищує загальний рівень задоволеності користувачів.

Підсумовуючи, HSS є потужним і гнучким інструментом для управління доступом і забезпечення безпеки на різних типах об’єктів.

Завдяки своїм передовим технологіям, модульній архітектурі та хмарним функціям система пропонує широкий спектр можливостей для забезпечення безпеки, зручності та ефективності.

Реалізовані проекти, такі як впровадження в міжнародному аеропорту Лондона, демонструють її здатність адаптуватися до складних умов і забезпечувати високий рівень захищеності.

Перейдемо до ще однієї моделі. Bosch Access Management є передовим рішенням у сфері управління доступом (рис. 1.2), розробленим для забезпечення високого рівня безпеки, гнучкості в налаштуванні та інтеграції з іншими системами. Це рішення ідеально підходить для великих корпоративних офісів, урядових установ і банків, де потрібно забезпечити багаторівневий контроль доступу та можливість швидкої адаптації до змінних умов.

Завдяки своїй інноваційній архітектурі, Bosch Access Management пропонує широкий спектр функцій, які дозволяють користувачам ефективно управляти доступом і забезпечувати захист чутливих даних.

Рисунок 1.2 – Bosch Access Panels

Однією з головних переваг системи є її багаторівневий підхід до контролю доступу. Bosch Access Management підтримує фізичну ідентифікацію, біометричні технології та двофакторну автентифікацію. Це означає, що користувач може отримати доступ до певної зони лише після проходження кількох рівнів перевірки, наприклад, використовуючи як RFID-картку, так і сканер відбитків пальців. Такий підхід значно підвищує безпеку, особливо на об'єктах, де зберігаються конфіденційні дані або матеріальні цінності. Наприклад, у банках система Bosch Access Management дозволяє обмежити доступ до сховищ лише для уповноважених осіб, використовуючи їхні біометричні дані.

Підтримка мобільного доступу є ще однією важливою особливістю системи. Bosch Access Management інтегрується з технологіями NFC (Near Field Communication) і BLE (Bluetooth Low Energy), що дозволяє використовувати смартфони як ключі доступу. Ця функція є особливо зручною для співробітників, які не хочуть носити з собою фізичні картки або ключі. Наприклад, у штаб-квартирі компанії BMW у Мюнхені співробітники можуть використовувати мобільні додатки для доступу до конференц-залів, виробничих приміщень або

архівів. Смартфони генерують тимчасові або постійні цифрові ключі, які можуть бути скасовані або змінені у випадку втрати пристрою.

Одним із важливих аспектів Bosch Access Management є його високий рівень інтеграції з іншими системами. Це включає зв’язок із пожежною сигналізацією, системами відеоспостереження та енергозберігаючими технологіями. Наприклад, у разі пожежі система автоматично розблокує певні виходи, щоб забезпечити безпечну евакуацію співробітників. Інтеграція з відеоспостереженням дозволяє використовувати відеоаналітику для розпізнавання осіб та виявлення підозрілої поведінки. У корпоративних офісах ця функція може бути використана для моніторингу зон із обмеженим доступом і попередження про потенційні загрози.

Технічні характеристики Bosch Access Management відповідають високим стандартам безпеки та функціональності. Система підтримує до 10000 користувачів, що робить її ідеальним вибором для великих компаній і урядових установ. Вона також забезпечує захищений хмарний доступ через Bosch Cloud, що дозволяє адміністраторам керувати системою з будь-якого місця, де є інтернет-з'єднання. Наприклад, адміністратор може віддалено додавати нових користувачів, змінювати права доступу або переглядати журнали дій. Завдяки використанню хмарних технологій система забезпечує високий рівень оперативності та адаптивності.

Підтримка відеоаналітики є ще одним важливим компонентом Bosch Access Management. Камери, інтегровані з системою, можуть розпізнавати обличчя користувачів, аналізувати поведінкові патерни та попереджати про підозрілу активність. Наприклад, якщо камера фіксує спробу проникнення до забороненої зони, система автоматично сповіщає оператора та блокує доступ до інших зон. Це значно підвищує рівень безпеки, особливо на об'єктах із великою кількістю точок доступу.

Приклад впровадження Bosch Access Management у штаб-квартирі компанії BMW у Мюнхені демонструє її гнучкість і ефективність. У цьому комплексі система використовується для управління доступом до всіх приміщень, включаючи конференц-зали, виробничі ділянки та архіви. Завдяки інтеграції з

мобільними додатками співробітники можуть швидко отримувати доступ до необхідних зон, а адміністрація має можливість оперативно змінювати права доступу залежно від поточних потреб. Крім того, система інтегрується з енергозберігаючими технологіями, що дозволяє автоматично вимикати освітлення та кондиціонери в приміщеннях, коли вони не використовуються.

Переваги Bosch Access Management також включають її зручність для кінцевих користувачів. Інтерфейс системи розроблений таким чином, щоб бути інтуїтивно зрозумілим як для адміністраторів, так і для звичайних співробітників. Наприклад, користувачі можуть отримувати сповіщення про зміни у своїх правах доступу через мобільний додаток, що значно спрощує процес управління.

У підсумку, Bosch Access Management є потужним інструментом для забезпечення безпеки на об'єктах із високими вимогами до захищеності. Її багаторівневий підхід до контролю доступу, підтримка мобільних технологій, інтеграція з іншими системами та розширені функції відеоаналітики роблять її одним із найкращих рішень на ринку. Впровадження цієї системи у великих корпораціях, таких як BMW, підтверджує її ефективність і здатність адаптуватися до складних умов.

Axis Communications є однією з провідних компаній у сфері розробки інтегрованих рішень для відеоаналітики та управління доступом. Її продукти орієнтовані на забезпечення високого рівня безпеки у громадських місцях, таких як торговельні центри, транспортні вузли, культурні об’єкти, а також на інфраструктурних об’єктах критичного значення. Завдяки поєднанню передових технологій штучного інтелекту, високої якості зображення та гнучкості у налаштуванні, рішення Axis Communications дозволяють створювати потужні системи відеоспостереження та автоматизації доступу.

Однією з ключових переваг Axis Communications є можливість розпізнавання поведінки завдяки інтеграції штучного інтелекту у свої камери. Камери з підтримкою AI-алгоритмів здатні аналізувати дії людей і виявляти потенційно загрозливу поведінку. Наприклад, у транспортних вузлах система може виявляти залишені без нагляду предмети, скупчення людей у заборонених

зонах або агресивну поведінку. У торговельних центрах такі системи можуть бути використані для моніторингу активності у магазинах, запобігаючи крадіжкам чи іншим інцидентам. Виявивши потенційну загрозу, система автоматично надсилає сповіщення оператору для вжиття необхідних заходів.

Ще однією важливою характеристикою рішень Axis Communications є підтримка камер із високою якістю зображення. Завдяки використанню 4K-камер система забезпечує детальний моніторинг, що дозволяє легко ідентифікувати об’єкти навіть у складних умовах освітлення. Наприклад, у метро Стокгольма, де камери Axis Communications встановлені у пасажирських зонах, система здатна розпізнавати осіб та деталі їхньої поведінки навіть у місцях із поганим освітленням. Це забезпечує високу точність і дозволяє мінімізувати ризик пропуску потенційної загрози.

Гнучкість у налаштуванні – це ще одна перевага систем Axis Communications. Користувачі можуть створювати індивідуальні сценарії реагування для різних ситуацій. Наприклад, у разі виявлення несанкціонованого доступу до технічних приміщень система може активувати сигналізацію, закривати доступ до інших зон і надсилати сповіщення відповідальним особам. У культурних об’єктах, таких як музеї, система може відслідковувати рух відвідувачів і попереджати про спроби торкання експонатів або проникнення у заборонені зони.

Axis Communications також приділяє велику увагу підтримці сучасних технологій бездротового зв’язку. Використання протоколів Wi-Fi 6 забезпечує швидку та стабільну передачу даних, що є критично важливим для роботи з великою кількістю камер одночасно. Це дозволяє легко інтегрувати систему в існуючу мережеву інфраструктуру без необхідності проведення додаткових кабелів. Наприклад, у великих торговельних центрах система Axis Communications може забезпечувати підключення до сотень камер, які передають дані у реальному часі на центральний сервер для обробки.

Технічні характеристики систем Axis Communications включають вбудовану підтримку AI-алгоритмів, що дозволяє виконувати складні аналітичні операції безпосередньо на камерах. Це знижує навантаження на центральний

сервер і забезпечує швидшу реакцію на події. Крім того, система підтримує до 500 одночасно активних камер, що робить її ідеальним вибором для великих об’єктів із високими вимогами до відеоспостереження. Для забезпечення безпеки даних система використовує передові алгоритми шифрування, що гарантує захист від несанкціонованого доступу.

Прикладом успішного впровадження системи Axis Communications є метро Стокгольма. У цьому транспортному вузлі система використовується для моніторингу пасажирських зон, запобігання несанкціонованому доступу до технічних приміщень і розпізнавання підозрілих осіб. Завдяки високій якості зображення та підтримці AI-алгоритмів система забезпечує швидку ідентифікацію потенційних загроз і допомагає операторам вживати необхідні заходи. Наприклад, якщо камера виявляє підозрілу поведінку, така як залишений багаж, система автоматично сповіщає операторів і відправляє деталі про місце інциденту.

Використання Axis Communications також сприяє оптимізації ресурсів безпеки. Завдяки автоматизації багатьох процесів зменшується потреба у великій кількості персоналу для постійного моніторингу. Наприклад, у великих торговельних центрах оператори можуть зосередитися на аналізі лише тих подій, які система визначила як потенційно загрозливі. Це дозволяє підвищити ефективність роботи служби безпеки і знизити витрати на її утримання.

У підсумку, рішення Axis Communications пропонують унікальне поєднання передових технологій відеоаналітики, високої якості зображення та гнучкості у налаштуванні. Вони дозволяють створювати інтелектуальні системи відеоспостереження та управління доступом, які можуть адаптуватися до потреб конкретних об’єктів. Успішні приклади впровадження, такі як метро Стокгольма, демонструють ефективність і надійність цих систем, роблячи їх ідеальним вибором для забезпечення безпеки у громадських місцях та інфраструктурних об’єктах.

Перейдемо до Hikvision Access Control. Hikvision Access Control є провідним рішенням у сфері управління доступом, що поєднує передові технології відеоаналітики, біометрії та IoT. Ця система вирізняється гнучкістю в

налаштуванні, масштабованістю та високим рівнем безпеки, що робить її ідеальним вибором для великих об’єктів, таких як торговельні центри, бізнес-центри, аеропорти та промислові комплекси. Завдяки широкому спектру функцій Hikvision Access Control дозволяє створювати інтегровані рішення, які забезпечують не лише контроль доступу, але й моніторинг поведінки та автоматичне реагування на загрози.

Однією з ключових особливостей системи є багатофакторна автентифікація. Вона поєднує використання біометричних даних, карток доступу та PIN-кодів, що дозволяє значно підвищити рівень безпеки. Наприклад, співробітники можуть використовувати RFID-картки для входу в загальні зони, а для доступу до критично важливих зон додатково використовувати сканери відбитків пальців або розпізнавання обличь. Такий підхід є особливо актуальним для банківських установ, дата-центрів та інших об'єктів із високими вимогами до захищеності.

Інтеграція з мобільними додатками є ще однією важливою особливістю Hikvision Access Control. Вона дозволяє адміністраторам і користувачам управляти системою у віддаленому режимі. Наприклад, співробітники можуть використовувати мобільний додаток для доступу до приміщень, отримуючи тимчасові цифрові ключі. Адміністратори, у свою чергу, можуть переглядати журнали доступу, змінювати налаштування та додавати нових користувачів без необхідності фізичної присутності на об’єкті. Ця функція є особливо корисною для великих підприємств, де управління системами доступу вимагає високого рівня гнучкості.

Система Hikvision Access Control підтримує масштабування для великих об’єктів. Це означає, що вона може обслуговувати тисячі точок доступу, що робить її ідеальним вибором для великих інфраструктурних об’єктів. Наприклад, у великих торговельних центрах система здатна контролювати доступ до входів, торговельних зон, службових приміщень і парковок, забезпечуючи злагоджену роботу всієї інфраструктури. У разі необхідності розширення об’єкта система дозволяє легко додати нові пристрої та точки доступу без значних змін у вже наявній інфраструктурі.

Перейдемо до технічних характеристики Hikvision Access Control.

Hikvision Access Control підтримує до 50000 пристроїв, що забезпечує надзвичайну масштабованість і функціональність. Ця характеристика є важливою для великих об’єктів, таких як аеропорти, де потрібно контролювати доступ до багатьох зон із різними рівнями безпеки.

Система інтегрує штучний інтелект (AI), що дозволяє розпізнавати обличчя користувачів і аналізувати їхню поведінку. Завдяки використанню AI система може ідентифікувати потенційні загрози, наприклад, підозрілу поведінку або спроби проникнення до заборонених зон. Такі функції є критично важливими для об’єктів із високими вимогами до безпеки, оскільки вони дозволяють автоматизувати процес виявлення загроз і мінімізувати вплив людського фактора.

Резервне живлення є ще одним важливим аспектом Hikvision Access Control. У разі відключення основного електроживлення система продовжує працювати завдяки вбудованим резервним батареям. Це забезпечує безперервність роботи навіть у критичних ситуаціях, таких як аварійне відключення електроенергії. Наприклад, у торговельних центрах це дозволяє зберігати контроль над входами та виходами навіть у разі перебоїв у роботі енергосистеми.

Приклад впровадження – торговельний центр у Дубаї.

У найбільшому торговельному центрі Дубая система Hikvision Access Control використовується для забезпечення безпеки на входах, у торговельних зонах та на парковках. Завдяки інтеграції з відеоаналітикою система дозволяє розпізнавати осіб, які входять до торговельного центру, та аналізувати їхню поведінку у реальному часі. Наприклад, у разі виявлення підозрілої поведінки система автоматично сповіщає операторів і надсилає їм зображення інциденту.

Крім того, система забезпечує зручність для клієнтів. Наприклад, відвідувачі можуть використовувати мобільні додатки для доступу до парковок, отримуючи цифрові ключі через свої смартфони. Це дозволяє значно зменшити час, необхідний для реєстрації та входу, і підвищує загальний рівень комфорту.

Розглянемо переваги Hikvision Access Control (табл. 1.1).

Hikvision Access Control має низку переваг, які роблять її одним із найкращих рішень для створення інтегрованих систем доступу:

– високий рівень безпеки. Завдяки багатофакторній автентифікації, AI-алгоритмам і відеоаналітиці система забезпечує надійний захист об’єктів;

– масштабованість. Система підтримує велику кількість пристроїв і точок доступу, що робить її придатною для використання на великих об’єктах;

– зручність для користувачів. Інтеграція з мобільними додатками забезпечує зручний доступ і управління системою;

– безперебійна робота. Завдяки резервному живленню система продовжує працювати навіть у разі відключення електроенергії.

Hikvision Access Control є потужним рішенням для створення інтегрованих систем доступу, які поєднують передові технології відеоаналітики, біометрії та IoT. Завдяки високій масштабованості, гнучкості в налаштуванні та зручності використання, система є ідеальним вибором для великих об’єктів із високими вимогами до безпеки. Успішне впровадження у найбільшому торговельному центрі Дубая підтверджує її ефективність і надійність, роблячи Hikvision Access Control одним із лідерів ринку систем доступу.

Таблиця 1.1 – Порівняння IoT систем

Система	Переваги	Недоліки	Сфера застосування
Honeywell Security	Інтеграція з IoT, масштабованість	Висока вартість впровадження	Аеропорти, промислові зони
Bosch Access Management	Гнучкість налаштувань, безпека	Складність інтеграції	Урядові установи, офіси

Продовження табл. 1.1

Система	Переваги	Недоліки	Сфера застосування
Axis Communications	Відеоаналітика, розпізнавання поведінки	Вимоги до високошвидкісного зв’язку	Громадські місця
Hikvision Access Control	Масштабованість, багатофакторна автентифікація	Залежність від мобільного зв’язку	Торговельні центри

2 АРХІТЕКТУРА ТА АЛГОРИТМИ СИМУЛЯЦІЇ IoT-СЕРЕДОВИЩ

2.1 Розробка архітектури симульованої IoT-системи

У процесі розробки системи автоматизації контролю доступу до охоронюваної зони було прийнято рішення базувати проектовану архітектуру на принципах Інтернету речей (IoT) з урахуванням сучасних вимог до надійності, безпеки, масштабованості та енергетичної автономності [13-16]. Архітектура побудована за модульним принципом і передбачає поділ системи на окремі взаємопов’язані підсистеми, кожна з яких виконує чітко визначену функціональну роль у загальній структурі (рис. 2.1).

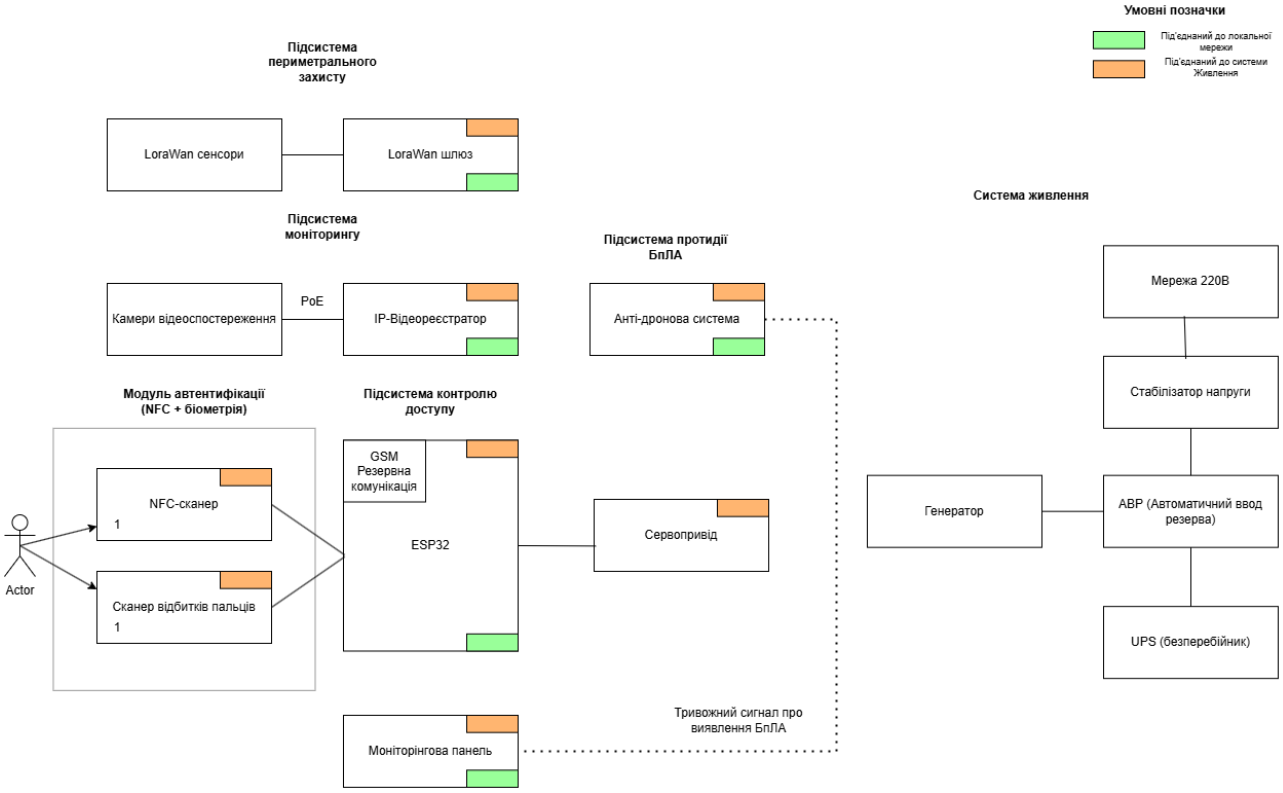

Рисунок 2.1 – Архітектура IoT системи для об’єкта, що охороняється

Основною підсистемою є підсистема контролю доступу, яка відповідає за автентифікацію користувачів та керування механізмом фізичного допуску на об’єкт. Центральним елементом цієї підсистеми виступає мікроконтролер ESP32,

який здійснює збір даних від пристроїв автентифікації – NFC-сканера та сканера відбитків пальців. Автентифікація користувача побудована за принципом двофакторної перевірки: спочатку ідентифікація за допомогою безконтактної карти, а потім верифікація біометричних даних. Для підвищення стійкості до потенційних атак зловмисників у якості носіїв ідентифікаторів використовується стандарт MIFARE DESFire EV1/EV2, що забезпечує захист даних шляхом використання симетричного шифрування DES, 3DES або AES-128. Завдяки DESFire реалізується динамічна автентифікація, захист записів даних та можливість розмежування рівнів доступу на основі внутрішніх додатків карти.

Модулі NFC та сканування відбитків підключені до ESP32 через сигнальні лінії SPI або UART відповідно. З метою забезпечення стабільності роботи під час активного використання обидва пристрої живляться від окремого стабілізованого джерела живлення 5 вольт, яке підключене через безперебійник (UPS). Таким чином мінімізуються ризики нестабільної роботи у разі перепадів напруги або втрати основного живлення.

Результати автентифікації обробляються у реальному часі на контролері ESP32. У разі позитивної верифікації подається команда на активацію сервопривода, що механічно відкриває доступ користувачу. Сервопривід отримує керуючий сигнал (PWM) від ESP32, проте живлення його здійснюється окремо від високостабільного джерела для уникнення перевантаження мікроконтролера.

Другим важливим елементом системи є підсистема моніторингу території. Для реалізації безперервного візуального спостереження встановлюється мережа IP-камер відеоспостереження, які живляться за допомогою технології Power over Ethernet (PoE) безпосередньо від IP-відеореєстратора. Це дозволяє передавати живлення та дані одним кабелем, що спрощує монтаж системи, підвищує її надійність та знижує витрати на додаткове електроживлення. Реєстратор відповідає за централізоване збереження відеоданих, що дозволяє швидко отримувати доступ до архіву записів у разі інцидентів.

Для підвищення рівня фізичної безпеки було передбачено встановлення підсистеми периметрального захисту на основі бездротових LoRaWAN-сенсорів. Вибір даної технології обумовлений її енергоефективністю, широким радіусом

дії (до 10–15 км на відкритій місцевості) та можливістю встановлення сенсорів у важкодоступних місцях без прокладки електропроводки. Сенсори фіксують спроби проникнення, зміни стану навколишнього середовища або несанкціоноване переміщення об'єктів, після чого передають дані на LoRaWAN-шлюз, що інтегрується до локальної мережі об'єкта.

Окрему увагу було приділено сучасним загрозам, пов’язаним із використанням безпілотних літальних апаратів (БпЛА). Для цього реалізовано підсистему протидії БпЛА, яка забезпечує виявлення дронів у межах контрольованої території. Анти-дронова система здатна за допомогою аналізу радіочастотного спектру або візуального моніторингу виявляти присутність сторонніх об’єктів у повітрі. У разі фіксації загрози формується тривожний сигнал, який передається безпосередньо до ESP32 та моніторингової панелі для подальшої реакції охоронного персоналу.

Оскільки безперервна робота системи критично важлива для забезпечення безпеки, архітектура передбачає використання резервованої системи живлення. Базове електроживлення здійснюється від мережі 220 В через стабілізатор напруги, що згладжує коливання та захищає обладнання від стрибків. У разі аварійного відключення мережі автоматично активується дизельний генератор через пристрій автоматичного вводу резерву (АВР). Підключення основних елементів системи через UPS гарантує безперервність живлення під час переходу між джерелами електроенергії.

Важливою особливістю є інтеграція резервної GSM-комунікації. За допомогою GSM-модуля, підключеного до ESP32, система здатна підтримувати зв'язок з охороною або відповідальними особами навіть у разі повної відмови локальної мережі або Інтернет-з'єднання. У критичних ситуаціях система надсилає текстові повідомлення або автоматичні виклики для негайного інформування про інциденти.

Таким чином, розроблена архітектура симульованої IoT-системи об'єднує сучасні технології бездротового передавання даних, криптографічний захист персональної інформації користувачів через використання стандарту DESFire, комплексний моніторинг території та периметра об'єкта, а також впроваджує

надійні механізми енергетичного резервування та аварійної комунікації. Завдяки багаторівневому підходу до безпеки система демонструє високу стійкість до загроз як фізичного, так і цифрового характеру та може бути використана на об’єктах із підвищеними вимогами до захисту.

2.2 Розробка алгоритму роботи симулятора

У межах реалізації системи автоматизації контролю доступу та захисту охоронюваної території було розроблено алгоритм роботи симульованої моделі, яка імітує взаємодію між ключовими апаратними та програмними компонентами проєкту. Метою створення симулятора є перевірка логіки функціонування окремих підсистем, забезпечення їхньої взаємодії, тестування основних сценаріїв роботи, а також оцінка відповідності запропонованих рішень технічним вимогам.

