Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут комп’ютерних наук та штучного інтелекту
Кафедра комп'ютерних систем та робототехніки

«Затверджую»
Завідувач кафедри комп’ютерних
систем та робототехніки
к. ф.-м. н., доц. ХРУСЛОВ М. М.
« » _____ 2024року

Пояснювальна записка

до кваліфікаційної роботи
бакалавра

на тему: «**Модель комп’ютеризованої системи контролю доступу до офісного приміщення через Інтернет»**

Захищено на засіданні
Атестаційної комісії № 42
протокол № __ від __.11.2024 р.
Оцінка _____ / _____
Голова Атестаційної комісії
_____ **СКОБ Ю. О.**

Виконав:
студент 4 курсу, групи КІ–41
Галузь знань: 12 – Інформаційні технології
Спеціальність: 123 – Комп’ютерна інженерія.
ПАПУША Руслан Олександрович

Керівник: к.т.н., доцент кафедри комп’ютерних систем та робототехніки
ЛАБЕНКО Дмитро Петрович

Рецензент:
професор кафедри ОВ ППО СВ ХНУПС імені Івана Кожедуба кандидат технічних наук, доцент
НАКОНЕЧНИЙ Олександр Анатолійович

Харків – 2024

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра складається зі вступу, трьох розділів, висновків, списку використаних джерел і чотирьох додатків. Загальний обсяг роботи складає 65 сторінки, із яких 38 сторінки основної частини з 24 рисунками, 2 таблицями, 7 найменуваннями списку використаних джерел та чотирма додатками.

Метою кваліфікаційної роботи є розробка моделі комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет.

Об'єкт дослідження – процес контролю доступу до офісного приміщення.

Предмет дослідження – методи та засоби забезпечення безпечного доступу до офісних приміщень через Інтернет із використанням біометричних даних та дистанційного контролю.

Проблема, яка вирішується в кваліфікаційній роботі, полягає в тому, щоб забезпечити безпечний і зручний доступ до офісних приміщень з використанням біометричних даних. Система повинна бути надійною, легкою у використанні і економічною в реалізації, а також забезпечувати високий рівень безпеки.

Область застосування – системи безпеки та контролю доступу.

Ключові слова: СКУД, СКД, сканер відбитків, розумний офіс, Arduino.

ABSTRACT

The explanatory note to the bachelor's qualification work consists of an introduction, three chapters, conclusions, a list of sources used and four appendices. The total volume of the work is 65 pages, of which 38 pages are the main part with 24 figures, 2 tables, 7 names of the list of sources used and four appendices.

The purpose of the qualification work is to develop a model of a computerized system for controlling access to an office space via the Internet.

The object of the study is the process of controlling access to office premises.

The subject of the study is methods and means of ensuring secure access to office premises via the Internet using biometric data and remote control.

The problem to be solved in the qualification work is to ensure safe and convenient access to office premises using biometric data. The system must be reliable, easy to use and economical to implement, and also provide a high level of security.

Scope of application – security and access control systems.

Keywords: ACS, SKD, fingerprint scanner, smart office, Arduino.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ

СКУД/СКД – система контролю та управління доступом

ПЗ – програмне забезпечення

PIN – персональний ідентифікаційний номер

RFID – радіочастотна ідентифікація

ID – ідентифікатор

ІЧ-датчики – інфрачервоні датчики

OTP – одноразовий пароль

SSL/TLS – протоколи захисту даних

VPN – віртуальна приватна мережа

2FA – двофакторна аутентифікація

IoT – Інтернет речей

GPIO – універсальний вивід/ввід

PWM – широтно-імпульсна модуляція

SPI – послідовний периферійний інтерфейс

I2C – інтерфейс інтегрованих схем

I2S – інтерфейс для передавання звуку між чіпами

UART – універсальний асинхронний приймач-передавач

ADC – аналогово-цифровий перетворювач

BLE – Bluetooth з низьким енергоспоживанням

MCU – мікроконтролер

CAN – мережа контролерів

ВСТУП

У сучасному світі інформаційна безпека стає все більш важливою, особливо у контексті офісних приміщень, де необхідно контролювати доступ до різних зон. З розвитком технологій управління доступом через Інтернет стало можливим підвищити рівень безпеки та зручності використання таких систем.

Актуальність роботи. Системи контролю доступу мають велике значення в різних галузях, зокрема в офісах, де безпека даних і захист конфіденційної інформації є критично важливими. Нині існує широкий спектр технологій і платформ для створення таких систем, проте вибір оптимальної платформи, яка б поєднувала надійність, ефективність та простоту використання, є складною задачею. Однією з таких платформ є Arduino, яка завдяки своїм можливостям дозволяє створювати високоефективні та гнучкі системи контролю доступу.