Архітектура моделі побудована таким чином, що на першому етапі ініціалізуються всі компоненти системи, включаючи модуль зчитування NFC-карток на базі PN532, сканер відбитків пальців R503, контролер ESP32, сервопривід електронного замка та модулі передачі тривожних сигналів. Після успішної ініціалізації система переходить у режим очікування взаємодії з користувачем. При наближенні користувача активується процедура автентифікації, яка полягає у двофакторній перевірці ідентичності: спочатку здійснюється зчитування унікального ідентифікатора NFC-картки, після чого проводиться обробка біометричних даних шляхом сканування відбитка пальця.

Отримані дані надходять до обчислювального модуля, де виконується їхня перевірка з попередньо збереженими записами у локальній базі даних. Для кожного користувача передбачено відповідність між UID картки та зашифрованими даними біометричних характеристик. Якщо обидві перевірки проходять успішно, контролер активує механізм керування замком через сервопривід, що фізично відкриває доступ на охоронювану територію. Паралельно факт доступу реєструється у внутрішньому журналі подій із зазначенням часу, ідентифікатора користувача та результату операції.

У разі, якщо одна з перевірок завершується невдачею, система блокує доступ та активує протокол безпеки. Відповідно до заданого алгоритму, формується тривожне повідомлення, яке передається на центральну моніторингову панель. Це дозволяє оперативно інформувати персонал охорони про потенційні загрози або несанкціоновані спроби доступу.

Окрему увагу у розробці алгоритму приділено моделюванню ситуацій, пов’язаних із виявленням небезпечних об'єктів у повітрі, зокрема БпЛА. Для цього реалізовано механізм прийому зовнішніх подій від модулів виявлення дронів, який передбачає миттєве формування спеціального типу тривоги з подальшою передачею на відповідні елементи системи сповіщення та журналювання. Інформація про кожен інцидент також реєструється у системному журналі для можливості подальшого аналізу, розслідування та вдосконалення процедур безпеки.

Усі функціональні елементи працюють у взаємозв'язаному режимі, що дозволяє забезпечити комплексне моделювання типових сценаріїв роботи системи. Розроблений алгоритм також враховує можливість переходу системи у аварійний режим у разі втрати живлення основної мережі, перемикання на резервні джерела електроживлення та подальше збереження працездатності критичних підсистем доступу та моніторингу.

Таким чином, побудований алгоритм роботи симулятора дозволяє максимально точно відтворити логіку функціонування майбутньої реальної системи. Це забезпечує виявлення можливих недоліків ще на етапі розробки, дає змогу оперативно вносити корективи у структуру процесів та гарантує відповідність запропонованої архітектури сучасним вимогам до систем автоматизації безпеки.

Робота підсистеми живлення побудована на забезпеченні безперебійного електроживлення усіх критично важливих компонентів автоматизованої системи контролю доступу до охоронюваної зони (рис. 2.2). Алгоритм її функціонування базується на принципі автоматичного перемикання між джерелами живлення залежно від наявності або відсутності напруги в основній мережі, з урахуванням

резервних засобів живлення – джерела безперебійного живлення (UPS) та генератора.

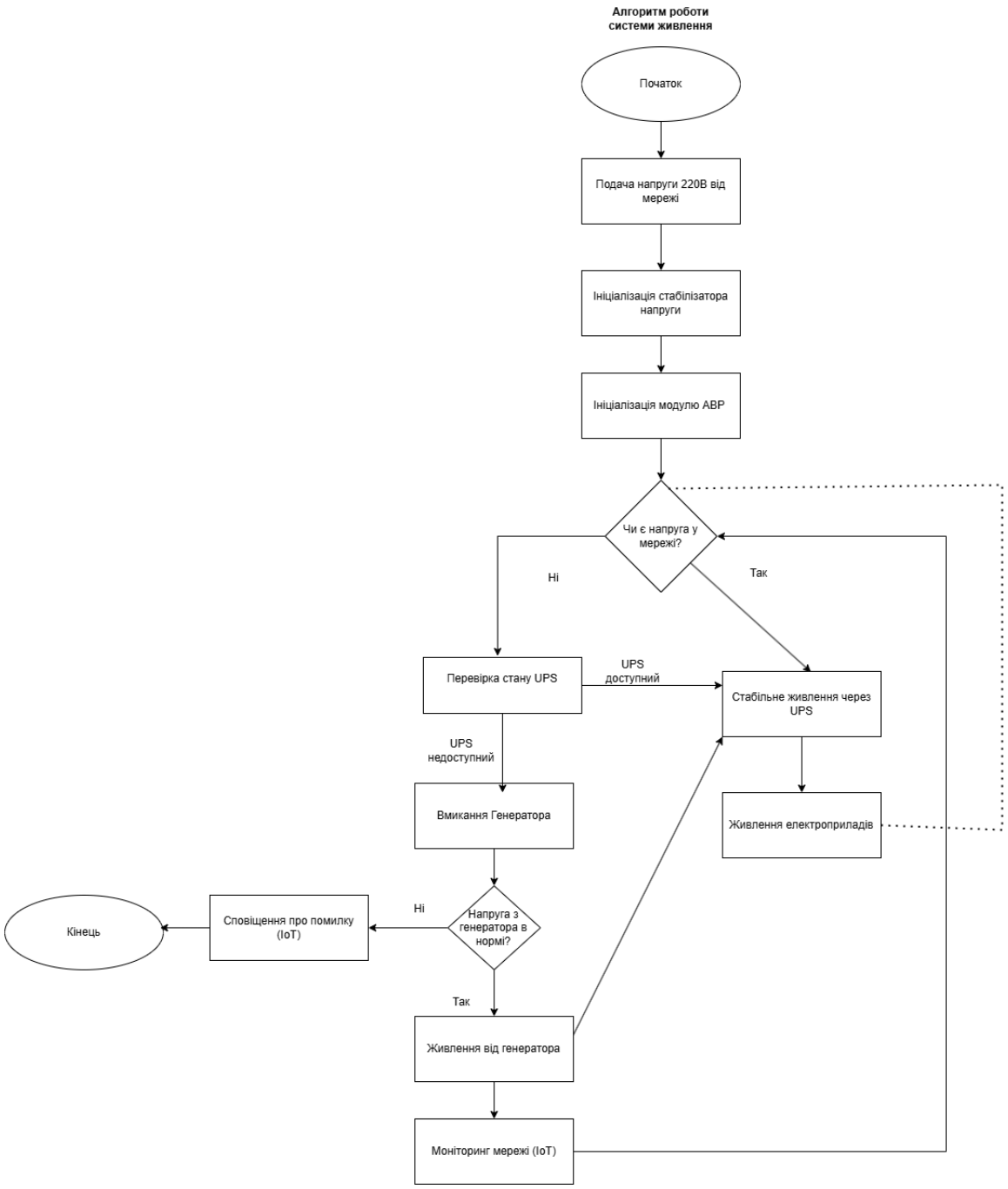

Рисунок 2.2 – Алгоритм роботи системи живлення

Процес роботи починається з подачі напруги 220 вольт від зовнішньої електромережі. На першому етапі відбувається ініціалізація стабілізатора напруги, який вирівнює параметри живлення, згладжує можливі перепади напруги та захищає підключене обладнання від коливань. Після цього

активується модуль автоматичного введення резерву (АВР), який відповідає за перемикання джерела живлення у разі відсутності напруги у мережі або виходу одного з компонентів із ладу.

Ключовим моментом є перевірка наявності напруги у мережі. У випадку, якщо напруга стабільна і знаходиться у межах допустимих значень, АВР передає сигнал на UPS, який, у свою чергу, забезпечує фільтрацію струму, накопичення енергії у вбудованих батареях та подачу електроживлення на кінцеві електроприлади. У такому режимі система працює у штатному стабільному режимі.

Якщо ж фіксується відсутність напруги у мережі, система переходить до перевірки стану UPS. У випадку, якщо UPS доступний та заряджений, відбувається автоматичне переключення на його живлення. Це забезпечує безперервну подачу енергії без критичного впливу на систему.

У ситуації, коли UPS недоступний (наприклад, у разі розрядження акумуляторів або внутрішньої несправності), ініціюється запуск резервного джерела живлення – генератора. Модуль АВР подає команду на автоматичне вмикання генератора. Після запуску проводиться контроль параметрів напруги, яка надходить від генератора. Якщо її значення відповідають встановленим нормам (наприклад, 220 ±10 вольт), АВР передає живлення на систему через UPS, де напруга додатково фільтрується і стабілізується перед подачею на споживачів.

В іншому випадку – при виявленні невідповідності напруги або інших критичних збоїв – система через IoT-модуль надсилає аварійне сповіщення про помилку до моніторингового центра. Це дозволяє оперативно втрутитись у процес і запобігти виходу з ладу компонентів.

На фінальному етапі, при переході на генераторне живлення, активується постійний моніторинг стану мережі за допомогою IoT-підсистеми. Після відновлення напруги у зовнішній електромережі система автоматично перемикається назад у штатний режим, припиняючи роботу генератора.

Такий алгоритм дозволяє забезпечити максимальну безпеку та автономність роботи всієї системи навіть за умов аварійного або бойового

відключення електропостачання, що особливо важливо у випадку військових або критично важливих об'єктів.

Робота підсистеми периметрального захисту починається з ініціалізації живлення сенсорів та LoRaWAN-шлюзу (рис. 2.3).

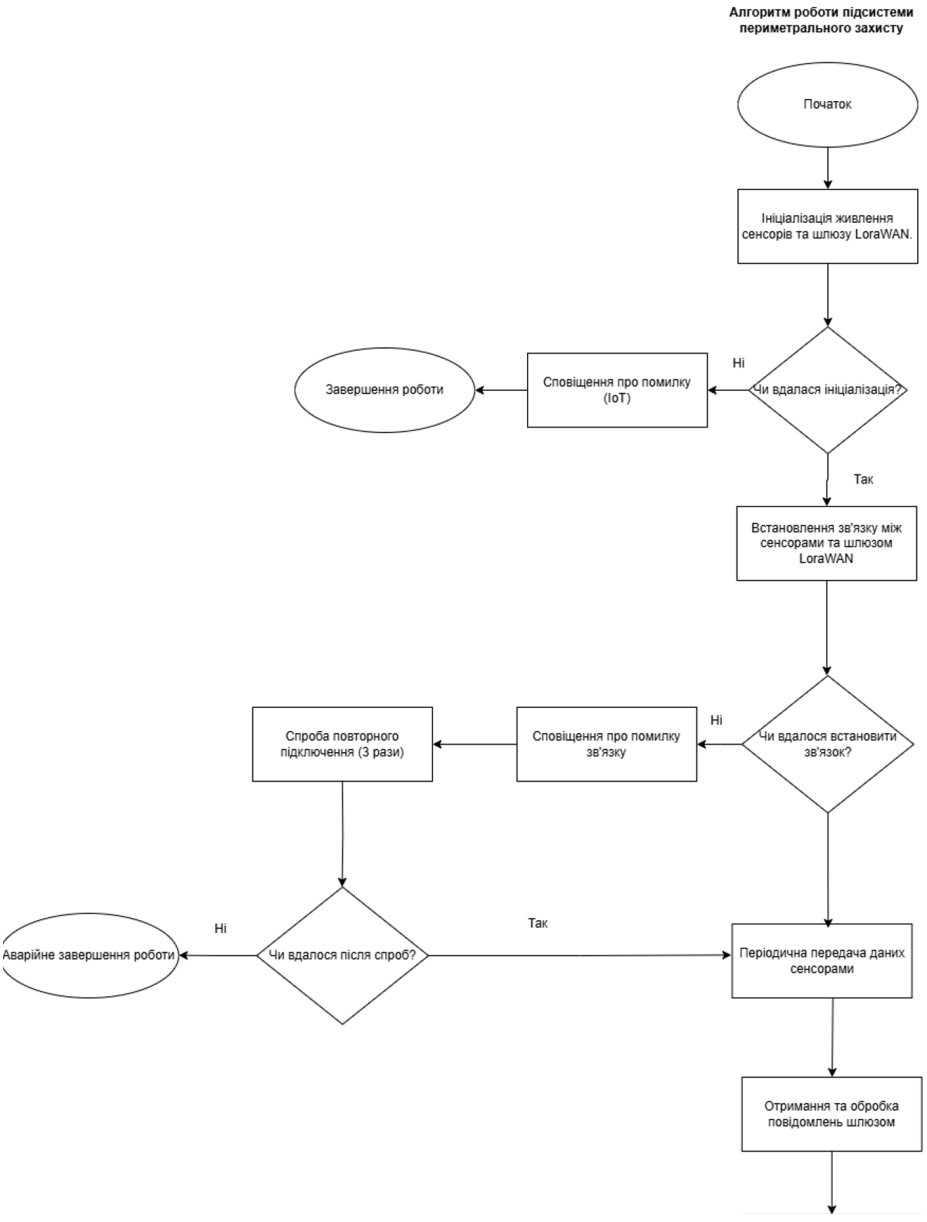

Рисунок 2.3 – Алгоритм роботи підсистеми периметрального захисту

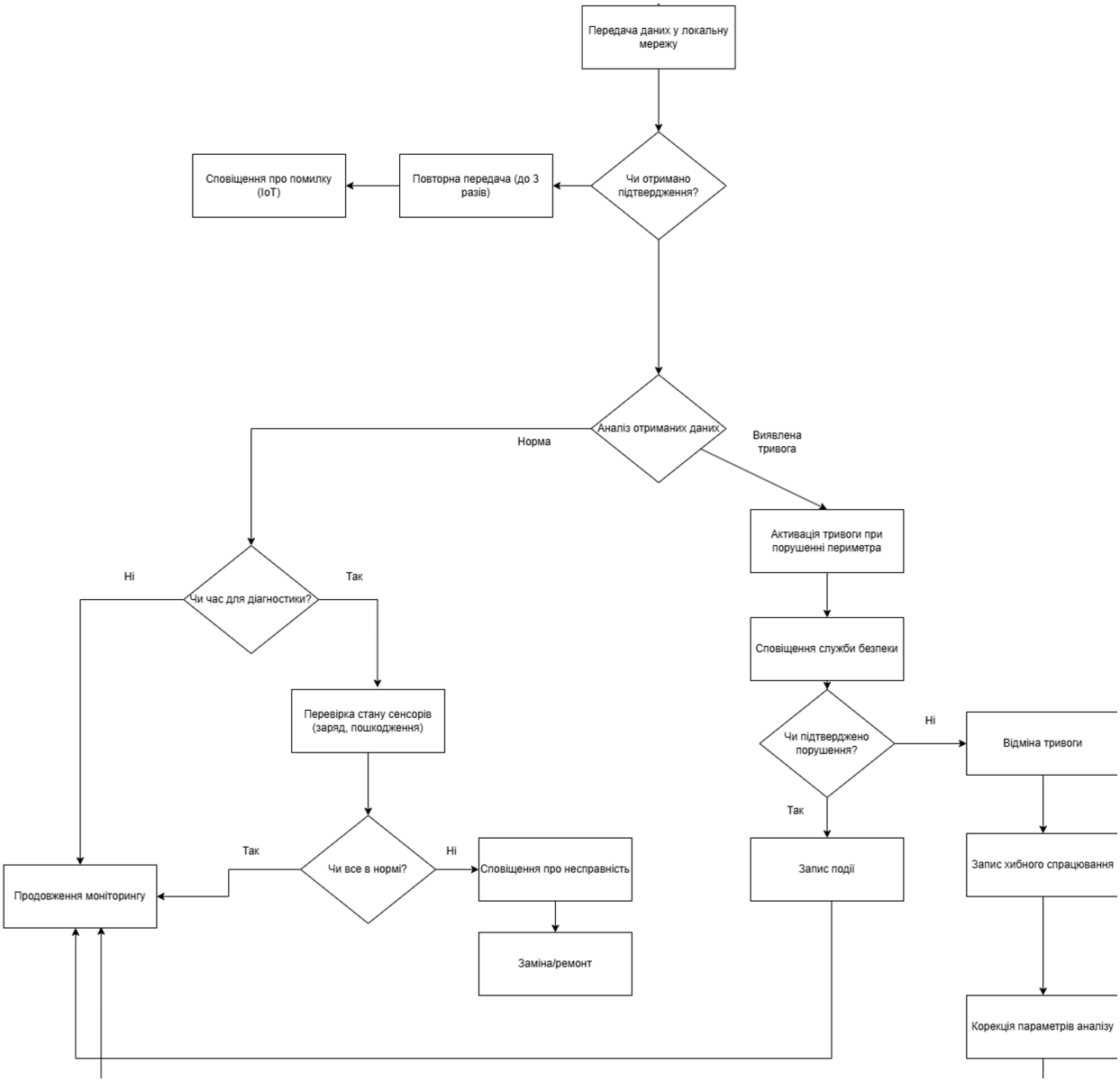

Рисунок 2.3, аркуш 2

Після активації відбувається перевірка успішності запуску: у випадку, якщо ініціалізація не вдалася, система фіксує помилку та передає повідомлення про несправність через IoT-канал, після чого завершує роботу. Якщо ж запуск пройшов успішно, система переходить до встановлення зв’язку між сенсорами та шлюзом.

У разі невдалої спроби встановлення з’єднання система здійснює до трьох повторних спроб. Якщо й після них з’єднання не вдалося – система аварійно завершує роботу, інформуючи про збій. При успішному підключенні розпочинається режим періодичної передачі даних сенсорами.

Передані дані надходять до LoRaWAN-шлюзу, який здійснює їх обробку та надсилає в локальну мережу. Далі відбувається перевірка, чи отримано підтвердження про прийом повідомлення. Якщо підтвердження не надійшло, шлюз намагається повторно надіслати дані до трьох разів. У разі невдачі система фіксує помилку і сповіщає про неї через IoT-канал.

Якщо підтвердження отримано, система проводить аналіз отриманих даних. У разі якщо значення перебувають у допустимих межах, моніторинг продовжується в штатному режимі. Якщо ж зафіксовано порушення (наприклад, рух на периметрі), ініціюється активація тривоги, паралельно з якою надсилається сигнал у службу безпеки.

Далі перевіряється, чи підтверджене порушення з боку відповідальної служби. У випадку помилкового спрацювання система скасовує тривогу та заносить подію до журналу із відповідною позначкою, після чого може скоригувати параметри аналізу для підвищення точності виявлення у майбутньому. Якщо ж порушення підтверджено, подія також реєструється в лог-файлі як безпековий інцидент.

У рамках запланованого технічного циклу відбувається періодична діагностика стану сенсорів, у тому числі перевірка заряду акумуляторів, механічних пошкоджень або обриву зв'язку. У разі виявлення відхилень надсилається повідомлення про несправність та вказується необхідність технічного втручання. Після усунення несправності або при відсутності помилок система повертається до стандартного режиму моніторингу.

Таким чином, підсистема периметрального захисту функціонує автономно, забезпечуючи як виявлення вторгнень, так і постійний контроль працездатності власних компонентів. Завдяки циклічній перевірці та використанню IoT-сповіщень система здатна забезпечити своєчасне реагування навіть у разі часткового виходу елементів з ладу, що особливо важливо в умовах роботи об'єктів з підвищеним рівнем безпеки.

Алгоритм функціонування підсистеми моніторингу починається з етапу ініціалізації IP-відеореєстратора. У разі успішного запуску система переходить до активації камер відеоспостереження через інтерфейс PoE (рис. 2.4). У разі

успішного запуску система переходить до активації камер відеоспостереження через інтерфейс PoE. Якщо ж ініціалізація відеореєстратора завершилася помилкою, система фіксує несправність, надсилає відповідне повідомлення і намагається відновити з’єднання. У разі невдалої повторної ініціалізації, після трьох спроб, робота системи аварійно завершується.

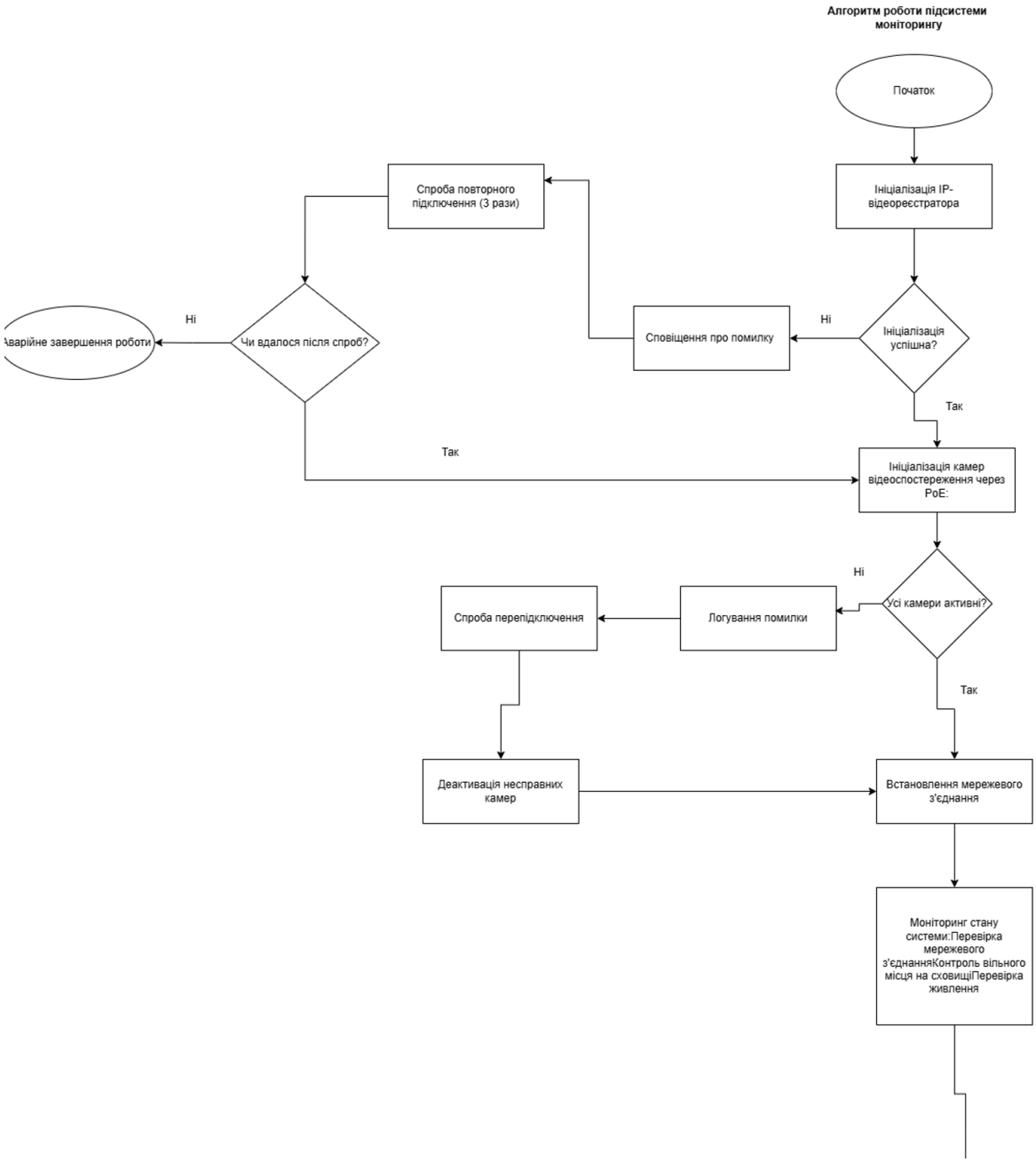

Рисунок 2.4 – Алгоритм роботи підсистеми моніторингу

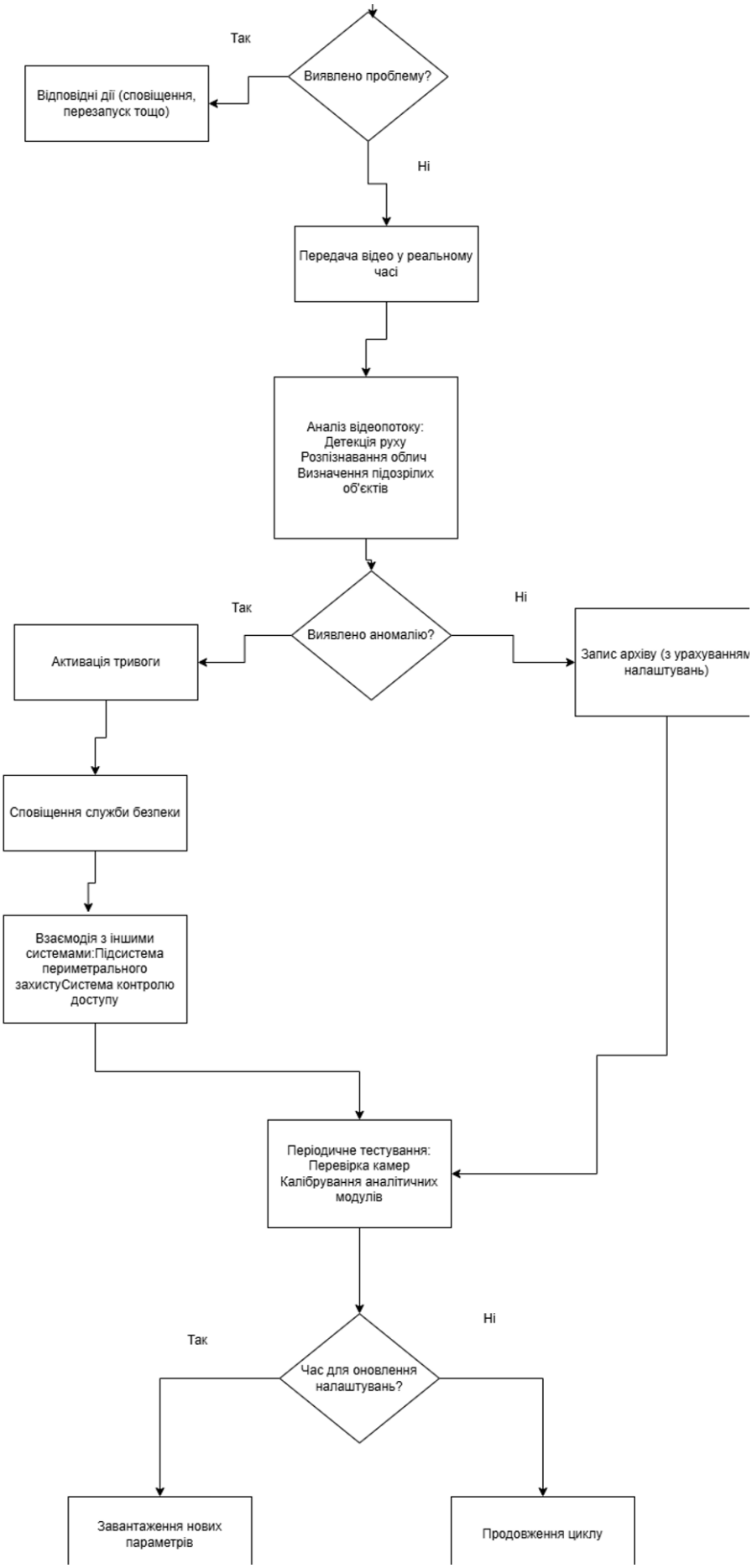

Рисунок 2.4, аркуш 2

Після активації камер проводиться перевірка їх стану. Якщо хоча б одна камера неактивна, відбувається спроба перепідключення, паралельно з якою помилка логуються. Якщо спроба виявляється безуспішною, система проводить деактивацію несправних пристроїв з відповідним повідомленням. Якщо ж усі камери активні, встановлюється стабільне мережеве з'єднання між камерами та відеореєстратором.

Далі система переходить до моніторингу стану: перевіряється передача зображення, працездатність кожного вузла, температура, рівень живлення і цілісність мережі. При виявленні будь-якої проблеми або загрози система автоматично виконує відповідні дії: відключення портів, надсилання повідомлень про перебої або перенаправлення потоків.

У разі стабільної роботи відеопотік передається в реальному часі для подальшого аналізу. Аналітичний модуль проводить оцінку зображення, виявляє підозрілі об'єкти, розпізнає обличчя, транспортні засоби, поведінкові шаблони. Якщо система не виявляє аномалій, дані просто зберігаються у відеоархів.

Якщо ж алгоритм фіксує аномалії (наприклад, вторгнення, несанкціонований рух, залишений предмет), спрацьовує тривога. Одночасно із сигналом система сповіщає службу безпеки та ініціює взаємодію з іншими підсистемами – периметрального захисту та контролю доступу.

Після цього запускається процедура повторної перевірки системи: здійснюється перевірка камер, калібрування аналітичних параметрів, оновлення моделей виявлення. Якщо настав запланований час для оновлення налаштувань, вони завантажуються із центрального сервера, і після завершення оновлення система повертається до циклу безперервного моніторингу.

Такий алгоритм дозволяє досягти високого рівня автономності, точності та відмовостійкості, забезпечуючи безперервний аналіз простору, фіксацію порушень та оперативне реагування на загрози у реальному часі.

Алгоритм роботи підсистеми автентифікації починається з ініціалізації системи (рис. 2.5). У першу чергу здійснюється очікування зчитування NFC-картки протягом певного проміжку часу (наприклад, 10 секунд). Якщо за цей час карта не піднесена до сканера, система видає повідомлення про закінчення часу

очікування та завершує поточний цикл. У разі піднесення карти система перевіряє її коректність. Якщо картка недійсна, надсилається повідомлення про помилку та здійснюється запис у лог, після чого процес починається заново.

Якщо картка є дійсною, система зчитує UID NFC-картки та переходить до наступного етапу – автентифікації за відбитком пальця. Користувач повинен прикласти палець до сканера. Зчитування відбитка триває певний проміжок часу (наприклад, до 3 секунд). Якщо палець не прикладено або відбиток зчитано некоректно, система повідомляє про помилку, фіксує подію в журналі та переходить у режим очікування повторної дії.

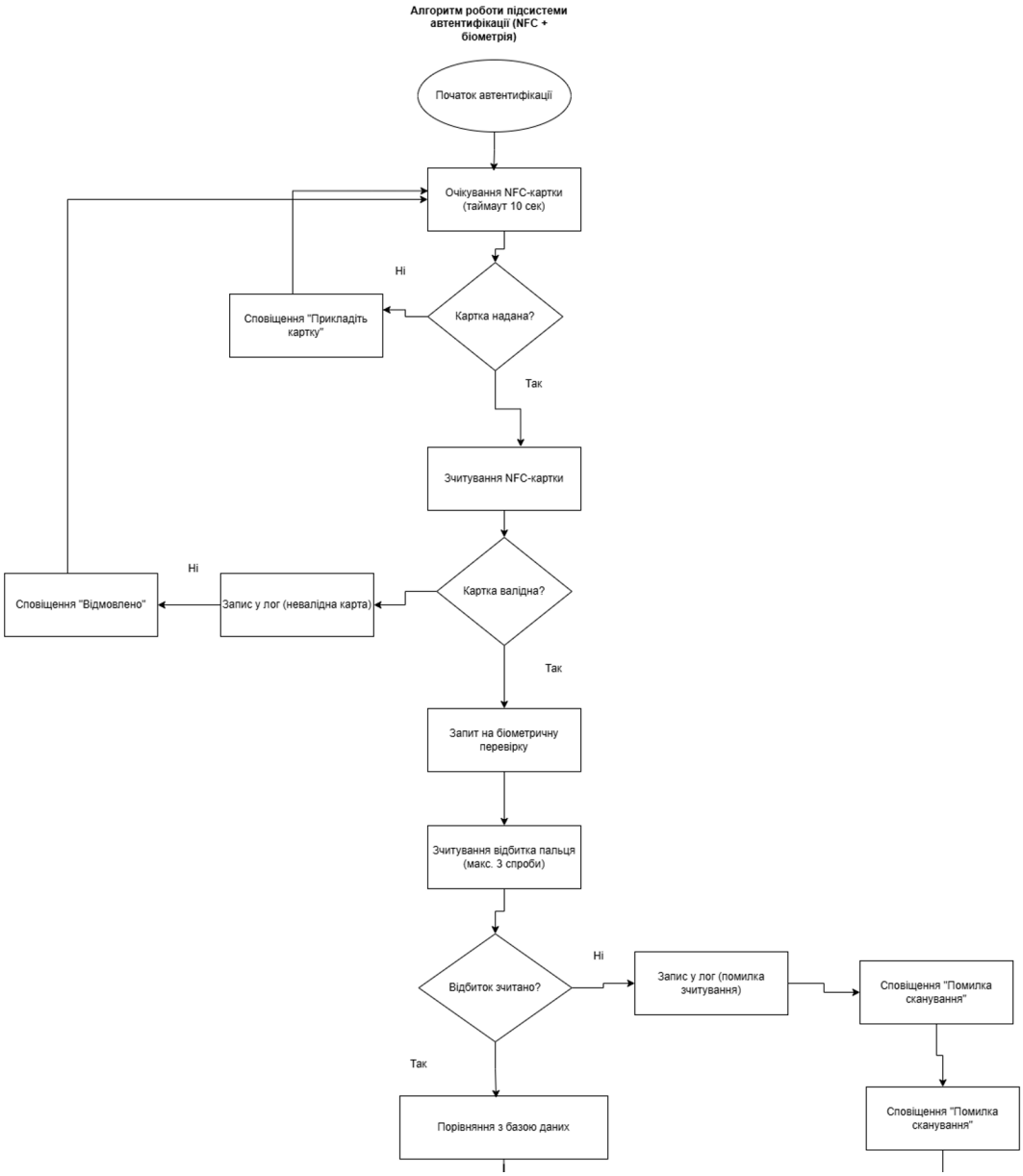

Рисунок 2.5 – Алгоритм роботи підсистеми автентифікації (NFC + біометрія)

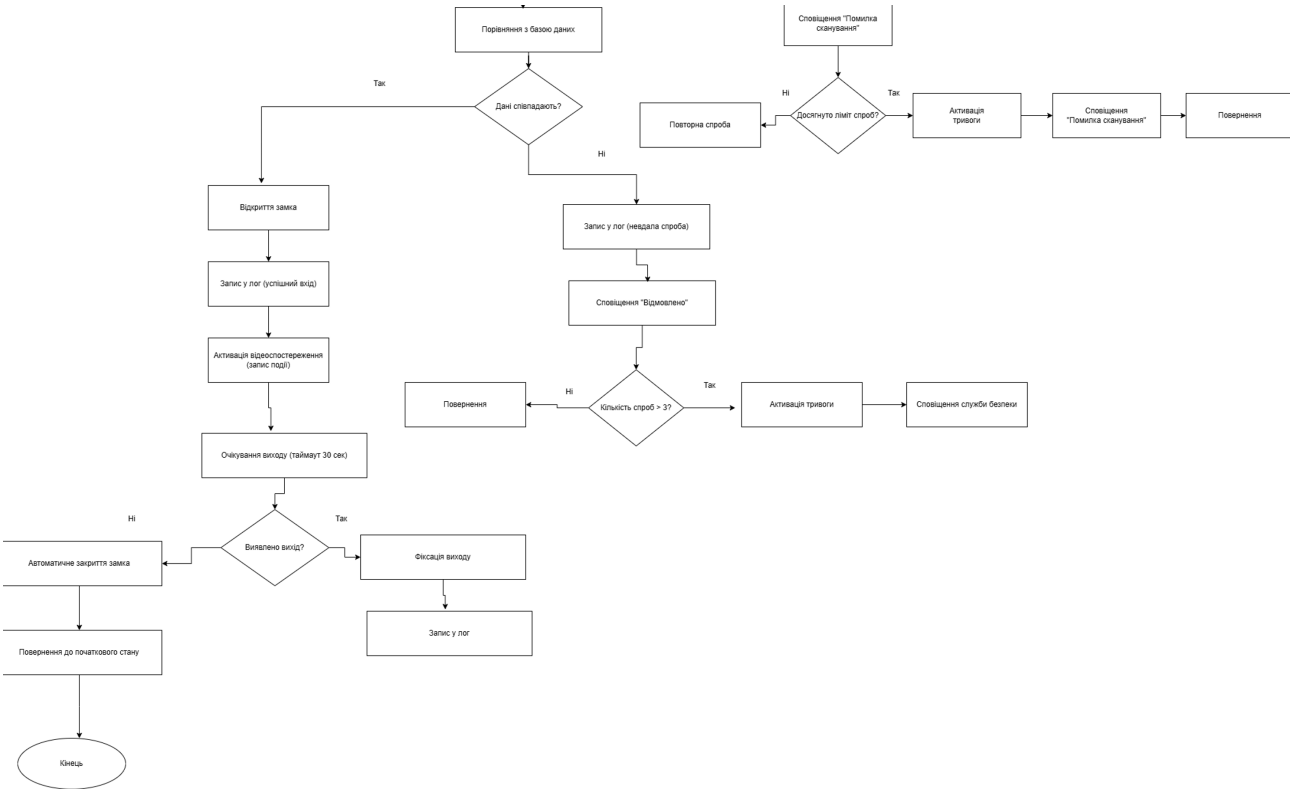

Рисунок 2.5, аркуш 2

Якщо зчитування пройшло успішно, отримані дані порівнюються з базою даних. Якщо запис знайдено, система перевіряє, чи співпадають UID картки та біометричні дані. У разі позитивного результату система активує електронний замок, фіксує відкриття в журналі, а також активує систему відеоспостереження на заданий період часу. Після очікування фіксованого інтервалу (наприклад, 30 секунд) система перевіряє, чи було зафіксовано фізичне відкриття замка. Якщо так – відбувається реєстрація входу в лог та повернення системи у початковий стан. Якщо ж двері не були відкриті, відбувається автоматичне замикання замка.

У разі, якщо зчитані дані не збігаються, проводиться додаткова перевірка на наявність спроб підбору. Якщо таких спроб зафіксовано понад заданий ліміт, система переходить у режим тривоги: активується звуковий або світловий сигнал, повідомляється служба безпеки, фіксується подія у журналі та блокується подальша автентифікація на визначений час. Якщо спроба не є критичною, фіксується невдала автентифікація, надсилається повідомлення та процес очікування поновлюється.

Таким чином, запропонований алгоритм дозволяє досягти високого рівня безпеки, забезпечує надійну перевірку особи за двома незалежними каналами (NFC та біометрія), реалізує детальне логування усіх дій та дозволяє оперативно реагувати на підозрілі ситуації.

Підсистема протидії безпілотним літальним апаратам (БпЛА) розпочинає свою роботу з ініціалізації усіх основних елементів, що забезпечують сканування простору навколо охоронюваного об'єкта. На цьому етапі запускаються сенсорні системи різних типів, здійснюється перевірка їхньої готовності до роботи, налаштування каналів обміну даними та синхронізація з центральним контролером (рис. 2.6).

Після успішної ініціалізації система переходить у режим постійного моніторингу повітряного простору. Використовується комплексний підхід, який передбачає одночасне застосування кількох типів сенсорів. Оптичні сенсори забезпечують візуальне виявлення об'єктів за допомогою відеоспостереження з високою роздільною здатністю. Радарні системи здійснюють моніторинг за допомогою радіохвильового сканування, що дозволяє виявляти об'єкти навіть за умов обмеженої видимості або вночі. RF-аналізатори контролюють наявність радіочастотних сигналів, характерних для роботи дронів, що дозволяє виявити БпЛА за їхнім каналом управління. Акустичні сенсори фіксують характерні звуки роботи пропелерів або двигунів безпілотних апаратів.

Інтеграція даних з усіх типів сенсорів дозволяє підсистемі проводити виявлення об'єктів з високою точністю. Після фіксації можливого БпЛА виконується ідентифікація об'єкта та його класифікація. На цьому етапі система аналізує отримані дані для визначення типу дрона, оцінки його розмірів, швидкості, типу керування (автономне або дистанційне), а також відстані до об'єкта.

Далі здійснюється оцінка рівня загрози, який потенційно несе виявлений БпЛА. Критеріями оцінки є відстань до об'єкта, швидкість наближення, тип і розміри дрона, а також спосіб його управління. Якщо об'єкт класифікується як потенційна загроза для об'єкта охорони, система автоматично формує тривожний сигнал.

Формування тривожного сигналу супроводжується передачею відповідних повідомлень на моніторингову панель операторів безпеки, а також активацією сценаріїв реагування. Залежно від налаштувань системи та рівня загрози, реалізуються заходи сповіщення персоналу, увімкнення тривожних сирен або ж активація засобів радіочастотного глушіння для припинення роботи ворожого БпЛА.

Рисунок 2.6 – Блок схема роботи підсистеми протидії БпЛА

Усі події, пов’язані з виявленням, ідентифікацією та реагуванням на БпЛА, реєструються у системному журналі. Логується час події, параметри виявленого об'єкта, рівень загрози, а також дії, які були здійснені у відповідь на інцидент. Створені звіти зберігаються для подальшого аналізу ефективності роботи системи та оптимізації алгоритмів виявлення і реагування.

Таким чином, алгоритм роботи підсистеми протидії БпЛА забезпечує комплексний підхід до захисту охоронюваного об'єкта від загроз з повітря, поєднуючи багаторівневий моніторинг, швидку оцінку ситуації та автоматизоване реагування.

2.3 Розробка структурної схеми симуляції

Для забезпечення моделювання роботи системи автоматизації контролю доступу та захисту охоронюваної території було розроблено комплексну структурну схему симуляції, яка відображає взаємозв’язок усіх ключових підсистем і компонентів. Структура побудована з урахуванням реальних технічних рішень і спрямована на імітацію повного циклу взаємодії між підсистемами у межах єдиного інформаційного та енергетичного середовища.

Схема передбачає поділ системи на чотири основні функціональні підсистеми: периметрального захисту, моніторингу, контролю доступу та протидії БпЛА. Додатково інтегровано систему електроживлення та мережеву інфраструктуру для забезпечення стабільності роботи всіх елементів.

Підсистема периметрального захисту складається із сенсорів Dragino LSN50 v2, які вимірюють рух, температуру та вологість, а також LoRaWAN-шлюзу Dragino LG308, що забезпечує збір і передачу даних сенсорів до локальної мережі для подальшого аналізу (рис. 2.7).

Підсистема моніторингу реалізується на базі камер відеоспостереження Hikvision DS-2CD2043G0-I із живленням через технологію PoE та відеореєстратора Hikvision DS-7608NI-K2/8P, який здійснює запис, обробку та збереження відеоархіву, а також забезпечує можливість моніторингу у реальному часі.

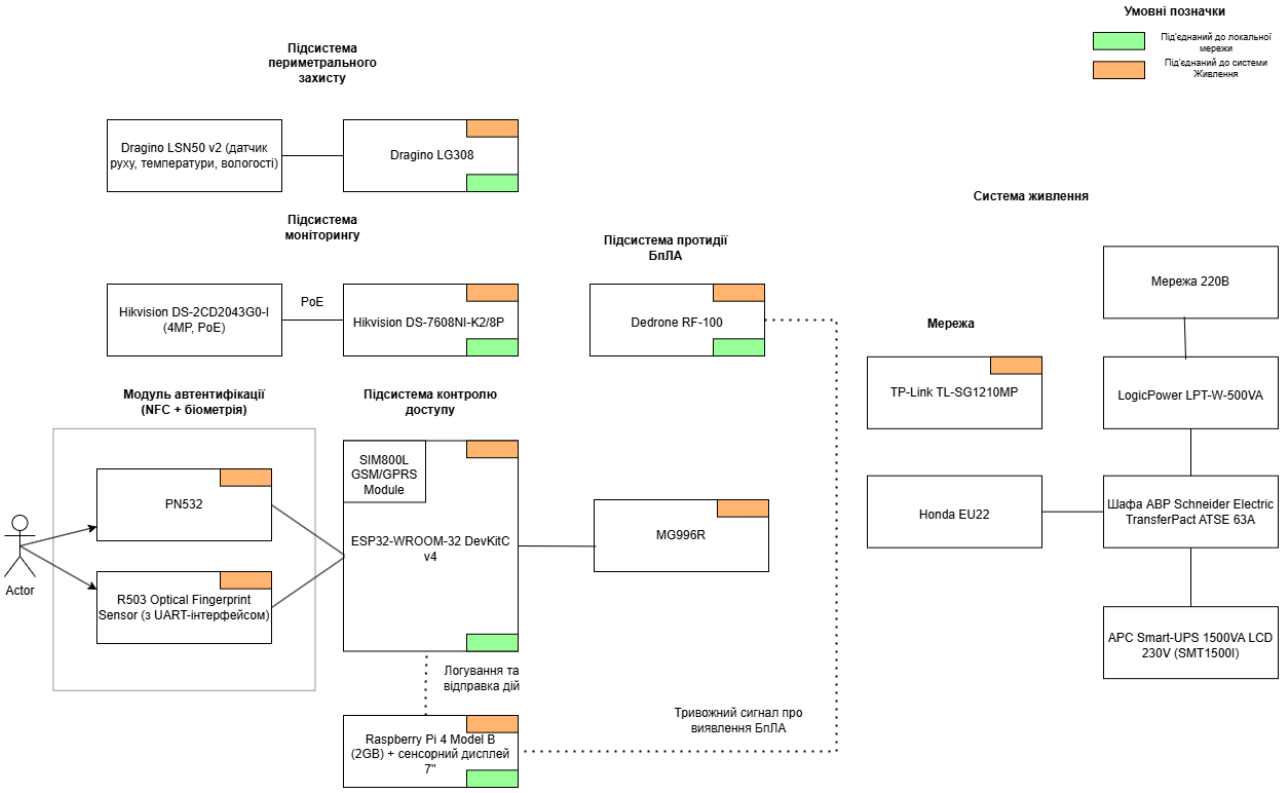

Рисунок 2.7 – Структурна схема апаратних частин

Підсистема контролю доступу побудована із застосуванням двофакторної автентифікації на основі модуля PN532 для зчитування NFC-карток та сканера відбитків пальців R503. Обробка даних автентифікації здійснюється контролером ESP32-WROOM-32 DevKitC v4, який також керує сервоприводом MG996R для фізичного відкриття замка. Для резервної передачі тривожних повідомлень у разі відмови основного каналу зв’язку використовується GSM-модуль SIM800L. Результати авторизації та дій користувачів відображаються на моніторинговій панелі на базі Raspberry Pi 4 Model B із сенсорним дисплеєм.

Підсистема протидії БпЛА реалізована з використанням детектора Dedrone RF-100, який здійснює моніторинг повітряного простору за допомогою радіочастотного аналізу. У разі виявлення загрози формується тривожний сигнал, який інтегрується у загальну систему моніторингу та безпеки.

Система живлення передбачає кілька рівнів резервування. Основним джерелом є мережа 220 В через стабілізатор LogicPower LPT-W-500VA. У випадку зникнення напруги, автоматичне перемикання здійснюється через шафу ABP Schneider Electric TransferPact ATSE 63A на живлення від генератора Honda

EU22. Для забезпечення безперебійної роботи критичних елементів використовується UPS APC Smart-UPS 1500VA LCD 230V (SMT1500I).

Локальна мережа для з'єднання всіх підсистем побудована на базі комутатора TP-Link TL-SG1210MP з підтримкою PoE, що забезпечує як передачу даних, так і живлення пристроїв.

Структурна схема симуляції дозволяє моделювати взаємодію між усіма елементами системи, перевіряти їхню працездатність у стандартних та аварійних режимах, аналізувати поведінку підсистем при виникненні загроз, а також забезпечує можливість тестування резервних сценаріїв підтримки роботи системи безпеки.

2.4 Обґрунтування вибору середовища реалізації

На етапі розробки симулятора IoT-системи автоматизації контролю доступу та захисту території постала задача вибору оптимального середовища моделювання. Для досягнення поставлених цілей було проаналізовано ряд існуючих рішень, серед яких розглядалися Proteus Design Suite, Tinkercad Circuits, SimulIDE та Wokwi IoT Simulator.

Proteus Design Suite є одним із найпотужніших інструментів для моделювання електроніки, який дозволяє детально відтворювати аналогові і цифрові процеси, взаємодію мікроконтролерів, а також складні електронні системи. Його сильними сторонами є глибока деталізація процесів та підтримка великої кількості мікроконтролерів різних архітектур. Водночас використання Proteus для моделювання сучасних IoT-рішень обмежене, адже середовище не має прямої підтримки популярних модулів ESP32, GSM або LoRaWAN. До того ж, вартість ліцензії на Proteus є значною, що ускладнює його використання для невеликих дослідницьких чи навчальних проєктів.

Tinkercad Circuits є простим онлайн-інструментом для створення базових електронних схем. Він зручний у використанні та безкоштовний, проте його можливості суттєво обмежені. Платформа підтримує лише прості проекти на основі Arduino і не надає функціоналу для роботи з ESP32, а також не має

можливості моделювання мережевої взаємодії чи IoT-інтеграцій. Для складних систем безпеки, які потребують двофакторної автентифікації, зв'язку через GSM або обробки даних із різних сенсорів, функціоналу Tinkercad є недостатнім.

Серед альтернатив також розглядалося середовище SimulIDE, яке дозволяє моделювати базові електронні пристрої з мінімальними системними вимогами. Його перевагами є простота використання та швидкість розгортання симуляцій. Проте можливості цього інструменту суттєво обмежені відсутністю повноцінної підтримки протоколів IoT, сенсорних мереж та складних сценаріїв обміну даними, що робить його придатним лише для тестування найпростіших логічних схем.

На основі аналізу можливих рішень було прийнято рішення обрати середовище Wokwi IoT Simulator для реалізації симулятора системи. Це середовище спеціалізується на підтримці мікроконтролерів ESP32, Arduino та ESP8266, що відповідає технічним вимогам проєкту. Wokwi надає можливість моделювати логіку роботи таких елементів як модуль NFC (PN532), сканер відбитків пальців (R503), серво-привод (MG996R) та GSM-модуль (SIM800L), які є складовими розробленої системи (табл. 2.1).