Метою дослідження є розробка моделі комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет, використовуючи платформу Arduino. Це включає аналіз існуючих технологій, вибір оптимальної платформи та реалізацію системи, що задовольняє сучасні вимоги безпеки.

Об'єкт дослідження – це процеси, що відбуваються під час контролю доступу до офісних приміщень, а також технології та методи, що використовуються для забезпечення цього процесу.

Методи дослідження: аналіз сучасних технологій контролю доступу, порівняння різних платформ, практична реалізація моделі системи на основі Arduino, тестування та оцінка ефективності запропонованої системи.

Таким чином, робота спрямована на створення надійної та ефективної системи контролю доступу, що дозволить підвищити рівень безпеки офісних приміщень, знизити ризики несанкціонованого доступу та забезпечити зручність управління доступом для користувачів.

Предмет дослідження – це апаратні та програмні компоненти системи контролю доступу, що забеспечують безпечний доступ до офісних приміщень через Інтернет із використанням біометричних даних, перепустки, тощо.

Завдання дослідження

1. Виконати аналіз існуючих моделей систем контролю доступу до офісного приміщення через Інтернет.
2. Вивчити основні принципи роботи системи контролю доступу до офісного приміщення через Інтернет.
3. Вибір платформи для розробки моделі системи контролю доступу до офісного приміщення.
4. Розробити модель комп’ютеризованої системи контролю доступу до офісного приміщення через Інтернет.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ДО ОФІСНОГО ПРИМІЩЕННЯ ЧЕРЕЗ ІНТЕРНЕТ

1.1 Система контролю та управління доступом (СКУД)

Підвищення рівня безпеки – одна з основних задач автоматизації. Це стосується як промислових і комерційних об'єктів, так і житлових приміщень. Активний розвиток відбувається і в сфері СКУД: знаходяться нові рішення для комплексів, розширюється функціональність обладнання.

Що таке СКУД?

Це комплекс обладнання, головна функція якого – обмеження доступу на об'єкт, що охороняється. Елементи СКУД об'єднані в мережу, яка керується за допомогою спеціалізованого програмного забезпечення. [1]

Розвиток сфери управління доступом привів до збільшення можливостей СКУД. Комплекси встановлюються на промислових підприємствах, у бізнес-центрах та офісах компаній, готелях, гіпермаркетах.

Для чого потрібна СКУД?

Комплекс обладнання для управління доступом у поєднанні з програмним забезпеченням здатний вирішувати такі задачі:

• захист інформації, що становить державну або комерційну таємницю;

• збереження активів і матеріальних цінностей;

• контроль проникнення на територію, що охороняється осіб, мета яких – порушення нормальної роботи організації шляхом саботажу або промислового шпигунства;

• відстеження кількості людей, що одночасно перебувають у приміщенні;

• облік робочого часу персоналу та фіксація запізнень, передчасних відходів з роботи, прогулів, переробок, тощо;

• організація пропускного режиму, заборона доступу на територію, що охороняється сторонніх осіб;

• облік транспортних засобів, які в'їжджають на територію об'єкта і виїжджають з неї.

Різновиди СКУД

Комплекси пристроїв для управління доступом поділяються на три групи, які відрізняються за автономністю, комплектацією та принципом роботи.

Автономні СКУД – встановлюються в комерційних приміщеннях, виконують функцію дверних замків. Доступ дозволяється за наявності картки з кодом, внесеним у програму. Якщо шифр картки збігається з даними у ПЗ, двері відчиняються. Такі СКУД мають мінімальний набір функцій і не потребують підключення до комп'ютера. [2]

Мережеві комплекси – мають більшу функціональність, ніж автономні СКУД. Вони підключені до ПК, а управління здійснюється дистанційно. До їх можливостей належать налаштування доступу на об'єкт за часовим графіком, облік робочого часу співробітників, інтеграція з камерами відеоспостереження, охоронним обладнанням та пожежною сигналізацією.

Біометричні. Ці СКУД відрізняються індивідуальною спрямованістю і працюють з унікальними особливостями співробітників – відбитком пальця, малюнком райдужної оболонки ока. Біометричний принцип розпізнавання підвищує рівень безпеки, на 95% знижує ймовірність помилок, надаючи інформацію про кожного працівника. Такі СКУД, окрім виконання основних функцій, враховують також час перерв, відпусток та відряджень, ведуть журнал відвідувань.

Характеристики існуючих моделей СКУД

Автономні системи контролю доступу

- Характеристики: Автономні СКУД працюють без підключення до мережі Інтернет. Вони зазвичай встановлюються в малих офісах і виконують основні функції контролю доступу, такі як відкриття дверей за допомогою картки або коду.

- Недоліки: Відсутність можливості віддаленого контролю та моніторингу, обмежена функціональність, складність інтеграції з іншими системами безпеки.
- Можливі удосконалення: Додавання функції підключення до мережі для віддаленого управління та моніторингу, інтеграція з іншими системами безпеки.