Таблиця 2.1 – Порівняння середовищ реалізації

Платформа	Підтримка ESP32	Моделювання IoT-логіки	Придатність для симуляції безпеки	Вартість
Proteus Design Suite	Часткова	Обмежена	Висока	Висока
Tinkercad Circuits	Немає	Немає	Дуже обмежена	Безкоштовно
SimulIDE	Обмежена	Немає	Дуже обмежена	Безкоштовно
Wokwi IoT Simulator	Повна	Оптимальна для тестування логіки	Достатня для навчальних цілей	Безкоштовно

Wokwi підтримує емуляцію базових протоколів інтернету речей, включаючи підключення до Wi-Fi, передачу HTTP-запитів та використання MQTT для обміну повідомленнями. Хоча середовище не забезпечує реальне фізичне підключення до зовнішніх мереж або мобільних операторів, воно дозволяє змоделювати логіку роботи IoT-системи у рамках симуляції, що повністю відповідає завданням даної роботи. Можливість моделювання передачі даних, реакції на події, перевірки автентифікації користувачів та генерації тривожних сигналів робить Wokwi достатньо функціональним для створення комплексної імітації роботи розробленої системи без необхідності використання фізичних пристроїв.

Ще однією важливою перевагою Wokwi є те, що середовище є повністю доступним онлайн, не потребує встановлення програмного забезпечення на локальні машини і має безкоштовний доступ у базовій версії, що робить його оптимальним вибором для розробки академічних та дослідницьких проєктів. Простота використання, велика бібліотека віртуальних пристроїв та можливість створення інтегрованих схем на базі сучасних протоколів робить Wokwi найбільш відповідним вибором серед усіх доступних альтернатив.

Підсумовуючи проведений аналіз, можна стверджувати, що незважаючи на обмеження щодо повноцінного мережевого з'єднання, Wokwi надає оптимальні можливості для тестування внутрішньої логіки IoT-системи, моделювання взаємодії компонентів безпеки, перевірки сценаріїв реагування на події, а також забезпечення логічного контролю за системою контролю доступу та захисту периметра. Вибір Wokwi обґрунтований поєднанням гнучкості, доступності, простоти у використанні та широких можливостей для емуляції сучасних сценаріїв роботи інтелектуальних систем.

2.5 Дослідження стійкості та якості лінійних систем автоматичного управління

Стійкість систем автоматичного управління (САУ) являється базовою умовою для працездатності цієї системи, а також налічує вимогу згасання у часі перехідного процесу.

Рівняння характеристичне для лінійної неперервної САУ має вигляд:

$$a_0\lambda^n + a_1\lambda^{n-1} + \ldots + a_n = 0,$$

де a_i – задані коефіцієнти,

n – порядок системи.

Для того, щоб стверджувати, що система є стійкою достатньо лише того, що всі корені даного рівняння системи матимуть негативні дійсні частини $Re\lambda_i$<0.

Всі корені, що являються негативними дійсними частинами називаються лівими, оскільки у комплексній площині коренів вони знаходяться у лівій частині від уявної осі, а ось корені з позитивними дійсними – правими.

При дослідженні стійкості за допомогою алгебраїчних критеріїв, потрібно в першу чергу перевірити виконання всіх необхідних умов стійкості, через те, що ця перевірка не потребує розрахунків і при невиконанні даної умови стійкості розрахунки вже не потрібні.

Основною умовою стійкості системи полягає в тому, що всі коефіцієнти рівняння характеристичного повинні мати один знак. Якщо ця умова не виконується, то система буде не стійкою. У випадку виконання умови, при 3 порядку система може бути стійкою або не стійкою, а у випадку першого та другого порядку даної умови буде достатньо.

Основним критерієм стійкості є критерій Гурвіца. При цьому критерії спочатку потрібно побудувати головний визначник Гурвіца. Даний критерій будується за таким правилом: на головній діагоналі розташовують коефіцієнти у

порядку збільшення їх індексів, починаючи з a_1 та закінчуючи a_n. Для кожного стовпчика під час руху від елемента, який розташований на головній діагоналі, вверх індекси коефіцієнтів будуть збільшуватись, а вниз – зменшуватись. При цьому на місці елементів, які мають індекси більше за n (під час руху вверх), та індексамия, що менше нуля (під час руху вниз) розставляються нулі

$$\Delta_n = \begin{vmatrix} a_1 & a_3 & a_5 & \dots & 0 \\ a_0 & a_2 & a_4 & \dots & 0 \\ 0 & a_1 & a_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & 0 & 0 & a_n \end{vmatrix}.$$

Якщо викреслити в головному визначникові Гурвіца діагональні мінори, то можна отримати визначники Гурвіца нижчого порядку:

$$\Delta_1 = a_1, \quad \Delta_2 = \begin{vmatrix} a_1 & a_3 \\ a_0 & a_2 \end{vmatrix}, \quad \Delta_3 = \begin{vmatrix} a_1 & a_3 & a_5 \\ a_0 & a_2 & a_4 \\ 0 & a_1 & a_3 \end{vmatrix}.$$

З даного критерію виходить те, що при третьому порядку необхідна ще додаткова умова стійкості:

$$a_0 > 0, \quad \Delta_1 = a_1 > 0, \quad \Delta_2 = a_1 a_2 - a_0 a_3 > 0, \quad \Delta_3 = a_3 \Delta_2 > 0.$$

3 РОЗРОБЛЕННЯ СИСТЕМИ АВТОМАТИЗАЦІЇ ДЛЯ КОНТРОЛЮ ДОСТУПУ ДО ОХОРОНЮВАНОЇ ЗОНИ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ IOT

3.1 Вибір апаратної платформи

Для розробки макета системи автоматизованого контролю доступу було обрано три апаратні рішення, кожне з яких дозволяє продемонструвати різні підходи до реалізації проєкту із використанням онлайн-симулятора Wokwi. Це дало можливість не лише розробити, а й протестувати сценарії роботи системи без потреби у фізичному обладнанні, що підтримується середовищем Wokwi.

Основною платформою було обрано ESP32 завдяки його широким можливостям, зокрема наявності вбудованого Wi-Fi та Bluetooth, великої кількості пінів для підключення різноманітних пристроїв, а також сумісності з Arduino IDE та Wokwi. Це дозволило реалізувати інтеграцію з Telegram Bot API для надсилання сповіщень про статус системи, спроби доступу та тривоги. Така версія макета є найбільш функціональною, оскільки підтримує підключення до Інтернету.

Arduino Uno було використано як базову автономну платформу для моделювання офлайн-системи контролю доступу без мережевих функцій. Це популярна мікроконтролерна плата для початкового вивчення систем автоматизації. Вона дозволяє підключати кнопки, світлодіоди, сервоприводи та датчики, використовуючи стандартні бібліотеки Servo.h і LiquidCrystal.h для виведення інформації на дисплей.

Raspberry Pi Pico W було обрано для демонстрації можливостей розробки на мові MicroPython, оскільки ця платформа також підтримується у Wokwi та має вбудований Wi-Fi для інтеграції з Telegram (табл. 3.1). Крім цього, на Python було розроблено веб-застосунок для розширеного керування системою.

Таблиця 3.1 – Порівняння можливостей систем

Критерій	Arduino Uno	ESP32 DevKit V1	Raspberry Pi Pico W
Тип підключення до Інтернету	Відсутній	Вбудований Wi-Fi та Bluetooth	Вбудований Wi-Fi
Мова програмування	C++ (Arduino IDE)	C++ (Arduino IDE)	MicroPython
Підтримка Telegram Bot API	Немає	Є (через Wi-Fi, HTTPS запити)	Є (через Wi-Fi, MicroPython запити)
Сумісність з симулятором Wokwi	Повна	Повна	Часткова (підтримка MicroPython, деякі обмеження в симуляції)
Обробка простих сценаріїв доступу	Так	Так	Так
Підтримка розширених сценаріїв (мережа, API)	Немає	Є	Є
Вартість (орієнтовно)	Низька	Середня	Низька
Складність у розробці	Низька (базова система без мережі)	Середня (робота з мережевими бібліотеками)	Середня (робота з MicroPython та мережею)
Гнучкість і масштабованість	Обмежена автономною роботою	Висока завдяки мережевим функціям та інтеграціям	Висока, підходить для розширень на Python і мережевих сервісів

У макетах на всіх обраних платах були використані такі основні компоненти: дві кнопки для імітації процесу авторизації користувача за допомогою NFC-технології та відбитка пальця, світлодіоди зеленого та червоного кольорів для відображення результату авторизації – успішного або відхиленого доступу відповідно, датчик руху PIR для виявлення присутності у контрольованій зоні, потенціометр для налаштування параметрів, наприклад, часу очікування або рівня живлення, а також сервопривід, що виконує функцію імітації фізичного відкриття дверей. Водночас важливо зазначити, що в середовищі Wokwi неможливо повноцінно симулювати роботу всіх елементів реальної системи, таких як промислові камери відеоспостереження, системи протидії БпЛА, сервери зберігання даних або джерела безперебійного живлення. Ці складові залишаються логічними елементами архітектури проєкту та виконуються як реальні незалежні пристрої в промислових умовах.

Попри ці обмеження, макет у Wokwi дозволяє повністю відтворити основні функціональні сценарії – авторизацію, індикацію доступу, реагування на рух і надсилання повідомлень через Інтернет. Це забезпечує збереження концепції та логіки роботи системи, дозволяючи ефективно демонструвати та тестувати її ключові функції навіть у віртуальному середовищі.

3.2 Інтеграція з Telegram Bot API

Однією з ключових особливостей рішення є інтеграція з Telegram, що реалізована на базі ESP32 та Raspberry Pi Pico W завдяки їх можливостям підключення до Wi-Fi (рис. 3.1). Для цього було розроблено Telegram-бота, який забезпечує зручну віддалену взаємодію з системою через мобільний додаток.

Telegram-бот у розробленій системі виконує низку важливих функцій. При запуску пристрою користувач автоматично отримує повідомлення із зазначенням дати та часу активації системи. Усі спроби авторизації супроводжуються повідомленнями в Telegram, які інформують про надання або відхилення доступу. Бот також повідомляє про перехід системи в режим очікування взаємодії з користувачем, наприклад, очікування відбитка пальця чи натискання кнопки.

Крім цього, система інтегрується з публічним API для сповіщення про повітряні та артилерійські загрози в Україні, надсилаючи користувачеві актуальні тривоги безпосередньо в Telegram. Завдяки таким можливостям користувач може моніторити стан системи в реальному часі без необхідності фізично перебувати поруч, своєчасно реагувати на спроби доступу чи загрози, а також отримувати повну історію подій у зручному форматі чату. Використання Telegram-бота є важливою складовою сучасної IoT-системи, що значно підвищує її зручність, безпеку та функціональні можливості.

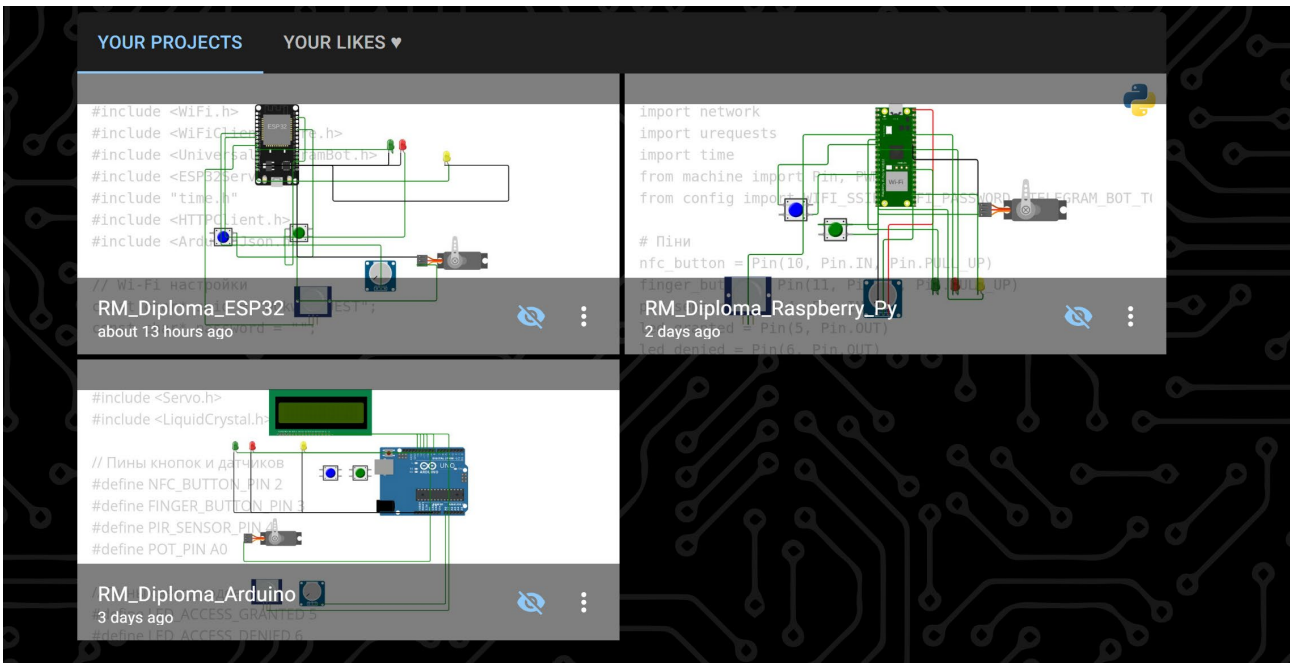

Рисунок 3.1 – Проекти Wokwi

3.3 Програмна робота на ESP32

Представимо електронну схему макету системи автоматизації контролю доступу з використанням мікроконтролера ESP32 (рис. 3.2). Дана схема реалізує логіку перевірки користувача, управління виконавчим пристроєм у вигляді сервоприводу, а також відстеження руху в зоні контролю (рис. 3.3).

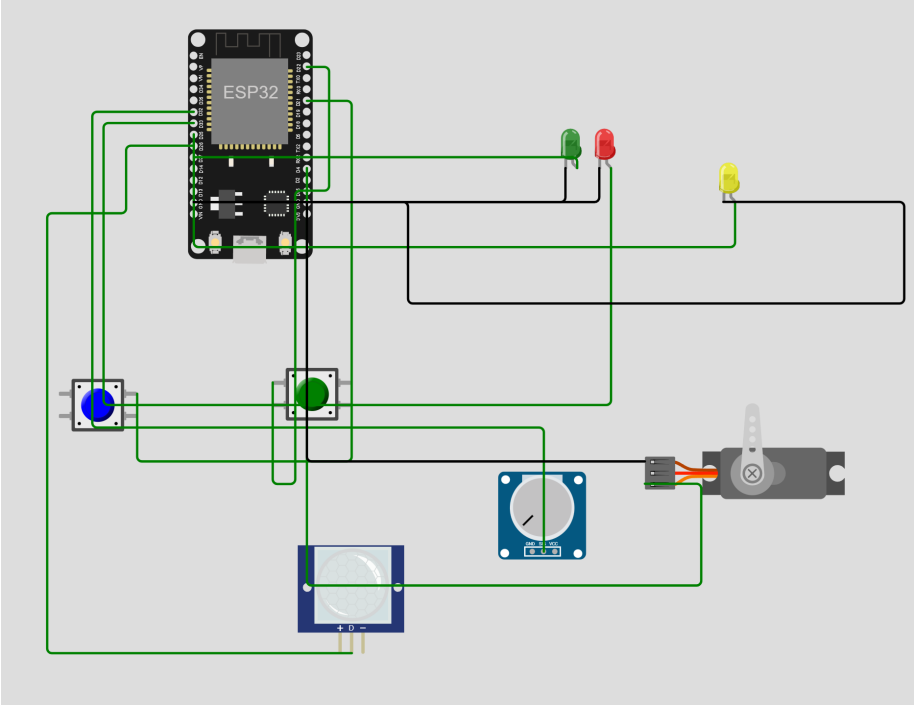

Рисунок 3.2 – ESP32 макет

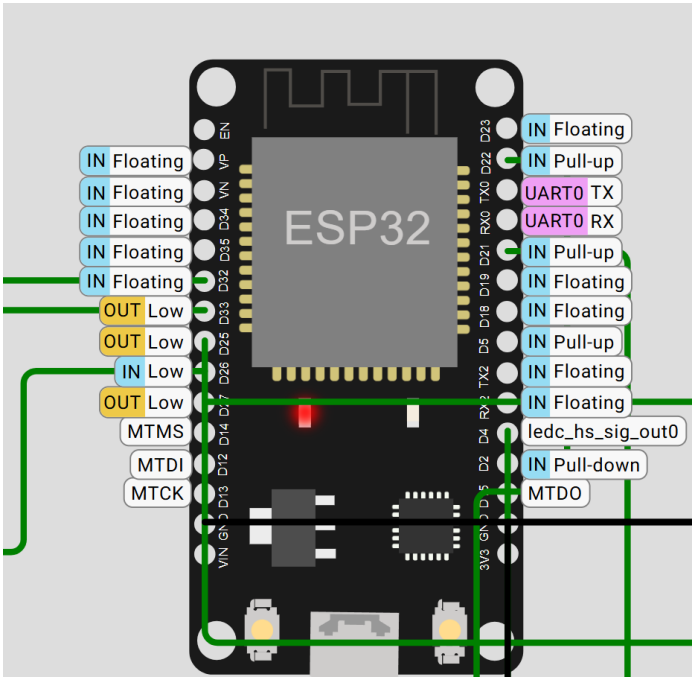

Рисунок 3.3 – ESP32 схема

Центральним елементом макету виступає мікроконтролер ESP32, до якого підключено всі необхідні компоненти. Для імітації процесу авторизації користувача використано дві кнопки. Синя кнопка умовно імітує перевірку NFC-тега, а зелена – сканування відбитка пальця. Після успішного введення імені користувача через серійний монітор та натискання обох кнопок у правильній

послідовності система надає доступ. Це супроводжується запалюванням зеленого світлодіода та плавним відкриттям серводвигуна, який імітує замок. Через кілька секунд замок автоматично зачиняється. У випадку невірного імені або неправильного порядку дій запалюється червоний світлодіод, що сигналізує про відмову в доступі.

Також до системи підключено датчик руху PIR, який виявляє присутність у зоні охорони. При спрацюванні цього датчика активується жовтий світлодіод та виводиться попередження про тривогу. Окрім цього, в систему додано потенціометр, що дозволяє імітувати рівень заряду батареї та виводити цей рівень на дисплей для візуального контролю.

Усі компоненти з’єднані згідно з представленою схемою (табл. 3.2), що дозволяє відтворити процес контролю доступу з багаторівневою перевіркою користувача, оповіщенням про спроби несанкціонованого доступу та візуалізацією стану системи. Такий макет є прикладом простої, але ефективної системи для демонстрації принципів роботи IoT-рішень у сфері безпеки та контролю доступу.

Таблиця 3.2 – Розподіл Пінів ESP32

Назва елементу	Призначення	Підключення до піну ESP32
NFC_BUTTON_PIN	Кнопка імітації авторизації через NFC	GPIO 21
FINGER_BUTTON_PIN	Кнопка імітації авторизації через відбиток пальця	GPIO 22
PIR_SENSOR_PIN	Датчик руху (PIR)	GPIO 26
POT_PIN	Потенціометр для тестування регульованих параметрів	GPIO 32
LED_GRANTED_PIN	Зелений світлодіод – доступ надано	GPIO 27

Продовження таблиці 3.2

Назва елементу	Призначення	Підключення до піну ESP32
LED_DENIED_PIN	Червоний світлодіод – доступ відхилено	GPIO 33
LED_MOTION_PIN	Світлодіод для індикації руху	GPIO 25
SERVO_PIN	Серводвигун для моделювання замка дверей	GPIO 4

Додатково до основного функціоналу система підтримує можливість автоматичного інформування про поточну безпекову ситуацію в Україні через інтеграцію з Telegram. При запуску макета система надсилає службове повідомлення до визначеного чату в Telegram (рис. 3.4) з інформацією про те, що система успішно запущена, із зазначенням поточної дати та часу. Це дозволяє користувачам віддалено переконатися в тому, що пристрій працює належним чином і готовий до виконання своїх функцій.

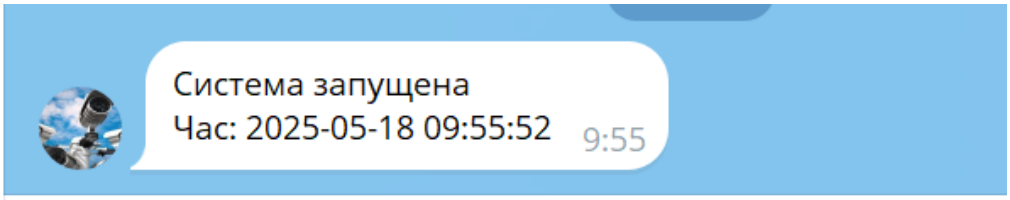

Рисунок 3.4 – Запуск системи

Одразу після запуску система здійснює перевірку наявності активних повітряних тривог або інших загроз, використовуючи зовнішній API (рис. 3.5), який надає актуальну інформацію про тривоги в різних областях України. У разі виявлення тривог користувач отримує повідомлення з переліком регіонів та типів загроз, наприклад, повітряна тривога (air_raid), артилерійський обстріл (artillery_shelling) або бойові дії в межах населених пунктів (urban_fights). Кожне таке повідомлення містить перелік областей та громад, де оголошено тривогу, а також точний час отримання інформації.

Таким чином, система не лише виконує локальний контроль доступу, але й забезпечує актуальне інформування про загрози в режимі реального часу, що значно підвищує її корисність як елементу безпеки в умовах воєнного стану або надзвичайних ситуацій. Ця реалізація виконана за допомогаю API alerts in ua.

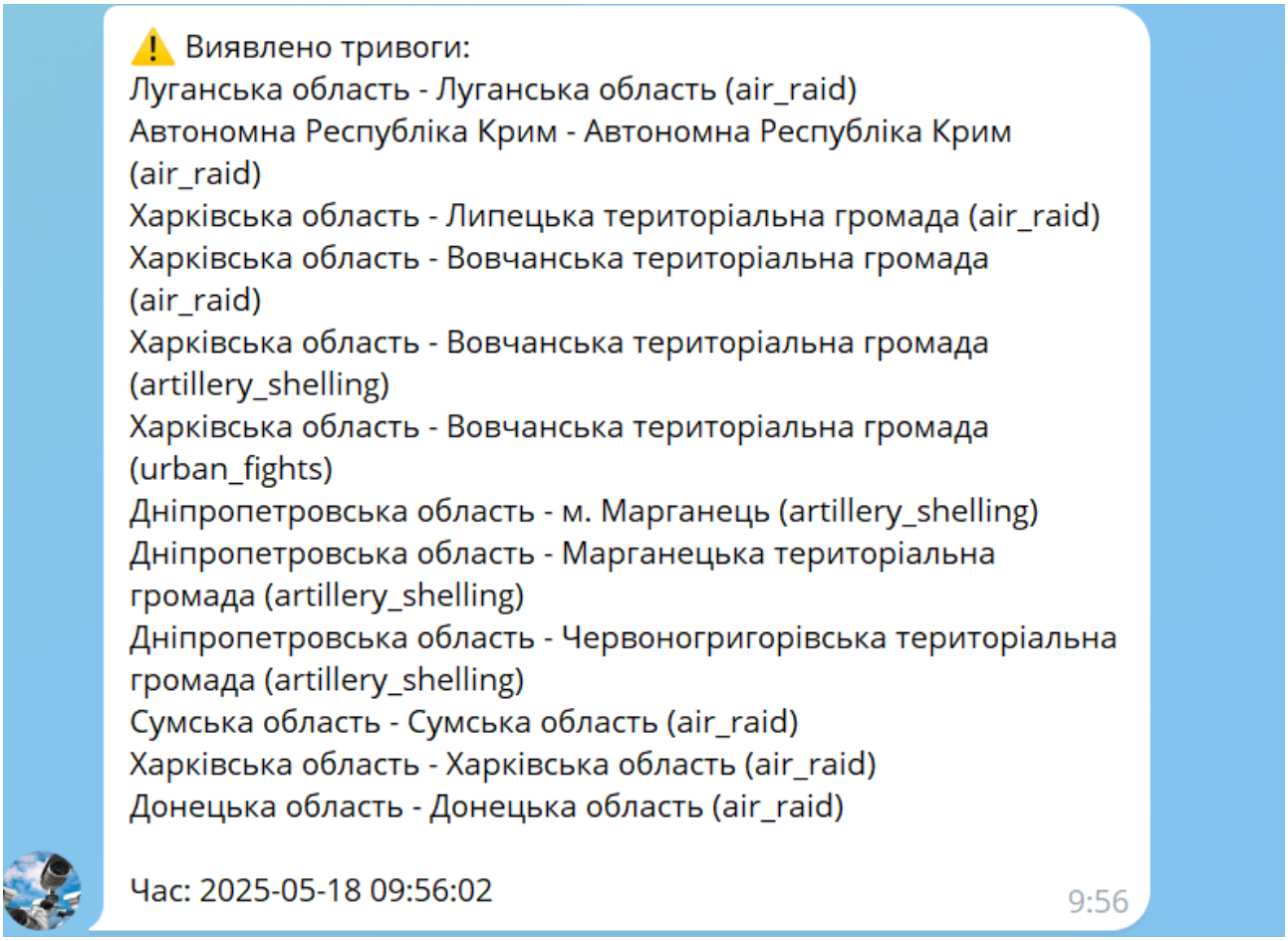

Рисунок 3.5 – Повідомлення про тривоги

Після запуску системи та перевірки безпекової ситуації через API, користувач переходить до наступного кроку. На цьому кроці система очікує натискання NFC-кнопки, що імітує прикладання картки або жетона доступу. Після натискання цієї кнопки система надсилає повідомлення в Telegram з текстом «Очікування відбитка…» (рис. 3.6) та зазначенням поточного часу. Це свідчить про те, що система перейшла в режим очікування другого фактору авторизації – підтвердження через кнопку відбитка пальця. Коли користувач натискає кнопку відбитка пальця, система успішно завершує процес перевірки, про що інформує в Telegram повідомленням «☑ Доступ надано» (рис. 3.7) разом

із фіксацією точного часу події. Одночасно з цим на макеті загоряється зелений світлодіод, що слугує візуальним підтвердженням наданого доступу. Після цього система активує сервопривід (рис. 3.8), який плавно переходить у відкрите положення (90 градусів), імітуючи відкриття замка та надання фізичного доступу користувачу. Зелений світлодіод (рис. 3.9) залишається увімкненим протягом усього часу, поки замок відкритий, а після автоматичного закриття замка він гасне, що сигналізує про завершення сеансу доступу.

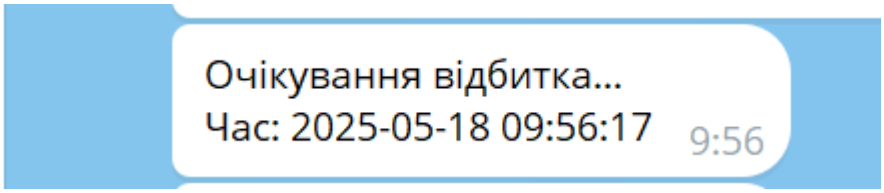

Рисунок 3.6 – Очікування відбитка

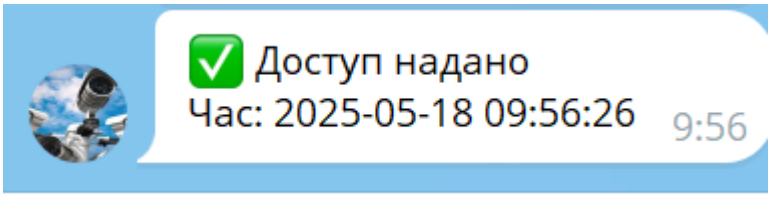

Рисунок 3.7 – Повідомлення про надання доступу

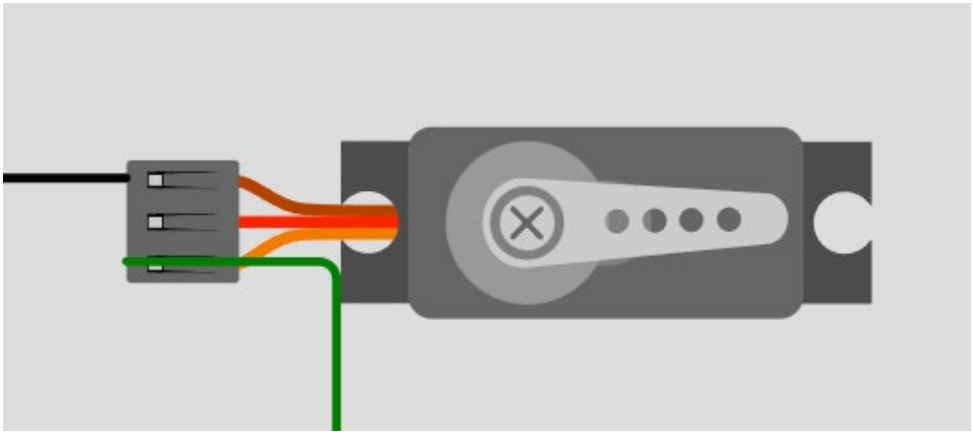

Рисунок 3.8 – Сервопривід

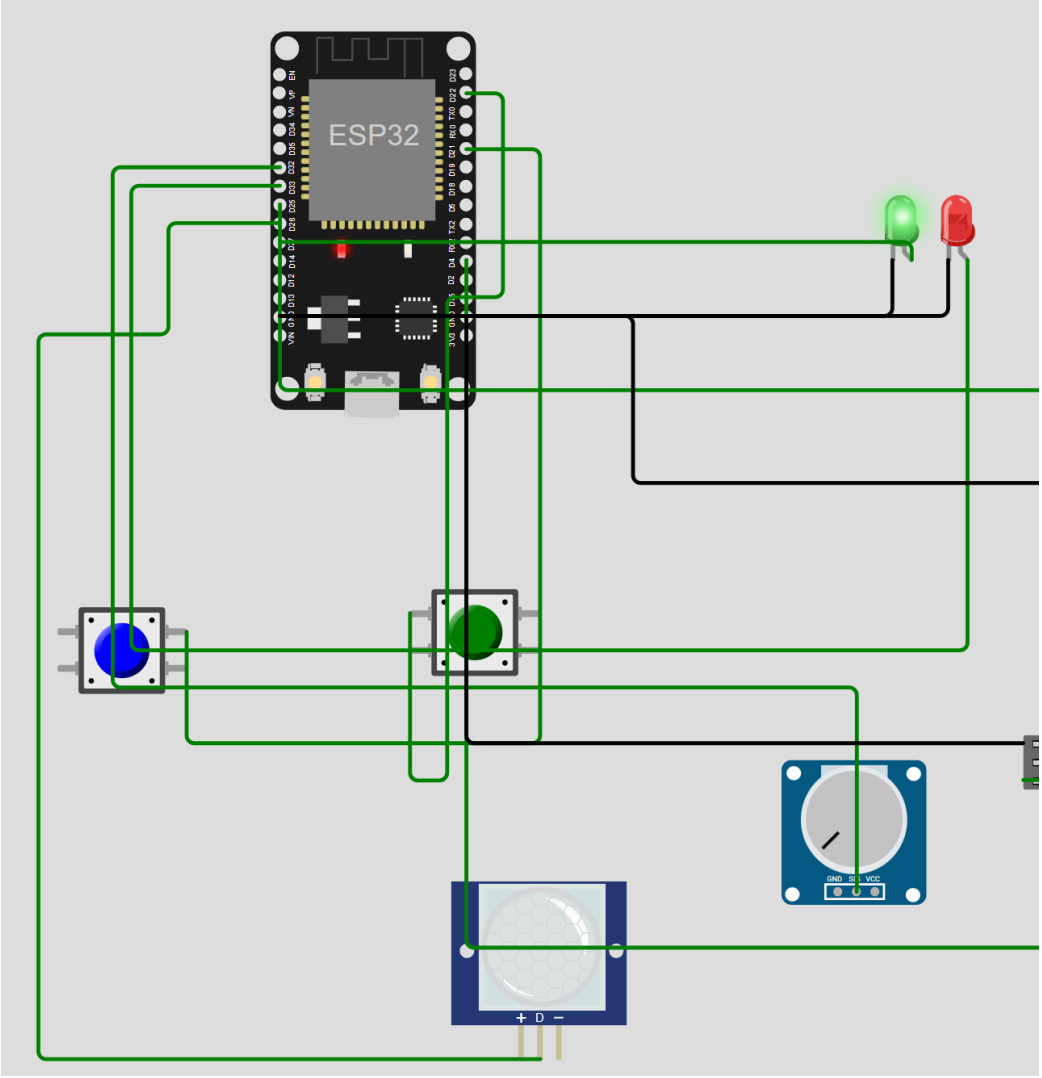

Рисунок 3.9 – Активація зеленого світлодіода

Якщо користувач натискає NFC-кнопку, але протягом визначеного часу (наприклад, 15 секунд) не підтверджує доступ натисканням кнопки відбитка пальця, система автоматично завершує спробу авторизації з результатом «Доступ відхилено» (рис. 3.10). Відповідне повідомлення з фіксацією часу події надсилається в Telegram, щоб проінформувати користувача або адміністратора про невдалу спробу доступу. Окрім цього, на самому макеті вмикається червоний світлодіод (рис. 3.11), який візуально сигналізує про те, що доступ не було надано. Це дозволяє одразу на місці бачити результат спроби, навіть без перевірки Telegram. Після короткої затримки червоний світлодіод гасне, а система повертається до початкового стану, очікуючи на введення нового імені користувача для наступної спроби авторизації.

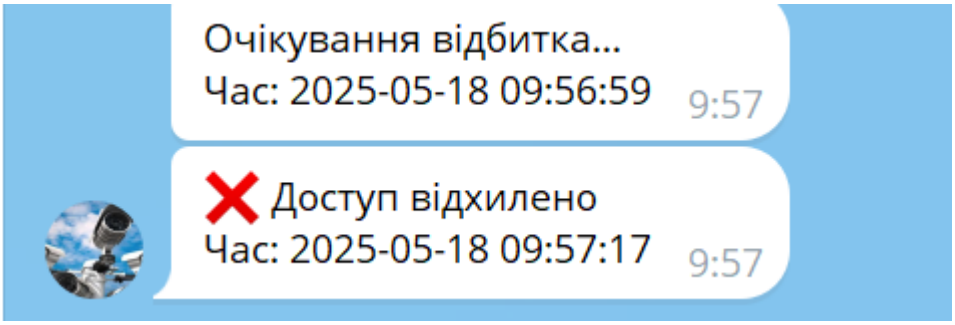

Рисунок 3.10 – Повідомлення про відхилення доступу

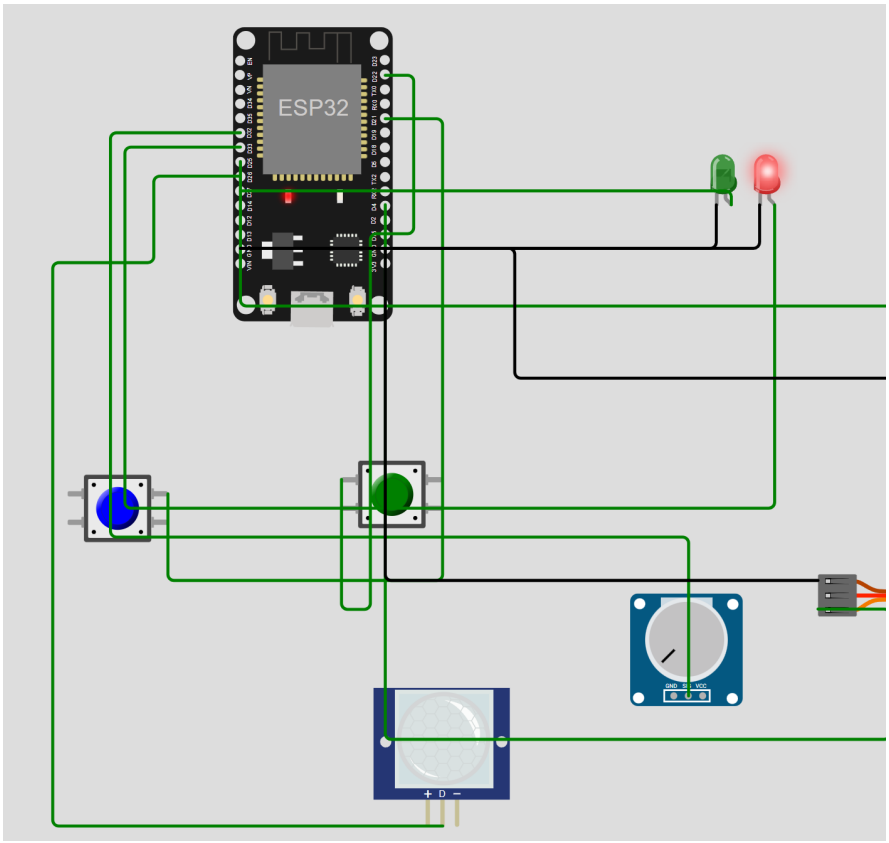

Рисунок 3.11 – Активація червоного світлодіода

Для додаткового підвищення безпеки система оснащена модулем виявлення руху PIR (Passive Infrared Sensor). Датчик постійно відслідковує рух у зоні контролю і спрацьовує, коли фіксує зміну інфрачервоного випромінювання, що відповідає руху людини або іншого об'єкта.

Після виявлення руху система миттєво активує жовтий світлодіод (рис. 3.12), який сигналізує про тривогу на місці встановлення пристрою. Одночасно користувач або відповідальна особа отримує повідомлення у Telegram із

зазначенням часу спрацювання, наприклад, « 🚨 Виявлено рух!» (рис. 3.13) разом із поточною датою та часом події.

Завдяки цьому система виконує не лише контроль доступу, але й функцію охоронного моніторингу, що дозволяє оперативно реагувати на несанкціоновані переміщення у визначеній зоні. Така інтеграція підвищує рівень захищеності об'єкта та забезпечує віддалене сповіщення про потенційні загрози.

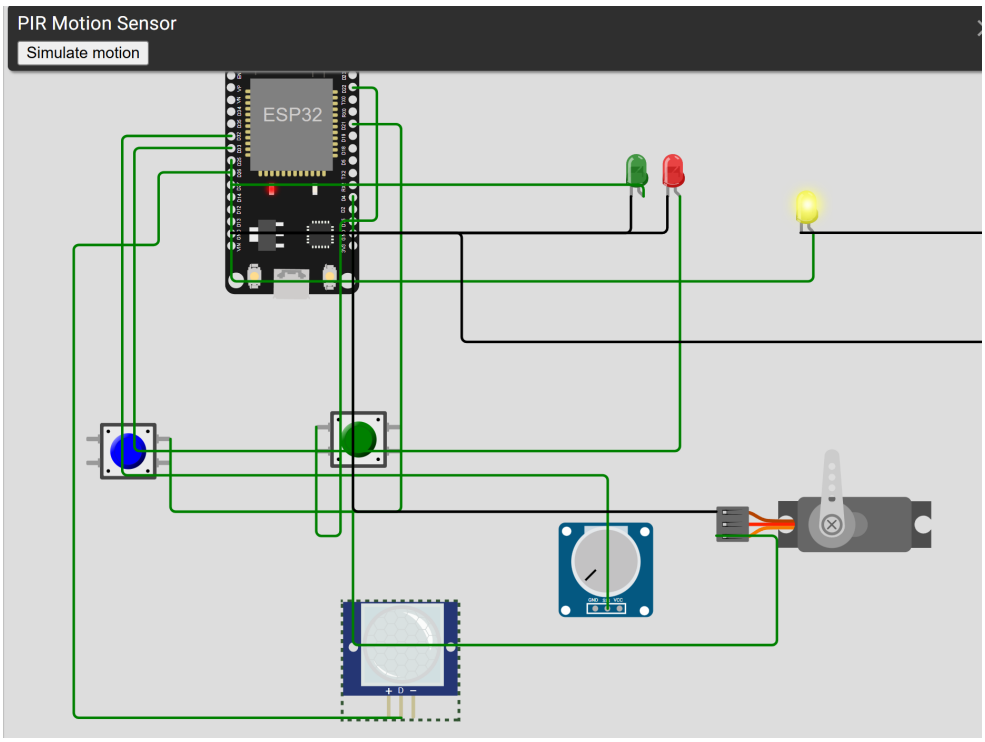

Рисунок 3.12 – Активація жовтого світлодіода

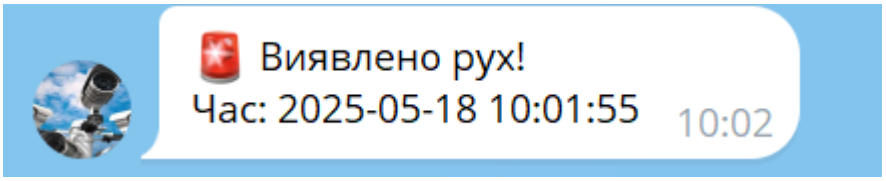

Рисунок 3.13 – Повідомлення про рух.

У макеті реалізовано можливість імітації рівня заряду живлення системи за допомогою потенціометра. Потенціометр підключений до аналогового входу мікроконтролера ESP32 і використовується для зчитування значення напруги, що дозволяє визначати поточний рівень умовного заряду батареї.

Користувач може обертати потенціометр, змінюючи його положення від мінімального до максимального (рис. 3.14). Отримане значення відображається на екрані макета у вигляді відсотків. Додатково, якщо потенціометр встановлений у максимальне положення, система надсилає попереджувальне повідомлення в Telegram, наприклад: «⚠ Потенціометр в максимальному положенні!» (рис. 3.15) з фіксацією поточного часу. Це дозволяє дистанційно контролювати стан живлення системи. Таким чином, потенціометр виконує роль симулятора батареї або джерела живлення, забезпечуючи можливість тестування поведінки системи при різному рівні напруги. За потреби цей функціонал може бути замінений або доповнений реальним моніторингом стану акумулятора або блоку живлення.

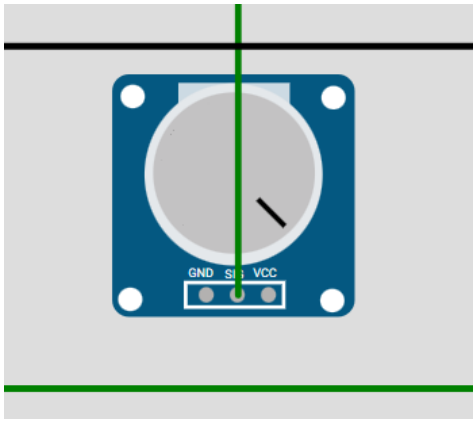

Рисунок 3.14 – Потенціометр у максимальному положенні

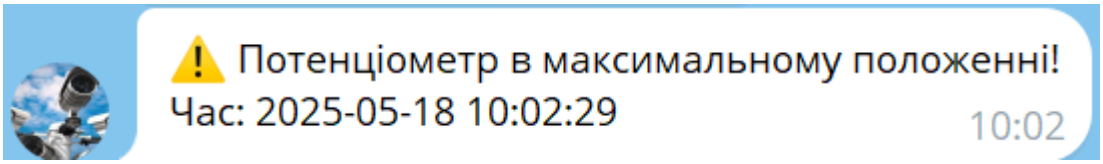

Рисунок 3.15 – Повідомлення у телеграмі

3.4 Програмна робота на Arduino UNO

У другому варіанті представлено електронну схему макету системи автоматизації контролю доступу з використанням мікроконтролера Arduino Uno (рис. 3.16). Дана схема реалізує логіку багаторівневої перевірки користувача,

управління виконавчим пристроєм у вигляді сервоприводу, а також виявлення руху в зоні контролю.

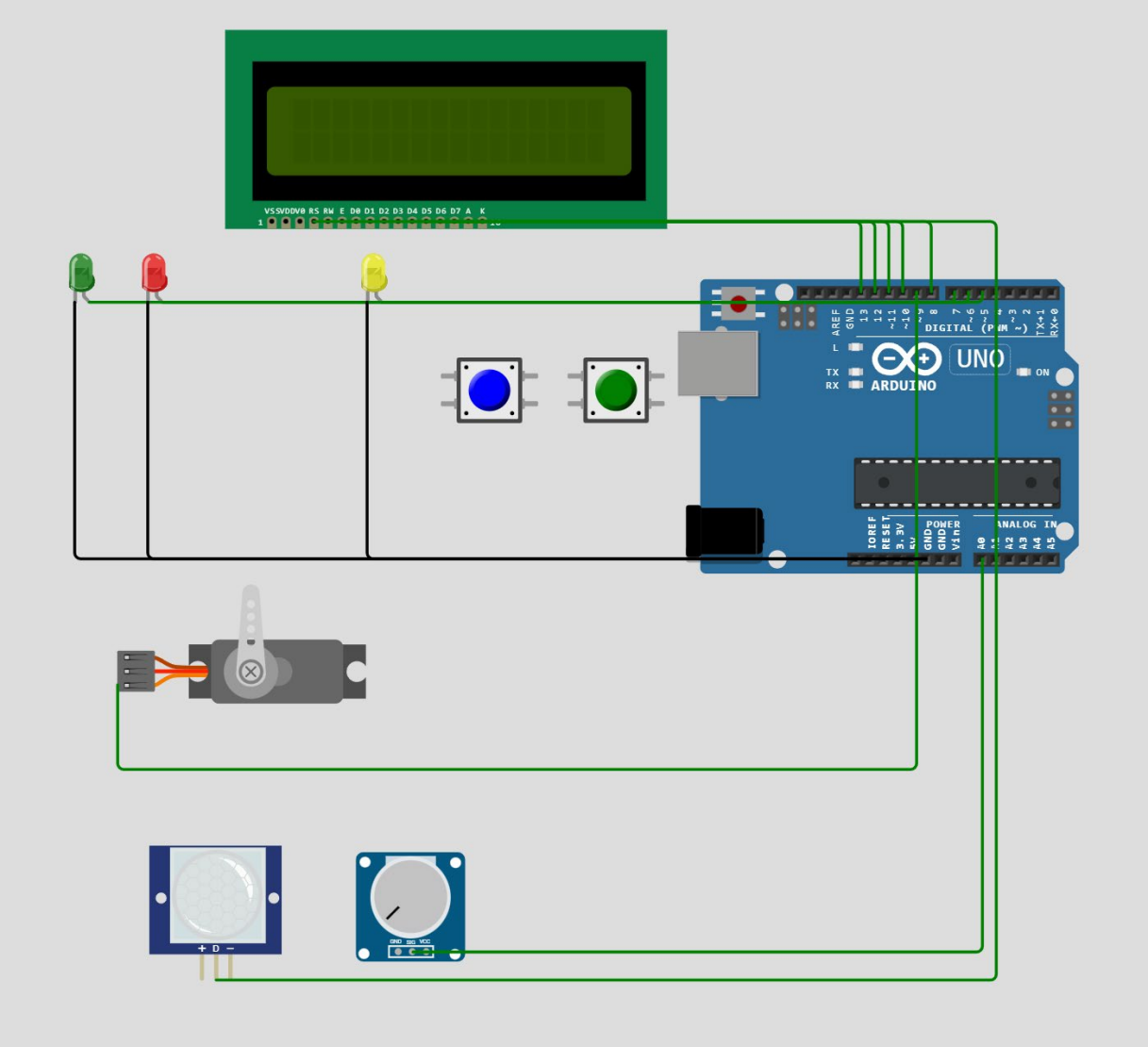

Рисунок 3.16 – Макет Arduino UNO

Центральним елементом макету виступає мікроконтролер Arduino Uno (рис. 3.17), до якого підключені всі необхідні компоненти. Для імітації процесу авторизації використано дві кнопки: синя – для моделювання зчитування NFC-картки, та зелена – для підтвердження доступу відбитком пальця. При успішному проходженні цих етапів система виводить інформацію на рідкокристалічний дисплей (LCD), запалює зелений світлодіод та активує сервопривід, який імітує відкриття замка. Через кілька секунд сервопривід повертається у вихідне положення, імітуючи закриття замка. У разі помилки чи неправильного порядку

дій на дисплеї виводиться повідомлення про відмову, а червоний світлодіод сигналізує про відхилення доступу.