Мережеві системи контролю доступу

- Характеристики: Мережеві СКУД підключені до локальної мережі або Інтернету, що дозволяє здійснювати віддалений контроль та управління. Вони можуть бути інтегровані з іншими системами безпеки, такими як відеоспостереження та пожежна сигналізація.
- Недоліки: Висока вартість впровадження та обслуговування, необхідність постійного інтернет-з'єднання, можливість кібератак.
- Можливі удосконалення: Підвищення захисту від кібератак шляхом використання передових методів шифрування та автентифікації, оптимізація витрат на впровадження та обслуговування.

Біометричні системи контролю доступу

- Характеристики: Використовують унікальні біометричні дані користувачів (відбитки пальців, сканування обличчя або райдужки ока) для контролю доступу. Інтегровані з Інтернетом для віддаленого управління.
- Недоліки: Висока вартість обладнання, можливість помилок розпізнавання, питання захисту та зберігання персональних даних.
- Можливі удосконалення: Підвищення точності розпізнавання за рахунок використання нових алгоритмів, забезпечення надійного захисту персональних даних.

Таблиця 1.1

Порівняльна характеристика існуючих моделей СКУД

Модель СКУД	Характеристики	Переваги	Недоліки
Автономні	Працюють без Інтернету, базові функції	Простота, низька вартість	Відсутність віддаленого контролю, обмежена функціональність
Мережеві	Підключення до мережі, інтеграція з іншими системами	Віддалений контроль, розширена функціональність	Висока вартість, потреба в інтернет-з'єднанні, ризик кібератак
Біометричні	Використання біометричних даних, високий рівень безпеки	Висока точність, складність підробки	Висока вартість, можливість помилок, питання захисту даних

Компоненти СКУД

Система включає в себе ряд складових, кожна з яких виконує свою задачу. Автоматизований комплекс контролю доступу складається з таких компонентів:

• датчики, які ідентифікують умови та події;

• виконавчі механізми;

• пристрій, що задає алгоритм, – контролер або персональний комп'ютер.

Окрім обов'язкових елементів, до СКУД входять додаткові, які розширюють функціональність комплексу. [3]

Ідентифікатори, зчитувальні пристрої

Ідентифікація користувача входить до переліку першочергових завдань комплексу контролю доступу та необхідна для надання людині прав або застосування обмежень. Для зчитування, розшифровки та передачі інформації в СКУД використовуються спеціальні датчики, які поділяються на два типи:

1. Зчитувачі електронних кодів.
2. Сканери біометрії.

Зчитувачі електронних кодів

Ці елементи СКУД потрібні для зчитування коду з носія інформації та передачі на апаратний ідентифікатор. Пристрої бувають наступних видів: оптичні, магнітні, контактні, безконтактні, зчитувачі віртуальної інформації або PIN-кодів.

Оптичні

Пристрої потрібні для обробки інформації, записаної на жорсткий носій – перепустку або ідентифікаційну картку.

Переваги оптичних зчитувачів СКУД:

• просте видавання кодів ідентифікації;

• висока ступінь захисту;

• складність підробки: оригінальну штрихову комбінацію важко відтворити без спеціального обладнання та вихідного програмного пакету.

Недоліком оптичних зчитувачів СКУД можна вважати відносно високу вартість пристроїв, здатних безпомилково розпізнавати символьні ID-шифри.

Магнітні

Ще 3 роки тому ідентифікація кодів, записаних на магнітні носії, була найбільш поширеним способом розпізнавання, що використовувався комплексами контролю та управління доступом.

Переваги магнітних зчитувачів СКУД:

• швидке виготовлення карток і просте нанесення на них закодованої інформації;

• гарна захищеність;

• низька вартість зчитувальних пристроїв.

Масове виробництво чистих магнітних карток, пристроїв запису та зчитування інформації призвело до того, що цей спосіб перестав відповідати сучасним вимогам безпеки. Сьогодні магнітні зчитувачі втратили колишню популярність у сфері контролю доступу та поступово витісняються більш передовими технологіями.

Контактні

В основі цієї технології лежить зчитування інформації, записаної в пам'ять транспондера (RFID-мітки). Для передачі її в контролер СКУД чип повинен бути під'єднаний до контактів датчика.

Плюси контактних пристроїв зчитування для СКУД:

- великий обсяг пам'яті чипа для запису інформації;
- висока надійність мікрочипів;
- зручність використання – мітки розміщують на різних носіях.

Мінус такого зчитувача – поступове зношування контактів, що обмежує експлуатаційний ресурс ID-карток.