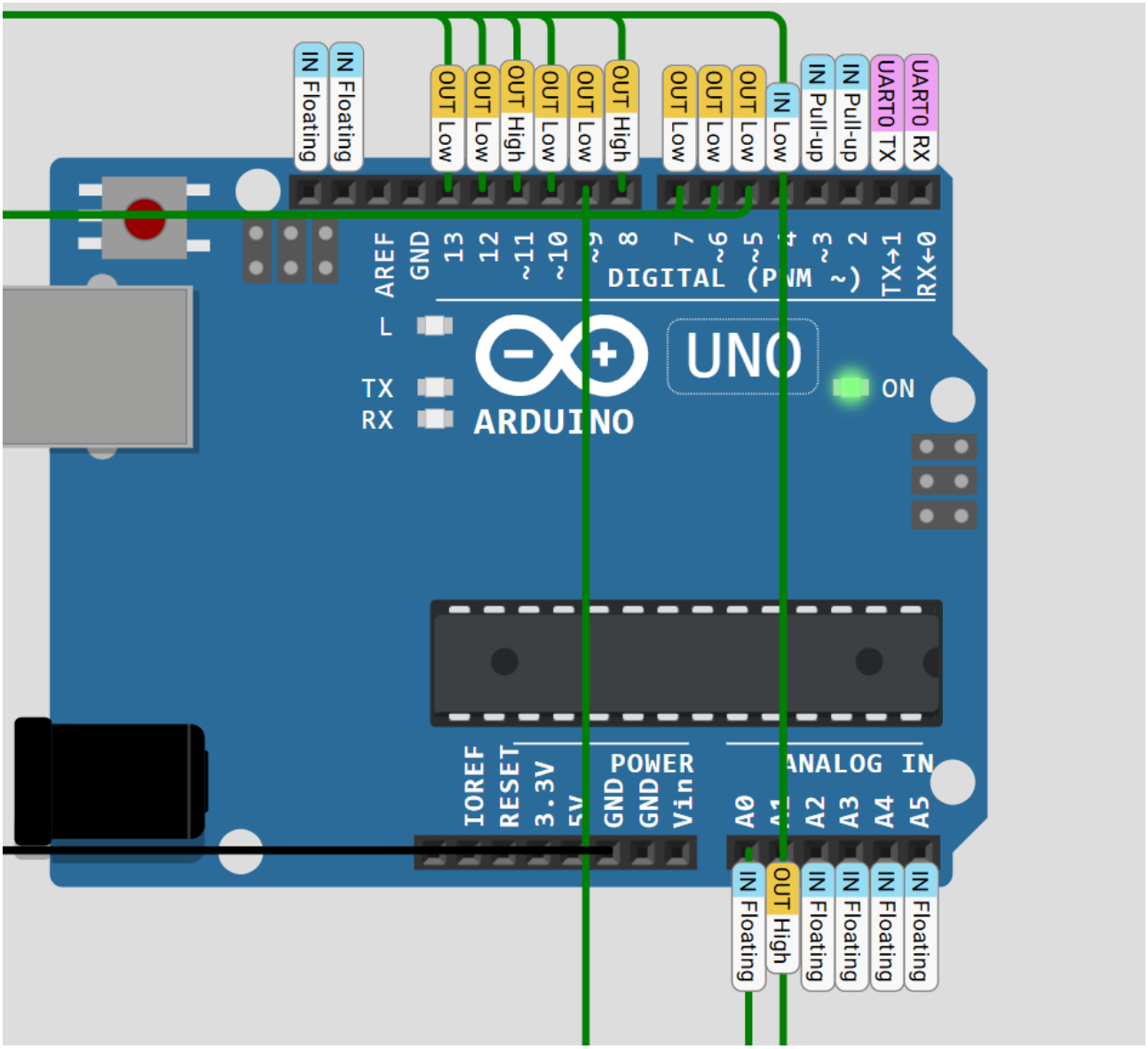

Рисунок 3.17 – Схема Arduino UNO

Крім авторизації, система оснащена датчиком руху PIR, який дозволяє виявляти присутність у зоні контролю. У випадку спрацювання датчика на дисплей виводиться попередження про рух, і жовтий світлодіод сигналізує про тривогу.Також до системи підключено потенціометр, що дозволяє моделювати різні параметри, зокрема рівень "заряду батареї" або затримку доступу. Значення з потенціометра виводиться на дисплей для наочного контролю.

На відміну від макета на ESP32, дана версія не підтримує підключення до мережі Інтернет та надсилання повідомлень через Telegram, оскільки Arduino Uno не має вбудованих мережевих модулів. Проте цей макет ідеально підходить для демонстрації автономної локальної системи контролю доступу, яка не залежить від підключення до Інтернету. Усі компоненти з'єднані відповідно до представленої схеми, що дозволяє наочно продемонструвати базові принципи роботи автономної системи контролю доступу з використанням доступних апаратних засобів.

Розподіл пінів Arduino UNO представлено в табл. 3.3.

Таблиця 3.3 – Розподіл пінів Arduino UNO

Назва елементу	Призначення	Підключення до піну ESP32
NFC_BUTTON_PIN	Кнопка імітації авторизації через NFC	D2
FINGER_BUTTON_PIN	Кнопка імітації авторизації через відбиток пальця	D3
PIR_SENSOR_PIN	Датчик руху (PIR)	D4
POT_PIN	Потенціометр для тестування регульованих параметрів	A0
LED_GRANTED_PIN	Зелений світлодіод – доступ надано	D5
LED_DENIED_PIN	Червоний світлодіод – доступ відхилено	D6
ALARM_LED_PIN	Світлодіод для індикації руху	D7
SERVO_PIN	Серводвигун для моделювання замка дверей	D9

Після ввімкнення системи на рідкокристалічному дисплеї (LCD) з'являється повідомлення «System is ready», що свідчить про успішний запуск (рис. 3.18) і готовність системи до роботи. Одночасно в серійному моніторі

виводиться запит на введення імені користувача. Це є стартовим етапом для початку процедури авторизації. У фоновому режимі система постійно зчитує значення з потенціометра, який виконує роль симулятора рівня заряду живлення. Поточний рівень відображається на дисплеї у вигляді відсоткового значення, наприклад «Power: 54 %» (рис. 3.19). Це дозволяє оператору контролювати умовний рівень заряду акумулятора або джерела живлення системи. Дана функціональність є корисною для демонстрації того, як система може відображати технічний стан живлення, що є важливим для забезпечення стабільної роботи пристрою в реальних умовах. Оператор отримує наочний індикатор рівня енергії без необхідності звертатися до додаткових вимірювальних пристроїв або програмних інструментів.

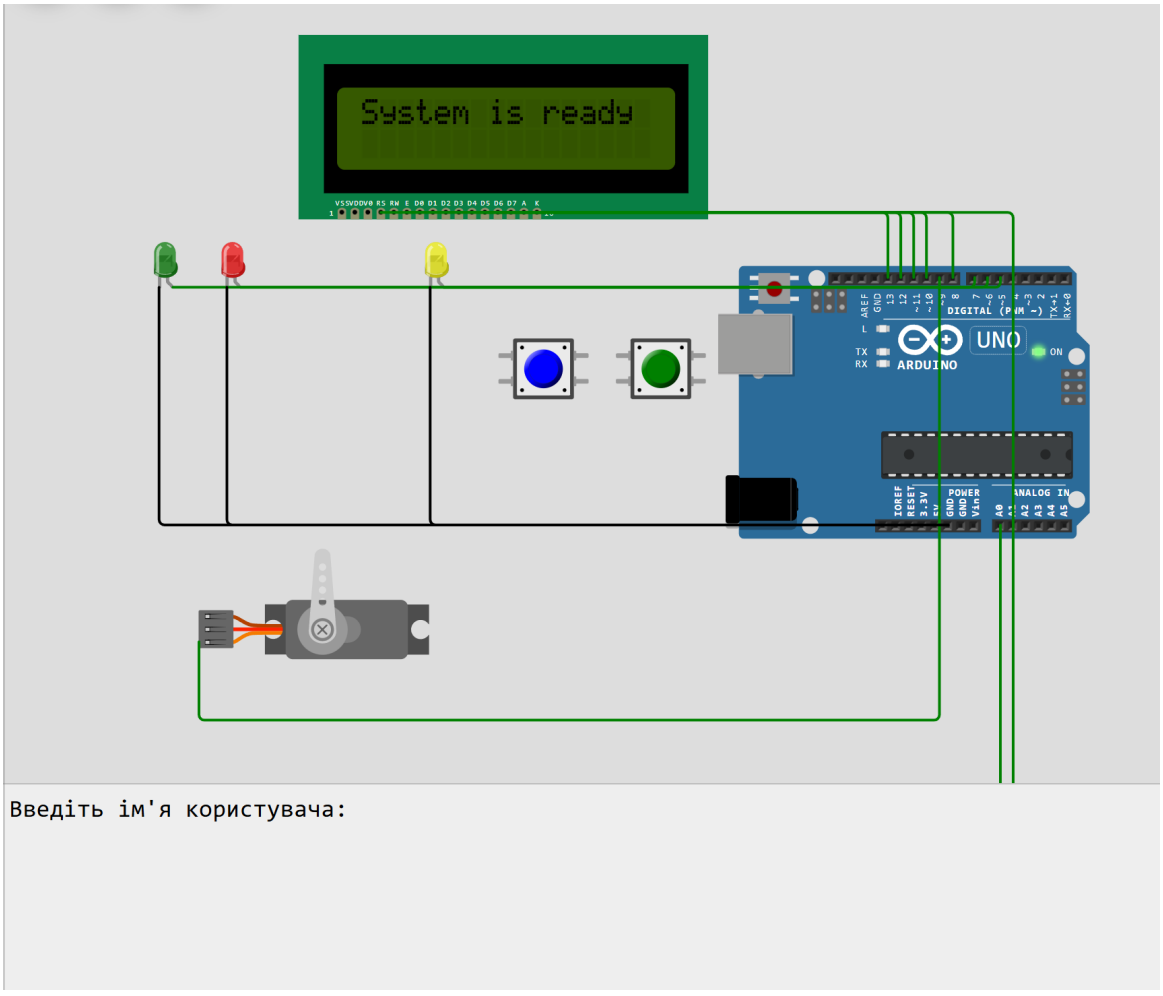

Рисунок 3.18 – Запуск системи

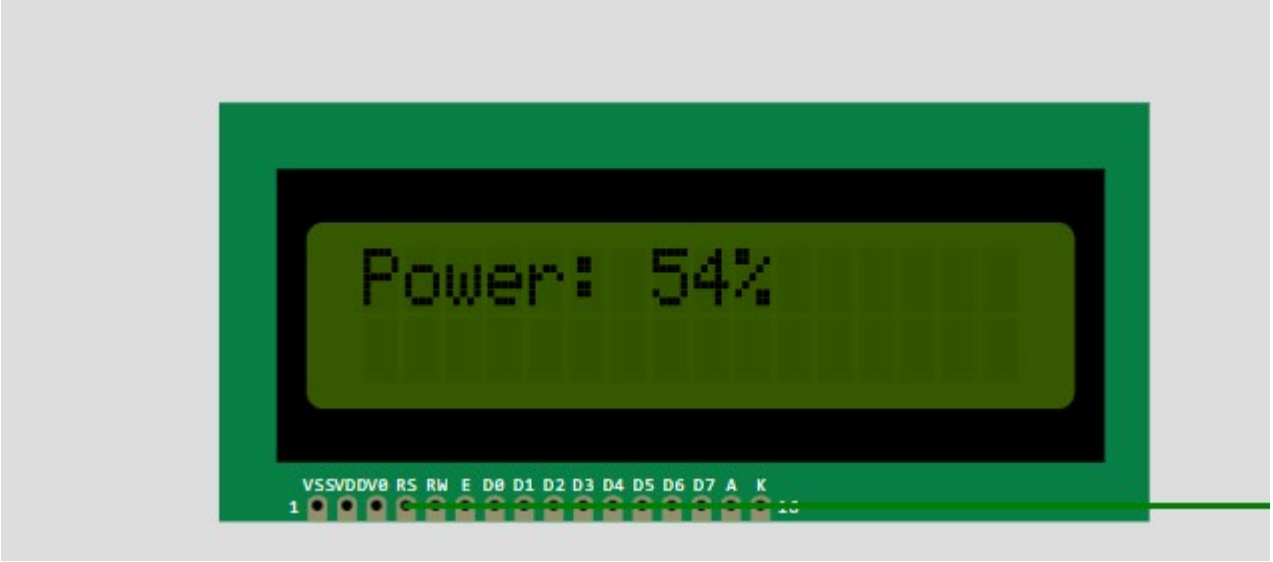

Рисунок 3.19 – Відображання заряду

Продемонстровано сценарій, коли користувач вводить неправильне ім’я, яке відсутнє у списку дозволених. У відповідь система миттєво блокує доступ і повідомляє про це як на рідкокристалічному дисплеї (рис. 3.20), так і через серійний монітор.

На дисплеї виводиться повідомлення «Access Denied», що супроводжується запалюванням червоного світлодіода. У серійному моніторі відображається відповідне повідомлення з червоним хрестиком «❌ Доступ відхилено». Система одразу повертається в початковий стан і пропонує повторити введення імені, запрошуючи користувача ще раз спробувати авторизуватись.

Така поведінка системи гарантує захист від несанкціонованого доступу. Користувач одразу отримує зрозумілий зворотний зв’язок щодо результату спроби авторизації. Завдяки цьому підвищується зручність користування та інтуїтивність взаємодії з пристроєм.

Система залишається готовою до подальших дій та забезпечує безперервний контроль доступу.

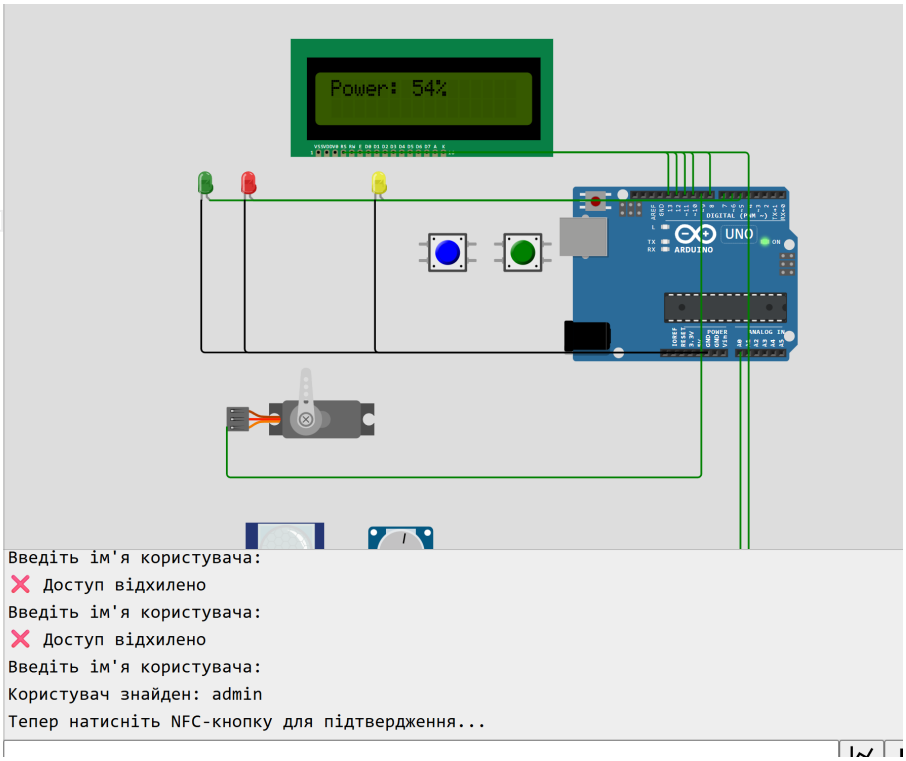

Рисунок 3.20 – Некоректний користувач

Водночас на дисплеї продовжує оновлюватися значення рівня живлення, наприклад «Power: 54 %», що забезпечує постійний моніторинг умовного стану енергоживлення системи.

Таким чином, система демонструє чіткий зворотний зв’язок при спробі несанкціонованого доступу, не дозволяючи перейти до наступного етапу перевірки та не активуючи виконавчі пристрої, що забезпечує безпеку і передбачувану поведінку системи.

Користувач вводить ім’я «admin», яке присутнє у списку дозволених. Система розпізнає користувача, про що повідомляє на дисплеї та в серійному моніторі. На дисплеї з’являється повідомлення «Тепер натисніть NFC-кнопку для підтвердження…», після чого система переходить до етапу очікування другого фактора авторизації – натискання кнопки, що імітує сканування відбитка пальця. Після натискання обох кнопок у правильній послідовності система виводить повідомлення «Access granted» та «Доступ наданий користувачу: admin». Зелене підсвічування світлодіода сигналізує про успішне надання доступу.

Також видно, що сервопривід перейшов у відкрите положення, імітуючи відкриття дверей для користувача. Це підтверджує правильне виконання всієї

послідовності дій – перевірку імені, очікування підтвердження через NFC і відбиток, активацію зеленої індикації (рис. 3.21) та фізичне відкриття механізму замка (рис. 3.22). Система готова знову повернутися до очікування наступного користувача після автоматичного закриття серво.

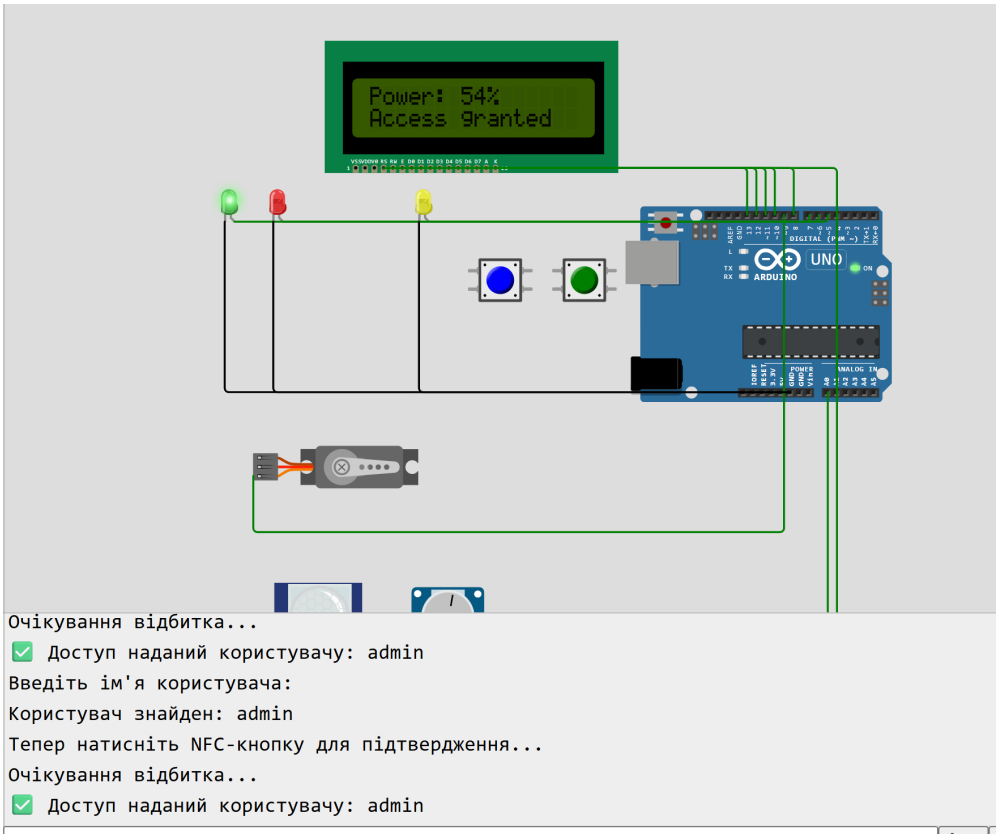

Рисунок 3.21 – Доступ наданий користувачу

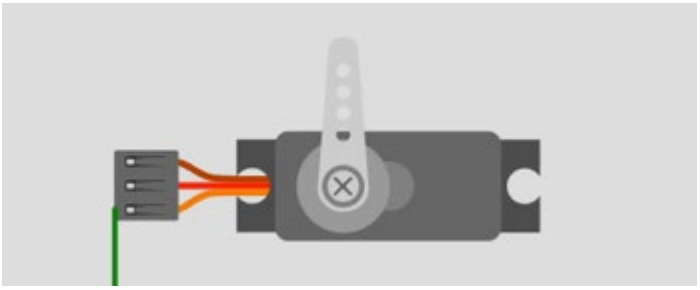

Рисунок 3.22 – Відкриття серво-привода

Після натискання NFC-кнопки система переходить у режим очікування натискання кнопки, яка імітує зчитування відбитка пальця. Це відображається на дисплеї повідомленням «Waiting Finger...», а також у серійному моніторі як «Очікування відбитка...» (рис. 3.23). Система надає користувачу обмежений час

для підтвердження своєї особи. Якщо протягом цього часу користувач не натискає кнопку відбитка пальця, система завершує спробу авторизації як невдалу. На дисплеї з'являється повідомлення «Access Denied», а у серійному моніторі – «❌ Доступ відхилено (не надано відбиток)». Одночасно загоряється червоний світлодіод, що сигналізує про відмову в доступі (рис. 3.24).

Після цього система повертається до початкового стану та знову запитує ім’я користувача, дозволяючи розпочати нову спробу авторизації. Такий механізм забезпечує додатковий рівень безпеки, запобігаючи безкінечному очікуванню та змушуючи користувача повторити повний процес ідентифікації.

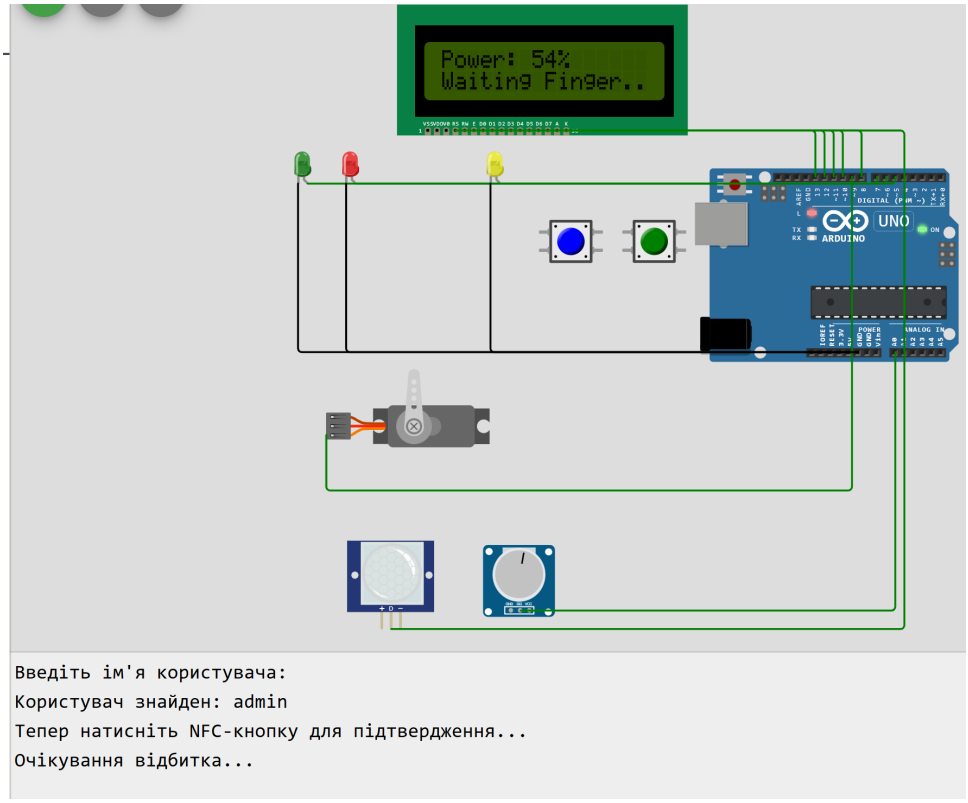

Рисунок 3.23 – Очікування відбитка

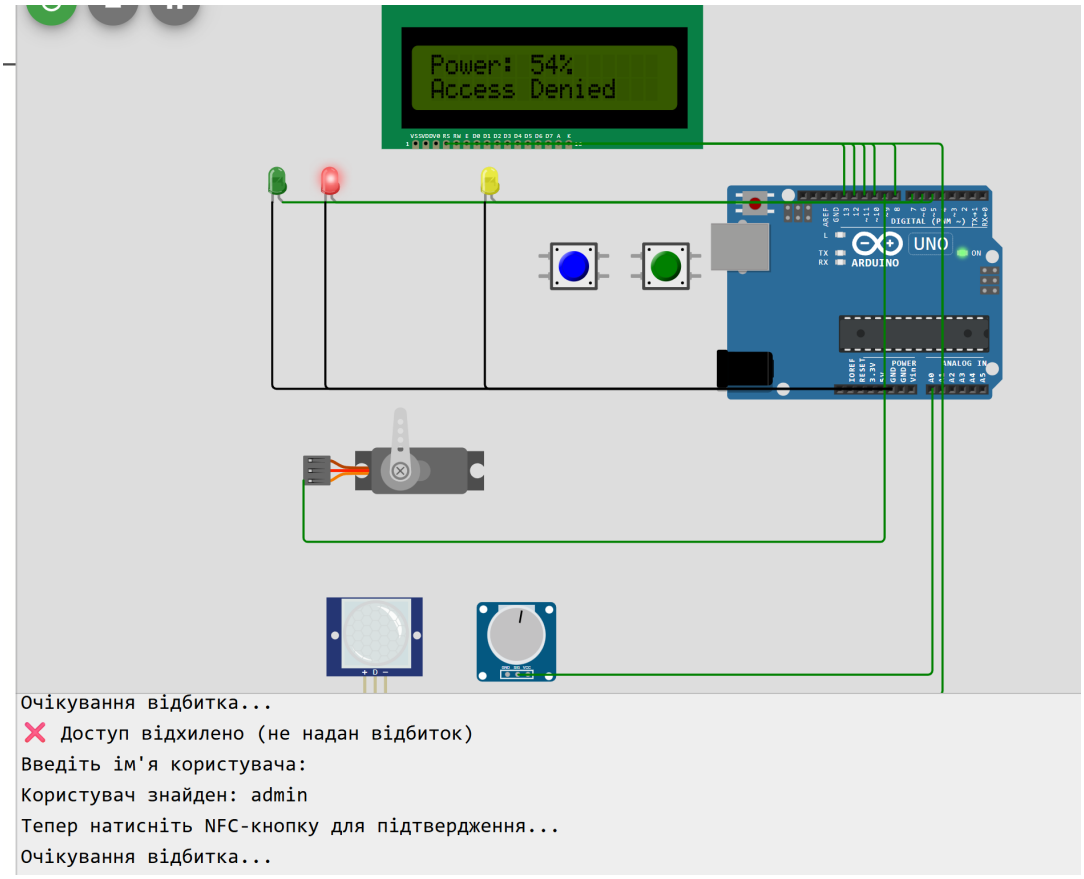

Рисунок 3.24 – Невдала спроба входу

Також система спроможня переходити у режим тривоги при виявленні руху. Це реалізовано за допомогою PIR-датчика руху, що постійно контролює простір перед пристроєм.