Безконтактні

Зчитувачі цього типу працюють за тим же принципом, що і контактні. Різниця в тому, що для передачі записаної на носії інформації фізичне підключення пристрою до контактів не потрібне. Безконтактні зчитувачі дуже широко поширені в СКУД. Вони підходять для роботи з програмованими картами proximity.

Переваги безконтактних зчитувачів:

- відносно простий пристрій і доступність апаратів для розпізнавання сигналів транспондера;
- необмежений термін служби;
- розміщення міток на носіях різних видів.

У цієї технології є тільки один недолік. Поява обладнання, здатного працювати з RFID-мітками, у вільному продажу призвела до часткової компрометації: умільці роблять дублікатори носіїв за 5–7 хвилин. Але відмовлятися від застосування безконтактних пристроїв у СКУД розробники не планують, борючись із проблемою розширенням асортименту RFID-міток.

Зчитувачі віртуальної інформації

Включення таких пристроїв до складу комплексу СКУД робить розпізнавання багаторівневим, підвищуючи рівень безпеки. Рішення про допуск приймається на основі двох факторів: інформації, записаної на носій, і цифрового коду, який вводить користувач.

Мінус такого підходу – прив'язка до апарату користувача. Для захисту інформації від дистанційного перехоплення під час передачі потрібно вживати спеціальних заходів.

Зчитувачі PIN-кодів

Ці пристрої не потребують ідентифікаторів, оскільки приймають рішення про допуск на основі коду, який користувач вводить вручну за допомогою клавіш на апараті.

Традиційний спосіб захисту відрізняється надійністю. Апаратні засоби ідентифікації в разі крадіжки компрометуються, стаючи доступними стороннім людям. PIN-код же позбавлений такого недоліку.

Біометричні сканери

Інноваційні технології поступово витісняють апаратні ідентифікатори, забезпечуючи розпізнавання користувачів за біометричною інформацією:

- папілярний візерунок на пальці руки;
- малюнок кровоносних судин на зап'ясті або зовнішній стороні кисті;
- геометричні параметри форми обличчя;
- райдужка ока.

До складу біометричних сканерів входять програмні комплекси, які перетворюють мультимедійну інформацію, переводячи її в цифровий код. Через це вартість обладнання підвищується, але зате розпізнавання стає достовірним і захищеним, що виправдовує використання таких пристроїв.

Використання в СКУД алгоритмів розпізнавання за біометрією вимагає надійного захисту персональної інформації. У базі обладнання зберігаються виключно цифрові коди, за якими неможливо відновити параметри особистості. [4]

Датчики

Крім ідентифікаторів і зчитуючих пристроїв, до комплекту СКУД входять датчики для розмежування внутрішнього доступу, контролю переміщень по території об'єкта та вирішення інших задач:

- розташовані всередині приміщень кнопки для подачі команд на відкриття дверей;
- датчики відкривання – геркони, контактні перемикачі;
- ІЧ-датчики для виявлення присутності, руху;
- датчики освітленості, вологості, температури та інші перетворювачі, показання яких важливі для коректування кодів і більш достовірної ідентифікації.

Для контролю обстановки на об'єкті та розпізнавання користувачів операторами до складу СКУД включають камери внутрішнього спостереження, здатні вести фото- та відеозйомку.

Виконавчі механізми

Для вирішення завдань, що стоять перед системами контролю доступу, в їх складі повинні бути виконавчі механізми, які ще називають загороджуючими. До них відносяться:

- запірні пристрої з електроприводом – замки, защіпки;
- турнікети;
- двері з функцією автоматичного відкривання і закривання;
- ворота з керованими стулками, бар'єри, шлагбауми.

Виконавчі механізми СКУД призначені для блокування доступу або його надання при умові проходження користувачем ідентифікації.

Разом із загороджуючими пристроями СКУД або окремо від них підключають:

- приводи відеокамер;
- пристрої сигналізації та оповіщення;
- записувальну апаратуру.

Контролери та комплекси управління

Контролер або керуючий комплекс – це "мозок" СКУД, який виконує наступні завдання:

- прийом сигналів від датчиків і зчитуючих пристроїв;
- визначення спрацювання тригерів, перевірка умов;

- формування відповідей на події за допомогою алгоритмів або вибірки з інформаційної бази;
- відправка керуючих сигналів на виконавчі механізми.

Конструкція, розташування та працездатність контролерів систем управління доступом повинні відповідати наступним вимогам:

- Відсутність збоїв у роботі навіть при відключенні електрики та інших надзвичайних ситуаціях. Для цього СКУД обладнуються автономними джерелами живлення, контролери розміщуються всередині захищених корпусів і монтуються у приміщеннях, добре захищених від впливу зовнішніх факторів.
- Обмеження доступу. Користувачі, які не мають прав адміністратора, не можуть працювати з апаратурою і програмними пакетами та перебувати у приміщеннях, де розташоване обладнання.
- Інформаційна безпека, включаючи захист від хакерських зломів та стійкість робочих алгоритмів.
- Надійність зберігання інформації. Накопичувачі цих систем зазвичай передбачають багаторазове резервування.

Як підвищити надійність?

Обладнання контролю доступу забезпечує надійність ідентифікації за двома напрямками:

- неможливість дискредитації носіїв та використання інформації сторонніми людьми;
- підвищення точності розпізнавання людини.

Дискредитацію носіїв запобігають наступними способами:

- створення складних і довгих кодів ідентифікації;
- підвищення надійності алгоритмів шифрування, зменшення ймовірності злому при передачі інформації;
- багаторівнева ідентифікація, що поєднує розпізнавання апаратної інформації з введенням PIN-коду;
- безпечні канали передачі, обмінні протоколи.

Які СКУД підходять для офісів?

Підбираючи систему контролю та управління доступом для офісних приміщень, потрібно враховувати масштаби організації. У великих компаніях обладнання допомагає підтримувати дисципліну і враховувати робочий час кожного працівника.

Оптимальне рішення для таких фірм і підприємств – впровадження біометричних систем, в яких кожен співробітник має свій індивідуальний код, що автоматично визначає ступінь його доступу і дозволяє безпомилково контролювати дотримання робочого графіка.

Автономні системи рекомендується застосовувати в бізнес-центрах, де можуть розташовуватися офіси різних організацій.

1.2 Основні принципи роботи системи контролю доступу до офісного приміщення через Інтернет

Системи контролю доступу до офісних приміщень, що працюють через Інтернет, стали важливим інструментом для підвищення безпеки та зручності управління доступом. Такі системи дозволяють адмініструвати доступ до приміщень віддалено, в режимі реального часу, та забезпечують високу гнучкість у налаштуванні політик доступу. Основні принципи роботи таких систем включають наступні аспекти:

1. Ідентифікація та аутентифікація користувачів

Одним із головних принципів роботи системи контролю доступу є ідентифікація та аутентифікація користувачів. Для цього використовуються різні методи, такі як:

- Електронні карти або брелоки: Користувачі проходять ідентифікацію за допомогою спеціальних карт або брелоків з вбудованими RFID-мітками.
- Біометричні дані: Використання відбитків пальців, сканування обличчя, райдужки ока або інших біометричних характеристик.

- Мобільні додатки: Аутентифікація через мобільні додатки, що підтримують генерацію одноразових паролів (OTP) або використання QR-кодів.
- Паролі та PIN-коди: Використання традиційних паролів або PIN-кодів для аутентифікації.

2. Віддалене управління та моніторинг

Інтернет-підключення дозволяє адміністраторам системи віддалено керувати доступом до офісних приміщень. Це включає:

- Реєстрація та видалення користувачів: Адміністратор може додавати нових користувачів або видаляти доступ неавторизованим особам.
- Налаштування політик доступу: Встановлення правил доступу для різних зон офісу, включаючи обмеження за часом або днями тижня.
- Моніторинг у реальному часі: Спостереження за активністю користувачів та оперативне реагування на будь-які підозрілі дії.
- Журнал подій: Ведення детального журналу всіх подій доступу для подальшого аналізу та звітності.

3. Захищені канали зв'язку

Для забезпечення безпеки даних під час передачі через Інтернет використовуються захищені канали зв'язку, такі як:

- Шифрування даних: Використання протоколів SSL/TLS для шифрування даних між клієнтом та сервером.
- VPN: Використання віртуальних приватних мереж для забезпечення безпечного підключення до системи управління доступом.
- Двофакторна аутентифікація: Введення додаткового рівня захисту шляхом використання двофакторної аутентифікації (2FA).

4. Інтеграція з іншими системами безпеки

Системи контролю доступу можуть бути інтегровані з іншими системами безпеки для підвищення загального рівня безпеки офісного приміщення:

- Відеоспостереження: Синхронізація з системами відеоспостереження для відстеження входів та виходів у реальному часі.
- Сигналізація: Інтеграція з охоронною сигналізацією для автоматичного реагування на порушення доступу.
- Системи пожежної безпеки: Підключення до систем пожежної безпеки для автоматичного розблокування дверей у разі евакуації.

5. Гнучкість та масштабованість

Сучасні системи контролю доступу через Інтернет дозволяють легко масштабувати рішення відповідно до зростання потреб організації. Це включає:

- Додавання нових точок доступу: Легке додавання нових дверей, турнікетів або воріт до існуючої системи.
- Підтримка великої кількості користувачів: Можливість обробляти велику кількість користувачів та різних рівнів доступу без зниження продуктивності системи.
- Мобільність: Доступ до системи управління доступом з будь-якого пристрою з підключенням до Інтернету, що забезпечує гнучкість в управлінні.