При фіксації руху система виводить на LCD-дисплей повідомлення «ALARM! Movement» разом з поточним рівнем живлення (рис. 3.25), активує жовтий світлодіод, що сигналізує про тривогу, відображає серію повідомлень «Тривога! Виявлено рух» у серійному моніторі (рис. 3.26). Цей механізм дозволяє оперативно реагувати на будь-які несанкціоновані переміщення в зоні охорони. Система багаторазово дублює повідомлення в серійному моніторі, що свідчить про безперервну реакцію на рух доти, доки датчик продовжує фіксувати активність.

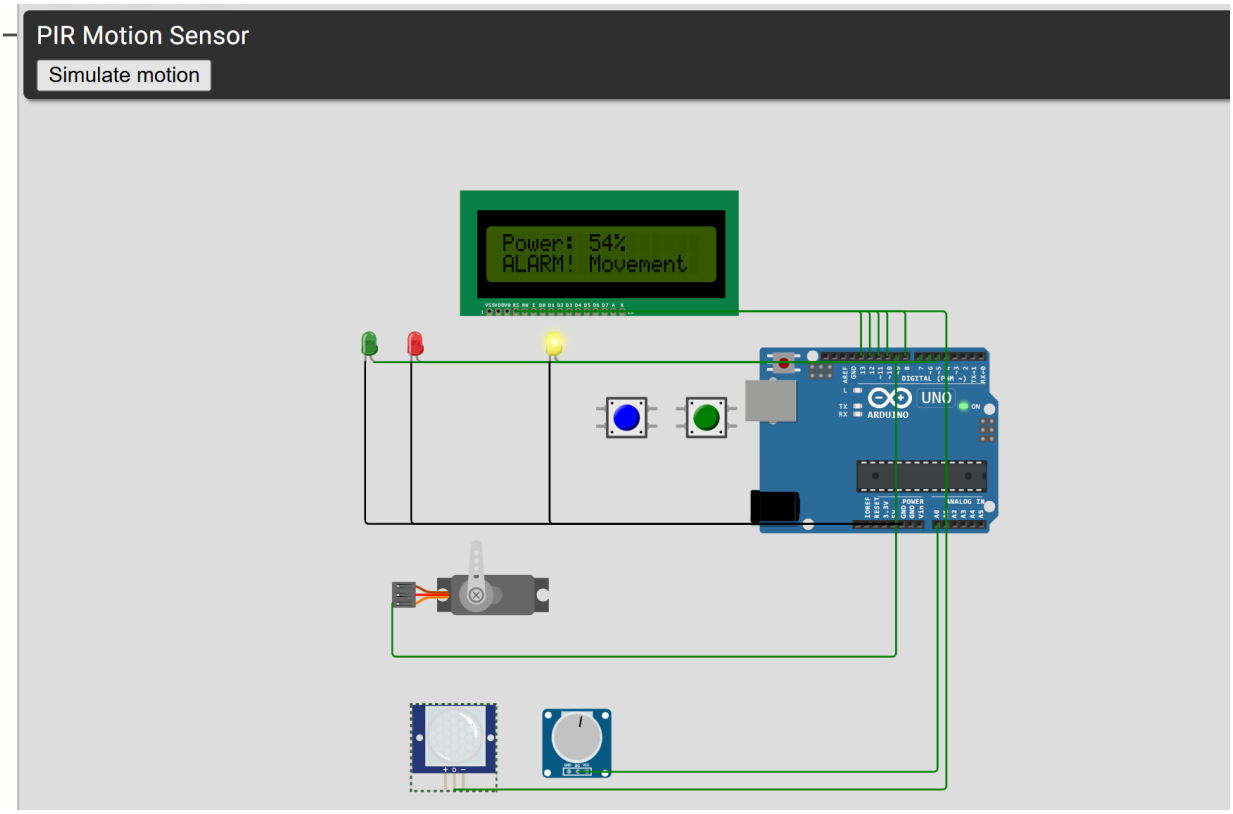

Рисунок 3.25 – Pir Motion Sensor реакція

```
Тривога! Виявен рух
Тривога! Виявен рух
Тривога! Виявен рух
Тривога! Виявен рух
Тривога! Виявен рух
```

Рисунок 3.26 – Сповіщення про виявлення руху

Така поведінка (рис. 3.26), імітує постійне моніторування з негайним візуальним та інформаційним сповіщенням що є важливою функцією для систем контролю доступу та охорони периметра.

3.5 Програмна робота на Raspberry Pico W

У рамках третього варіанту реалізації системи було розроблено макет на базі мікроконтролера Raspberry Pi Pico W (рис. 3.27). Цей пристрій обрано

завдяки його компактності, енергоефективності та підтримці бездротового зв’язку Wi-Fi, що дозволяє інтегрувати макет у мережу Інтернету речей. Додатковою перевагою стала можливість програмування мовою MicroPython, яка забезпечує простий синтаксис, широкий набір бібліотек та підтримку роботи з мережею і зовнішніми пристроями.

Макет було змодельовано у середовищі Wokwi, яке підтримує Raspberry Pi Pico W та дозволяє тестувати основні функції (табл. 3.4) без потреби у фізичних компонентах (рис. 3.28). У конструкції передбачено імітацію перевірки доступу за допомогою двох кнопок – одна з яких відповідає за успішну аутентифікацію користувача, інша – за відмову у доступі. Система додатково оснащена датчиком руху PIR, який реагує на рух у зоні контролю. Для візуального зворотного зв’язку передбачено три світлодіоди: зелений сигналізує про успішний доступ, червоний – про відмову, а жовтий спрацьовує при виявленні руху. Для моделювання відкривання або закривання фізичного замка використовується сервопривід, що обертається у разі дозволеного доступу.

Особливістю цього макета є інтеграція з Telegram Bot API. Програма з'єднується з Wi-Fi мережею та надсилає адміністратору сповіщення про всі події в системі – спроби доступу, їх результат та виявлення руху. Таким чином забезпечується віддалений моніторинг у режимі реального часу. Програмне забезпечення на MicroPython опрацьовує сигнали від кнопок та датчика, керує світлодіодами та сервоприводом, а також формує повідомлення для Telegram.

На схемі розведено окремі з'єднання для всіх елементів системи. Кнопки і датчик підключені до цифрових входів, потенціометр – до аналогового входу, а світлодіоди та сервопривід – до цифрових виходів. Завдяки використанню Raspberry Pi Pico W вдалося створити компактний і багатофункціональний макет (табл. 3.4), який дозволяє продемонструвати принципи побудови сучасних IoT-систем контролю доступу з віддаленим керуванням та моніторингом.

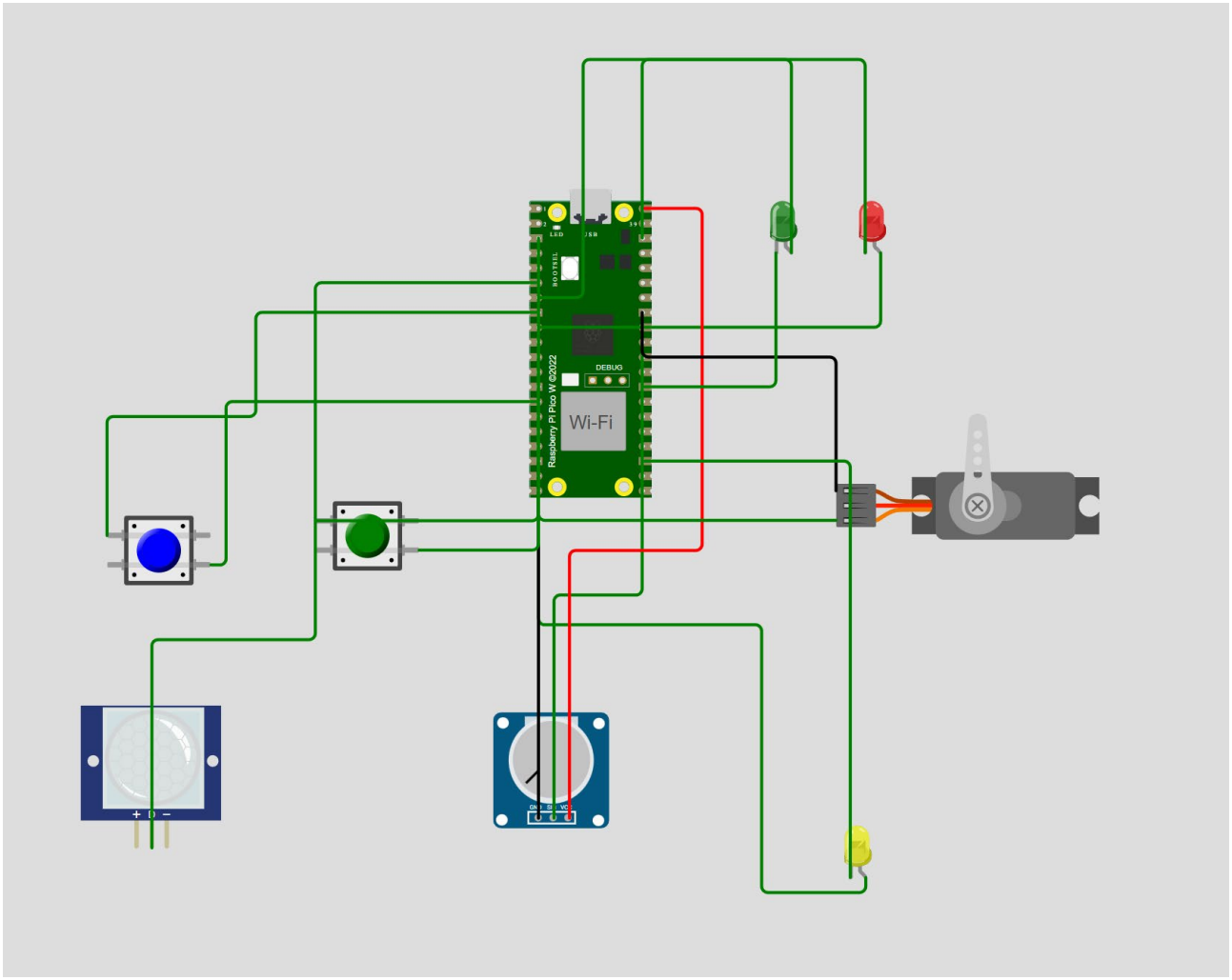

Рисунок 3.27 – Макет Raspberry Pico W

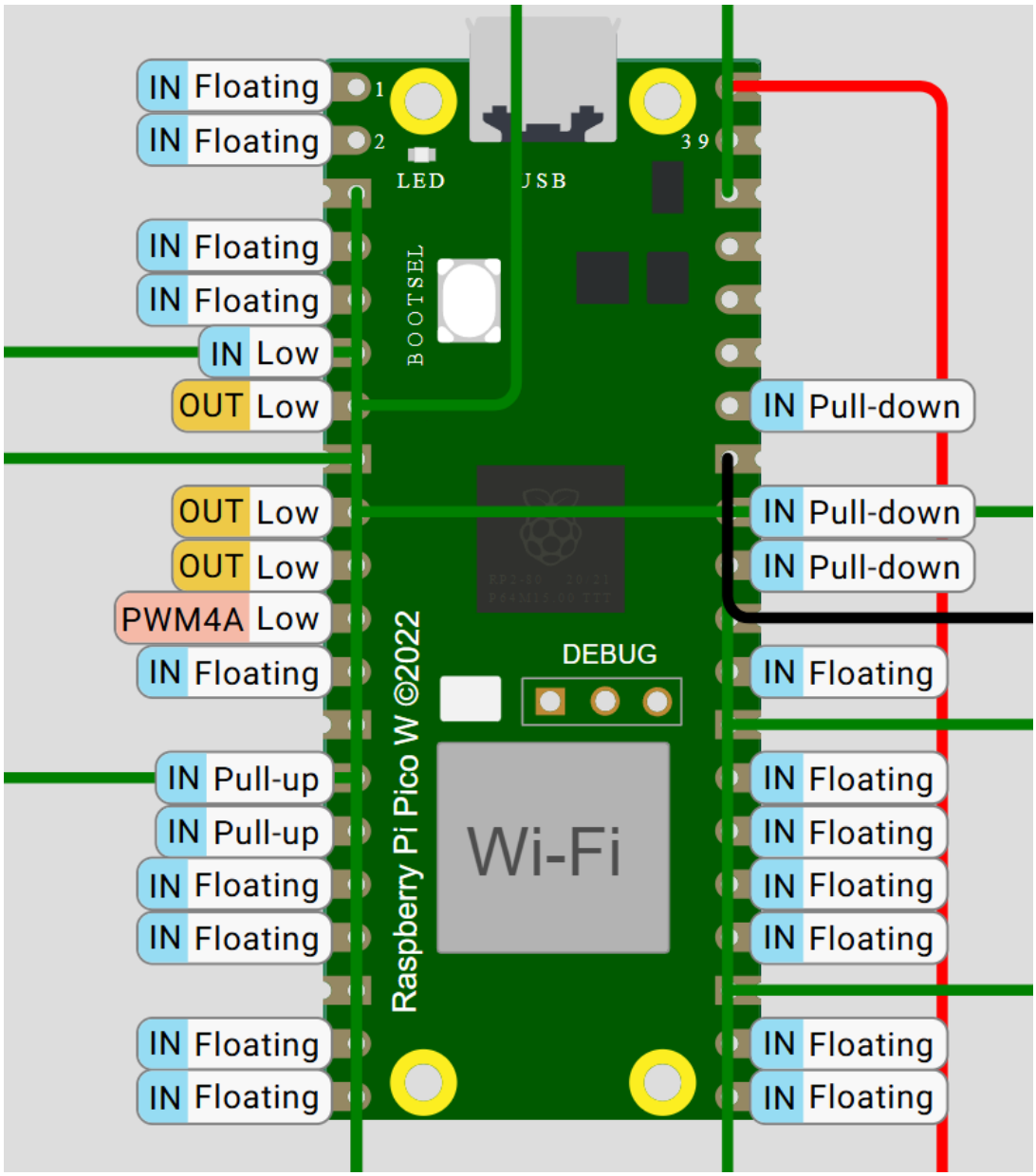

Рисунок 3.28 – Схема Raspberry Pico W

Таблиця 3.4 – Розподіл пінів Raspberry Pico W

Назва елементу	Призначення	Підключення до піну ESP32
NFC_BUTTON_PIN	Кнопка імітації авторизації через NFC	GP10
FINGER_BUTTON_PIN	Кнопка імітації авторизації через відбиток пальця	GP11
PIR_SENSOR_PIN	Датчик руху (PIR)	GP4

Продовження таблиці 3.4

Назва елементу	Призначення	Підключення до піну ESP32
POT_PIN	Потенціометр для тестування регульованих параметрів	A0
LED_GRANTED_PIN	Зелений світлодіод – доступ надано	GP5
LED_DENIED_PIN	Червоний світлодіод – доступ відхилено	GP6
ALARM_LED_PIN	Світлодіод для індикації руху	GP7
SERVO_PIN	Серводвигун для моделювання замка дверей	GP8

Під час запуску програмного забезпечення мікроконтролера Raspberry Pi Pico W виконується підключення до локальної Wi-Fi мережі (рис. 3.29), параметри якої (ім’я мережі та пароль) задаються в коді.

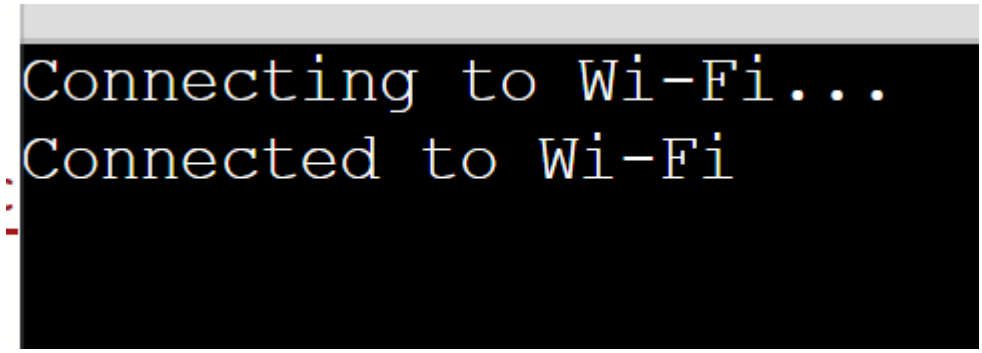

Рисунок 3.29 – Підключення до Wi-Fi

На цьому етапі система повідомляє про початок процесу підключення шляхом виведення повідомлення про спробу з'єднання. Після встановлення з’єднання програма підтверджує успіх повідомленням про підключення. Це свідчить про те, що пристрій отримав доступ до мережі Інтернет, що дозволяє йому взаємодіяти з хмарними сервісами, такими як Telegram. Встановлений зв'язок забезпечує можливість надсилати сповіщення про події, отримувати

команди або передавати дані для віддаленого моніторингу та керування. Підключення до Wi-Fi є критично важливим для забезпечення роботи системи в рамках концепції Інтернету речей.

Після підключення мікроконтролера до Wi-Fi система переходить до очікування взаємодії з користувачем. На цьому етапі виводиться повідомлення "Waiting for Finger..." (рис. 3.30), що імітує підготовку до сканування відбитка пальця або введення іншого засобу ідентифікації. Одночасно це повідомлення дублюється у Telegram-бот, завдяки чому адміністратор бачить (рис. 3.31), що система активна і чекає дію користувача.

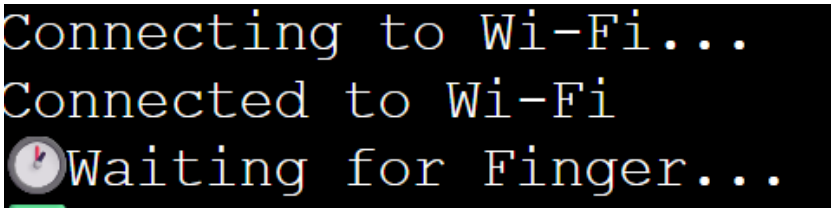

Рисунок 3.30 – Очікування відбитка

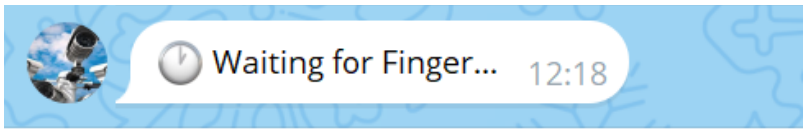

Рисунок 3.31 – Сповіщення Телеграм

Коли користувач натискає на кнопку, що відповідає за успішну ідентифікацію, система спрацьовує – активує зелений світлодіод і приводить у дію сервопривід, імітуючи відкриття замка. У цей момент надсилається повідомлення у Telegram з текстом "☑ Доступ наданий", яке дублюється на екран серіального монітору (рис. 3.32). Таким чином, адміністратор у режимі реального часу отримує підтвердження про успішне надання доступу.

На схемі видно, що зелений світлодіод активовано (рис. 3.33), а сервопривід знаходиться у відкритому положенні, що вказує на успішне завершення перевірки доступу. Уся взаємодія супроводжується відображенням відповідної інформації як на екрані, так і у Telegram, що підтверджує коректну роботу віддаленого моніторингу і керування системою доступу.

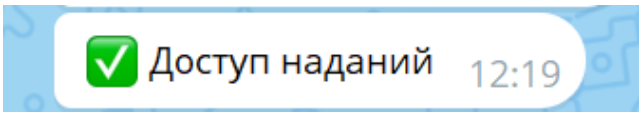

Рисунок 3.32 – Сповіщення про надання доступу

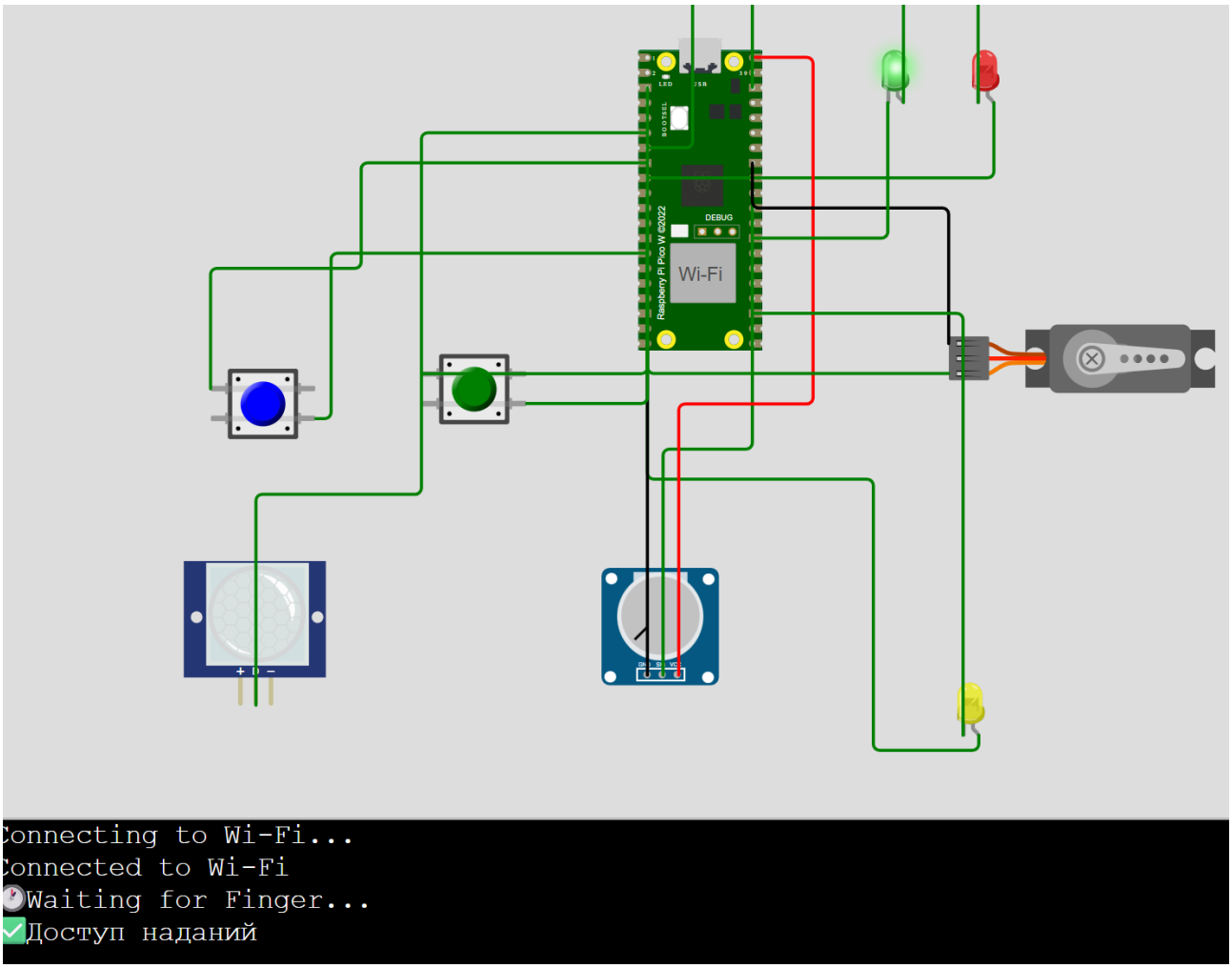

Рисунок 3.33 – Спрацювання зеленого світлодіода

Сервопривід у цей момент повернув свій важіль у положення відкриття, імітуючи фізичне відкривання замка (рис. 3.34). Це означає, що доступ користувачу було надано, і система дозволила пройти в охоронювану зону. Активне положення сервоприводу є підтвердженням успішного спрацювання всієї системи.