1.3 Вибір платформи для розробки моделі системи контролю доступу до офісного приміщення

Вибір платформи для розробки моделі комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет є важливим етапом, що визначає ефективність, надійність і масштабованість кінцевого рішення. Далі розглянемо основні платформи, які можуть бути використані для реалізації даної системи, з акцентом на їхні переваги та недоліки, а також обґрунтуємо вибір платформи Arduino для цієї задачі.

1.3.1 Raspberry Pi - одноплатний комп'ютер[5].

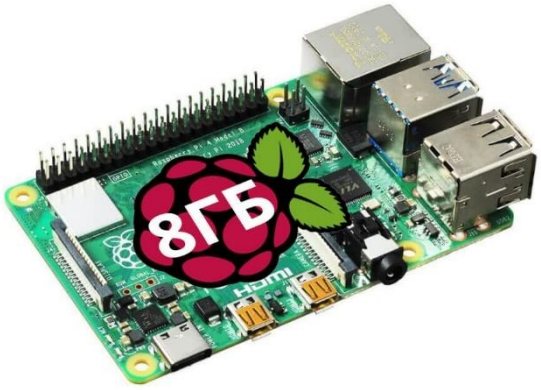


Рисунок 1.1 – Raspberry Pi

Raspberry Pi (рис. 1.1) є одним із найпопулярніших виборів для проектів, пов'язаних з Інтернетом речей (IoT). Цей мінікомп'ютер пропонує високу обчислювальну потужність, що робить його привабливим для різних застосувань, включаючи системи контролю доступу.

Переваги:

- Висока обчислювальна потужність: Raspberry Pi оснащений потужним процесором, що дозволяє виконувати складні завдання, такі як обробка відео і зображень. Це може бути корисним для систем, які потребують розпізнавання обличчя або інших форм біометричної аутентифікації.
- Підтримка ОС Linux: Платформа підтримує повноцінну операційну систему Linux, що забезпечує доступ до широкого спектра програмного забезпечення та бібліотек. Це дозволяє розробникам використовувати різні інструменти та фреймворки для створення надійних і гнучких рішень.
- Інтерфейси вводу/виводу: Raspberry Pi має велику кількість GPIO-пінів, що дозволяє підключати різні периферійні пристрої, такі як датчики, реле і зчитувачі. Це робить платформу дуже гнучкою і дозволяє легко адаптувати її до конкретних вимог проекту.

Недоліки:

- Вартість: Raspberry Pi, особливо в повній конфігурації з усіма необхідними модулями та аксесуарами, може бути дорожчим порівняно з іншими платформами. Це може стати важливим фактором, якщо бюджет проекту обмежений.
- Споживання енергії: Raspberry Pi споживає більше енергії порівняно з іншими мікроконтролерами, що може бути критичним у випадках, коли система повинна працювати автономно або за допомогою батарей.

1.3.2 ESP8266/ESP32 Контролери[6].

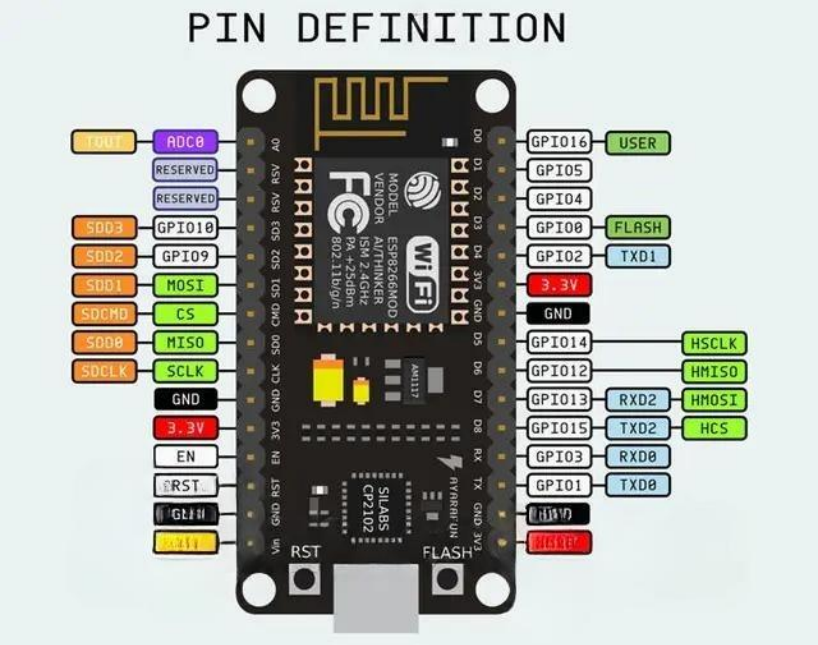


Рисунок 1.2 – ESP8266

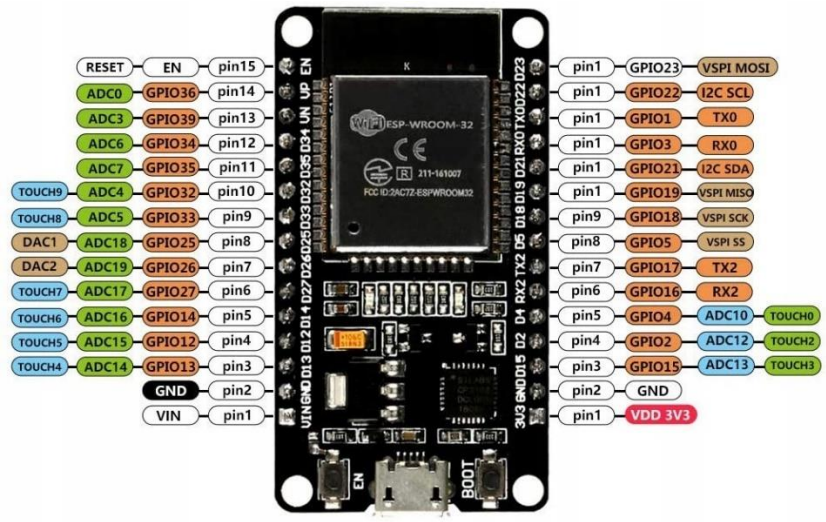


Рисунок 1.3 – ESP32

ESP8266 (рис. 1.2) та його більш потужний наступник ESP32 (рис. 1.3) є популярними виборами для IoT-проектів завдяки їхній низькій вартості та вбудованій підтримці Wi-Fi. Ці мікроконтролери ідеально підходять для реалізації бездротових рішень, таких як система контролю доступу через Інтернет.

Переваги:

- Вбудована підтримка Wi-Fi: ESP8266 та ESP32 мають вбудовані модулі Wi-Fi, що спрощує підключення до Інтернету та реалізацію віддаленого доступу. Це дозволяє легко інтегрувати систему з хмарними сервісами для моніторингу та управління в режимі реального часу.
- Низька вартість: Ці мікроконтролери мають значно нижчу вартість порівняно з іншими платформами, що робить їх доступними для широкого кола проектів. Це особливо важливо для розробників з обмеженим бюджетом.
- Енергоефективність: ESP8266 та ESP32 відзначаються високою енергоефективністю, що дозволяє використовувати їх у автономних системах з живленням від батарей. Це робить їх ідеальними для рішень, які повинні працювати тривалий час без зовнішнього живлення.

Недоліки:

- Обмежена обчислювальна потужність: Хоча ESP32 є більш потужним, обчислювальні можливості цих мікроконтролерів все ж обмежені у порівнянні з Raspberry Pi. Це може бути недостатнім для виконання дуже складних завдань, таких як обробка великих обсягів даних або виконання інтенсивних обчислень.
- Обмежена кількість GPIO: ESP8266 має меншу кількість GPIO-пінів порівняно з Raspberry Pi, що може обмежити можливості підключення периферійних пристроїв. ESP32 має більше пінів, але все ж може не задовольняти всі вимоги складних проектів.

Таблиця 1.2

Порівняльна характеристика контролерів ESP8266 та ESP32

Параметр	ESP8266	ESP32
MCU	Xtensa Single-core 32-bit L106	Xtensa Dual-Core 32-bit LX6 з 600 DMIPS
802.11 b/g/n Wi-Fi	HT20	HT40
Bluetooth	X	Bluetooth 4.2 та BLE
Типова частота	80 MHz	160 MHz
SRAM	X	✓
Flash	X	✓
GPIO	17	36
Апаратний / Програмний PWM	Немає / 8 каналів	Немає / 16 каналів
SPI/I2C/I2S/UART	2/1/2/2	4/2/2/2
ADC	10-біт	12-біт
CAN	X	✓
Ethernet MAC Interface	X	✓
Сенсор дотику	X	✓
Датчик температури	X	✓
Датчик Холла	X	✓
Робоча температура	-40°C до 125°C	-40°C до 125°C

1.3.3 Arduino - апаратна обчислювальна платформа[7].

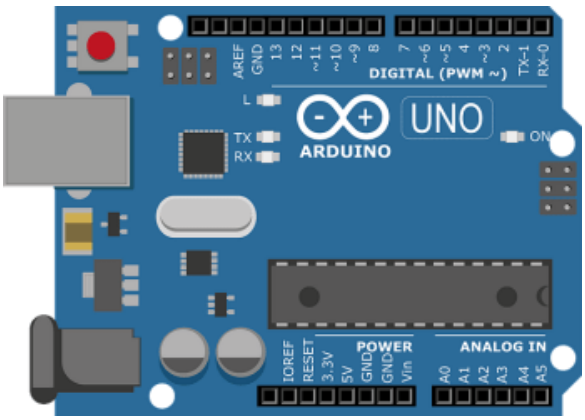


Рисунок 1.4 – Arduino

Arduino є однією з найпопулярніших платформ для розробки прототипів і освітніх проектів. Ця платформа відома своєю простотою використання, широким спектром доступних периферійних пристроїв та низькою вартістю, що робить її ідеальною для реалізації систем контролю доступу.