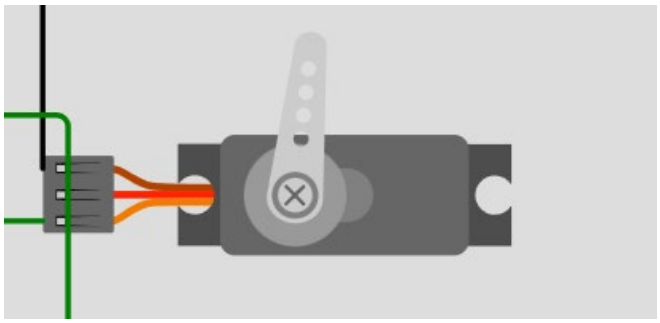

Рисунок 3.34 – Відкриття сервопривіда

Після підключення до Wi-Fi система переходить у режим очікування взаємодії з користувачем. У цей момент користувач здійснює спробу отримати доступ, натискаючи кнопку, що імітує невірну ідентифікацію або спробу сторонньої особи. Програма визначає спробу як неуспішну, і система сигналізує про відмову.На макеті активується червоний світлодіод, що вказує на відмову в доступі. Сервопривід при цьому залишається у закритому положенні, що означає, що вхід до зони залишився заблокованим. На екрані з’являється повідомлення "Доступ відхилено" (рис. 3.35), яке також надсилається адміністратору в Telegram з червоним хрестиком, що підкреслює невдалу спробу входу.

Таким чином, система чітко відпрацьовує ситуацію неправильної ідентифікації: блокування доступу, світлова індикація про відмову та миттєве інформування відповідальної особи через Telegram (рис. 3.36). Це дозволяє своєчасно реагувати на потенційно небажані або несанкціоновані спроби доступу.

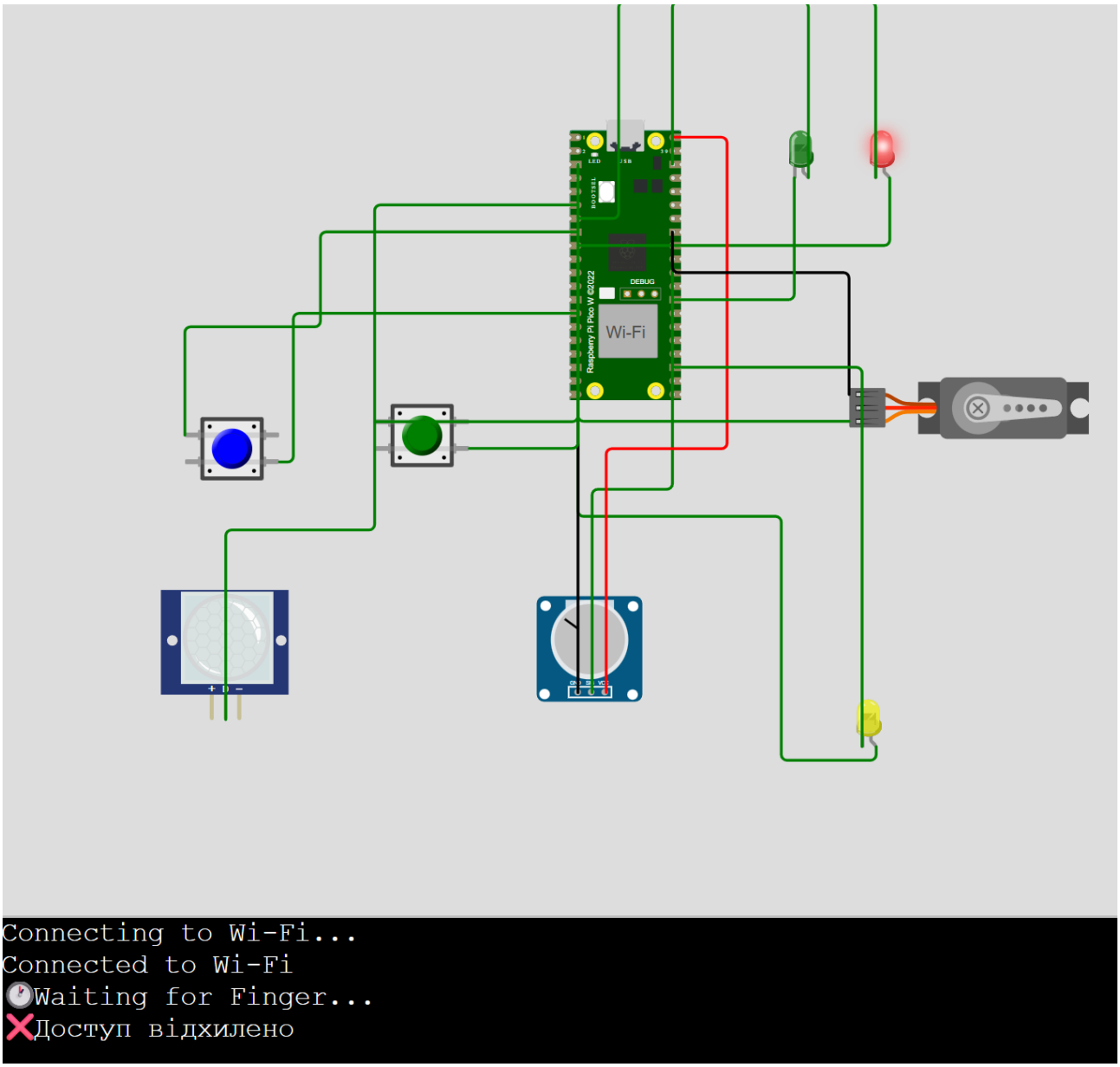

Рисунок 3.35 – Доступ відхилено

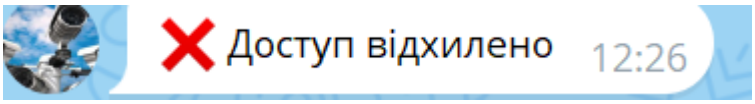

Рисунок 3.36 – Доступ відхилено, сповіщення телеграм

Після успішної авторизації користувача система продовжує моніторинг простору за допомогою датчика руху PIR. При появі об’єкта у зоні дії датчика система миттєво реагує, вмикаючи жовтий світлодіод, що сигналізує про виявлення руху. У той самий момент у Telegram надсилається повідомлення з

текстом "🚨 Рух зафіксовано!" (рис. 3.37), що інформує адміністратора про присутність або рух у контрольованій зоні.

Це дозволяє контролювати не лише спроби ідентифікації, а й подальші події у зоні доступу (рис. 3.38). Таким чином, навіть якщо доступ був попередньо наданий, система продовжує стежити за ситуацією і оперативно сповіщає відповідальну особу про будь-яку активність. Це підвищує рівень безпеки, оскільки адміністратор отримує повну картину подій у режимі реального часу.

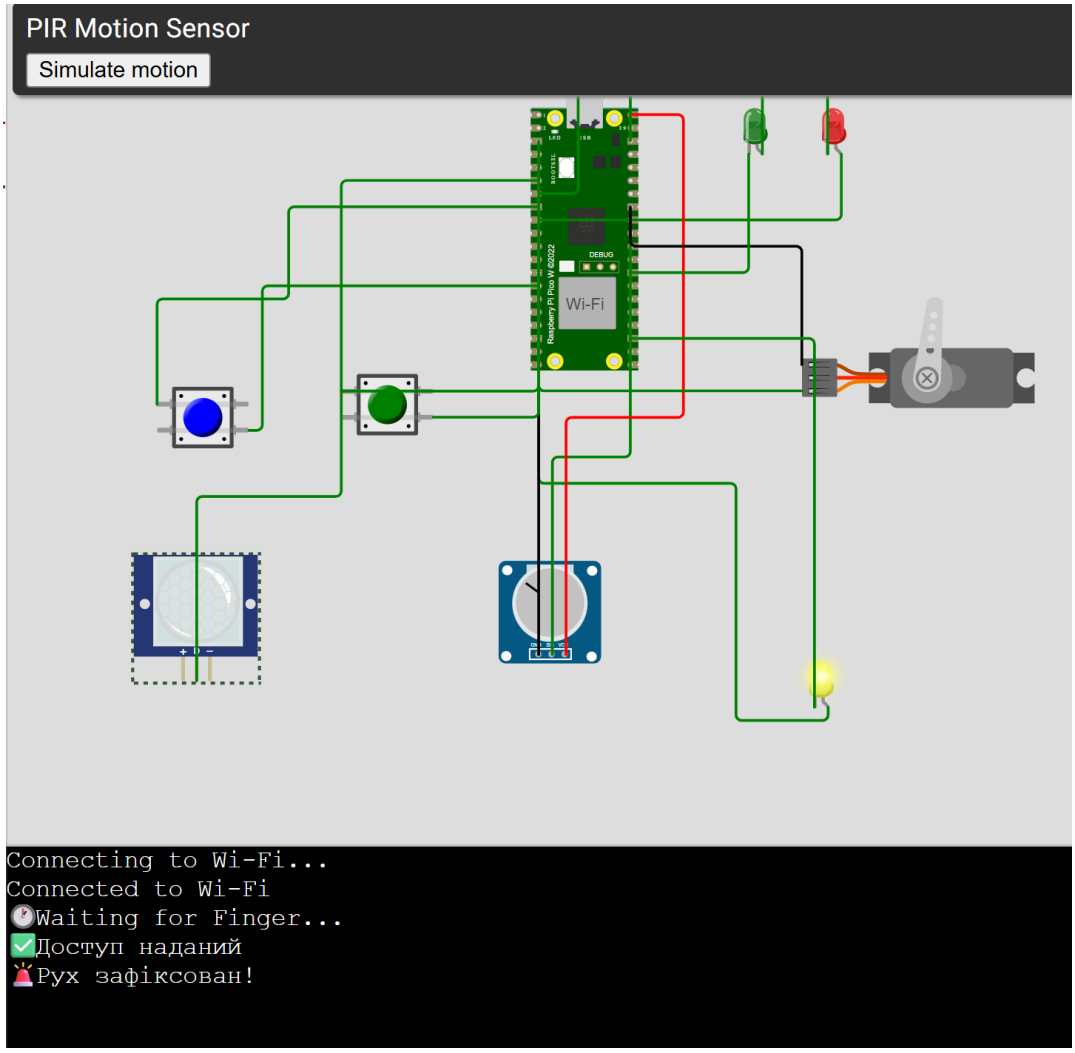

Рисунок 3.37 – Фіксація руху

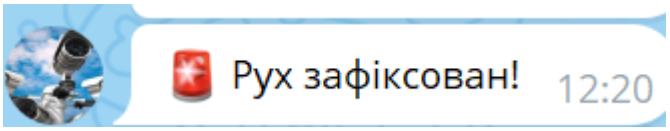

Рисунок 3.38 – Фіксація руху сповіщення

3.6 Розробка застосунку тривог

Окрім програмної частини для мікроконтролера, в рамках роботи також було створено веб-додаток, який взаємодіє з відкритим API сервісу тривог України (https://alerts.in.ua). Даний веб-додаток реалізовано на базі мікрофреймворку Flask, що дозволяє розгорнути простий сервер для обробки запитів і відображення інформації у зручному для користувачів форматі через браузер (рис. 3.39).

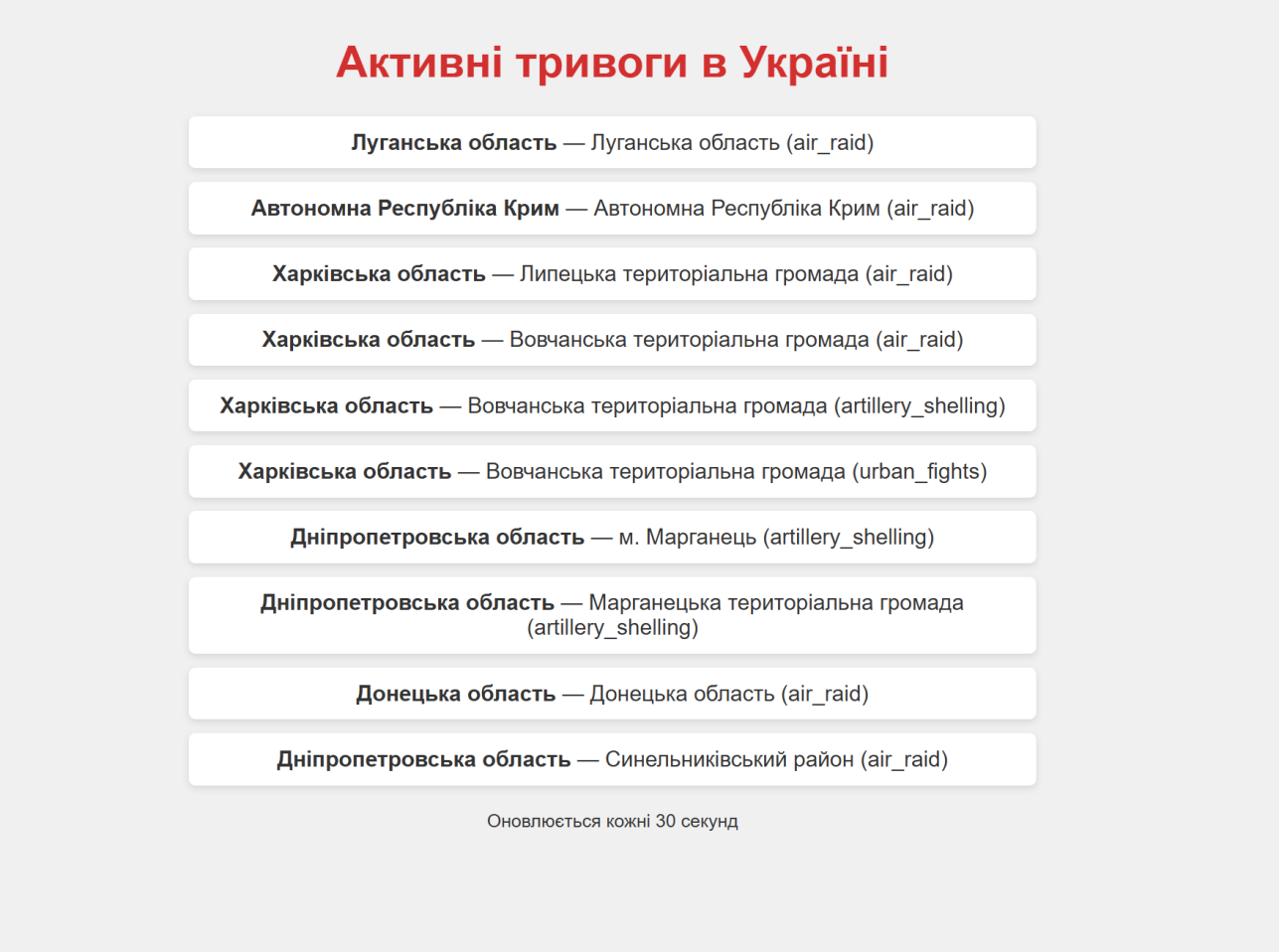

Рисунок 3.39 – Веб-інтерфейс додатку

Основною функцією веб-додатку є отримання актуальних даних про активні тривоги на території України за допомогою HTTP-запитів до офіційного API. Додаток обробляє отримані дані та виводить їх у вигляді списку, що містить область, громаду та тип тривоги. Наприклад, у списку можуть бути вказані

повітряні тривоги, артилерійські обстріли або бойові дії. Кожна тривога відображається окремим блоком з чіткою структурою для зручності сприйняття.

Важливою особливістю веб-додатку є автоматичне оновлення даних кожні 30 секунд, що дозволяє користувачам бачити поточну ситуацію без необхідності перезавантажувати сторінку вручну. Це досягається завдяки простому вбудованому JavaScript-скрипту, який виконує автоматичне оновлення сторінки.

Крім цього, веб-додаток надає два режими доступу:

– веб-інтерфейс для людей, де інформація подається у вигляді зрозумілого списку з візуальним оформленням;

– JSON API для пристроїв, доступний за спеціальним шляхом /api, що дозволяє отримувати ті самі дані у форматі JSON. Це може бути корисно для підключення до різних автоматизованих систем або IoT-пристроїв, зокрема для використання у проекті на Raspberry Pi Pico W.

Таким чином, створений веб-додаток виступає додатковим інструментом моніторингу та інтеграції даних про безпекову ситуацію в Україні, що розширює функціональні можливості системи та дозволяє реагувати на події в режимі реального часу як через браузер, так і через автоматизовані пристрої.

3.7 Охорона праці

У сучасному світі, де більшість людей проводять значну частину свого часу в офісних та виробничих приміщеннях, створення комфортних та безпечних умов праці є одним із головних пріоритетів. Одним із важливих аспектів, що впливає на комфорт та продуктивність працівників, є належний рівень освітленості в робочих приміщеннях.

Освітленість має прямий вплив на сприйняття інформації, зорову активність, концентрацію та настрій працівників. Недостатня або некоректна освітленість може призводити до зриву робочого процесу, погіршення зору, збільшення втому та навіть до виникнення професійних захворювань.

Одним з важливих аспектів проектування освітлення є розрахунок оптимального рівня освітленості для конкретного приміщення. У даному розділі

розглянуто розрахунок освітленості для об’єкту розміром 50 м х 20 м, в якій буде функціонувати макет для моніторингу охоронної та пожежної безпеки. За допомогою відповідних формул та рекомендованих стандартів, визначається необхідний рівень освітленості, щоб забезпечити комфортні та безпечні умови роботи.

Виміряння та врахування правильного рівня освітленості в приміщеннях є важливою складовою процесу планування та розробки робочих місць. Правильне освітлення не тільки сприяє підвищенню продуктивності працівників, але й має позитивний вплив на їхнє фізичне та психологічне самопочуття. Врахування рекомендованих норм та стандартів з освітленості в проектуванні приміщень є важливим етапом для створення безпечного та комфортного робочого середовища

У цьому розділі будуть наведені необхідні формули та рекомендації для розрахунку освітленості в кімнаті розміром 50 м х 20 м. Використовуючи ці дані, буде змога визначити оптимальний рівень освітленості для макету, що забезпечити комфорт та безпеку працівників під час виробничих процесів.

Для розрахунку освітленості в кімнаті розміром 50 м х 20 м потрібно враховувати рекомендований рівень освітленості для даного типу діяльності. Зазвичай для офісних та виробничих приміщень рекомендована освітленість знаходиться в діапазоні від 300 люкс до 750 люкс.

Для розрахунку загальної освітленості можна використовувати наступну формулу:

$$E = A \cdot E_r,$$

де E – загальна освітленість, люкс;

A – площа кімнати, $м^2$;

E_r – рекомендована освітленість, люкс.

Для прикладу, якщо взято рекомендовану освітленість 600 люкс, то розрахунок буде наступним:

$$E = 1000 \cdot 600 = 600000 \text{ люкс.}$$

Відповідно, для приміщення розміром 50 м х 20 м з рекомендованою освітленістю 600 люкс буде необхідно забезпечити загальну освітленість в 600000 люкс.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи здійснено комплексний аналіз сучасних IoT-технологій у контексті автоматизації контролю доступу. Проведений аналіз показав, що використання таких технологій, як RFID, NFC, біометричні системи, штучний інтелект, відеоаналітика, хмарні платформи та LoRaWAN, дозволяє створювати високоефективні інтегровані рішення. Виявлено, що сучасні IoT-системи від провідних виробників (Honeywell, Bosch, Hikvision, Axis) характеризуються високою ефективністю, але мають певні недоліки, зокрема високу вартість та складність інтеграції.

Другий розділ присвячено проектуванню архітектури та алгоритмів роботи системи автоматизованого контролю доступу. Реалізовано модульну структуру системи, що включає двофакторну автентифікацію за допомогою NFC-карток та біометричних сканерів, систему відеомоніторингу, периметрального захисту з використанням LoRaWAN-сенсорів та анти-дронову підсистему. Розроблено алгоритми функціонування системи у звичайних, аварійних та загрозливих ситуаціях, що забезпечують оперативну реакцію на події та безперебійність роботи.

Третій розділ присвячений практичній реалізації проєкту. Проведено порівняльний аналіз апаратних платформ (Arduino Uno, ESP32, Raspberry Pi Pico W). Створено детальну цифрову модель системи у середовищі Wokwi, реалізовано інтеграцію з Telegram-ботом для сповіщень і API системою повітряних тривог. Виконані тести підтвердили коректність роботи всіх елементів, включаючи підсистему резервного живлення.

Унікальність розробленої системи полягає в її комплексному характері: інтеграції IoT, мобільного зв’язку, біометричної ідентифікації, хмарного контролю та автономного енергоживлення. Завдяки цьому система забезпечує реальний контроль доступу, автоматичну реєстрацію подій, оперативне сповіщення користувачів та збереження працездатності навіть у критичних ситуаціях.

Запропонована система автоматизації контролю доступу може бути легко масштабована та адаптована до різних умов експлуатації, включаючи промислові об'єкти, приватні володіння та критичну інфраструктуру. Отримані в роботі результати мають потенціал для комерціалізації та можуть служити базою для розвитку нових та вдосконалення існуючих систем безпеки на основі технологій Інтернету речей.

ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ 3008-15. Документація. Звіти у сфері науки та техніки. структура та правила оформлення. Введ. 2015-06-22. К. Держстандарт України, 2017. – 29 с.

2. Методичні вказівки з підготовки кваліфікаційної роботи бакалавра для студентів усіх форм навчання спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології» / Упоряд.: І.Ш. Невлюдов, А.О. Андрусевич, О.В. Токарєва, С.П. Новоселов, О.В Сичова. Харків: ХНУРЕ, 2022. – 55 с.

3. Marunich, R., Sotnik, S. Approaches to ensuring the effective implementation of iot technologies in various industries // International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024». – 2024. – pp. 22-23

4. Маруніч Р.В. Особливості застосування IoT у сфері безпеки / Р.В. Маруніч // Автоматизація та приладобудування («Automation and Development of Electronic Devices» ADED-2024 Part 2) [Електронний ресурс]: збірник студентських наукових статей / Харківський національний університет радіоелектроніки; [редкол.: І.Ш. Невлюдов та ін.]. –Харків : ХНУРЕ. – 2024. – Вип. 2. – Р. 71-76

5. Marunich, R.V. Features of IoT application in the security sector / R.V. Marunich, S. V. Sotnik // «Computer-integrated technologies, automation and robotics» CITAR-2025. – 2025. – pp. 80-84

6. Nevliudov, I. Software development for small details production warehouse automated system / I. Nevliudov, et al. // Proceedings of the 2 nd International Scientific and Practical Conference, 2023. - pp. 321-323

7. Polikanov, K. Smart home with house module: overview of automation technologies / K. Polikanov, S. Sotnik // International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024», 2024 - pp. 20-21

8. Невлюдов І. Ш. Виробничі процеси та обладнання об'єктів автоматизації: Підручник для студентів вищих навчальних закладів / І. Ш. Невлюдов та інш. Кривий Ріг: Криворізький коледж НАУ. – 2017. – 444 с.

9. Невлюдов І. Ш. Комп’ютерно-інтегровані технології виробництва технічних засобів автоматизації. – 2021. – 604 с.

10. Невлюдов І.Ш. Механізми технічних засобів автоматизації (довідкові матеріали з курсового і дипломного проектування): навчальний посібник. / І.Ш. Невлюдов, В.І. Роменський, І.О. Яшков. – Харків: ХНУРЕ, 2021. – 292 с.

11. Невлюдов І. Ш. Технічні засоби автоматизації: Підручник / І.Ш. Невлюдов, А.О. Андрусевич, О.І. Филипенко, Н.П. Демська, С.П. Новоселов. – Кривий Ріг : Криворізький коледж НАУ, 2019. – 366 с.

12. Khalimonov, Y. I., & et al. Integration of IoT into security systems: opportunities and risks // Комп’ютерно-інтегровані технології автоматизації технологічних процесів на транспорті та у виробництві: матеріали всеукр. наук.-практ. конф. здобувачів вищ. освіти і молодих учених, 20 листоп. 2024 р. – 2024. – pp. 117-121

13. Lykho, T. A. & et al. Pattern recognition and computer vision technologies in decision support systems of robotic systems // Proceedings of the XVII International scientific and practical conference «Information technologies and automation – 2024». –2024. – pp. 645-648

14. Халімонов, Я. І., та інш. Створення інтелектуального модулю для автоматизованого моніторингу середовища у приватних та комерційних приміщеннях з використанням комп'ютерно-інтегрованих технологій // International Conference on Advanced Trends in Radioelectronics and Telecommunications dedicated to the 85th anniversary of the Department of Theoretical Radio Engineering and Radio Measurements. – 2024. – 1. – pp. 176 -181

15. Khalimonov, Y., & et al. Approaches to ensuring proper working conditions using sensor technologies IoT // International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024». – 2024. – pp. 24-25

16. Sotnik, S. Integration of IoT into security systems: opportunities and risks // International Journal of Academic Engineering Research (IJAER). – 2024. – Vol. 8, Issue 11. – pp. 56-61