Переваги:

- Простота використання: Arduino відома своєю простотою використання, що робить її ідеальним вибором для швидкої розробки прототипів і освітніх проектів. Велика кількість прикладів і документації полегшує процес розробки навіть для початківців.
- Широка підтримка периферійних пристроїв: Існує велика кількість доступних шілд (модулів розширення) і сенсорів, що легко інтегруються з платформою Arduino. Це дозволяє швидко додати необхідні функції до системи контролю доступу.
- Низька вартість: Доступна ціна як на самі плати, так і на аксесуари та додаткові модулі робить Arduino привабливим вибором для проектів з обмеженим бюджетом.
- Енергоефективність: Низьке споживання енергії дозволяє використовувати Arduino в автономних рішеннях, що живляться від батарей.

Це є важливою перевагою для систем, які повинні працювати тривалий час без зовнішнього живлення.

Недоліки:

- Обмежена обчислювальна потужність: Arduino має меншу обчислювальну потужність порівняно з Raspberry Pi та ESP32, що обмежує його використання для дуже складних завдань. Проте, для більшості завдань контролю доступу ця потужність є достатньою.
- Відсутність вбудованої підтримки Wi-Fi: Більшість плат Arduino не мають вбудованого Wi-Fi модуля, що вимагає використання додаткових модулів для підключення до Інтернету. Це можна вирішити за допомогою модулів, таких як ESP8266, що забезпечує необхідну функціональність.

Порівняльний аналіз

При виборі платформи для розробки моделі системи контролю доступу до офісного приміщення через Інтернет необхідно врахувати такі аспекти, як обчислювальна потужність, вартість, енергоефективність, простота використання та можливості підключення до Інтернету.

- Raspberry Pi забезпечує високу обчислювальну потужність і гнучкість, але є дорожчим і менш енергоефективним.
- ESP8266/ESP32 пропонують вбудовану підтримку Wi-Fi та низьку вартість, але мають обмежену обчислювальну потужність і кількість GPIO-пінів.
- Arduino відзначається простотою використання, широкою підтримкою периферійних пристроїв, низькою вартістю та енергоефективністю. Хоча він має обмежену обчислювальну потужність і відсутність вбудованої підтримки Wi-Fi, ці недоліки можна подолати шляхом використання додаткових модулів, таких як Wi-Fi шілд або модуль ESP8266.

Вибір платформи

Враховуючи всі перелічені фактори, платформа Arduino є оптимальним вибором для розробки моделі системи контролю доступу до офісного приміщення через Інтернет. Простота використання, доступність, широкі

можливості розширення і висока енергоефективність роблять Arduino ідеальним варіантом для швидкої розробки прототипів та реалізації системи контролю доступу.

Висновки за розділом 1

На основі проведеного аналізу можна зробити висновок, що сучасні СКУД мають різні переваги та недоліки, що залежать від їх типу та технологій, які використовуються. Для удосконалення існуючих моделей СКУД рекомендується:

1. Інтеграція сучасних методів шифрування та автентифікації для підвищення захисту від кібератак.
2. Оптимізація витрат на впровадження та обслуговування за рахунок використання масштабованих рішень та хмарних сервісів.
3. Підвищення точності та надійності біометричних систем за рахунок впровадження новітніх алгоритмів розпізнавання та вдосконалення технологій зберігання даних.
4. Розробка гібридних систем, що поєднують переваги автономних, мережевих та біометричних моделей для забезпечення максимального рівня безпеки та зручності використання.

Вибір платформи для розробки моделі системи контролю доступу до офісного приміщення через Інтернет є важливим етапом, що визначає успіх кінцевого рішення. Розглянувши кілька популярних платформ, таких як Raspberry Pi, ESP8266 та Arduino, було встановлено, що платформа Arduino пропонує оптимальне поєднання простоти використання, широких можливостей розширення, низької вартості та енергоефективності.

Отже, вибір платформи Arduino для реалізації системи контролю доступу забезпечує необхідну функціональність, економічність і простоту впровадження, що робить її оптимальним рішенням для сучасних офісних приміщень.

РОЗДІЛ 2
РОЗРОБКА МОДЕЛІ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА БАЗІ ARDUINO З ВИКОРИСТАННЯМ ІНТЕРНЕТ МОДУЛЮ

2.1 Загальні принципи побудови системи контролю доступу

Сучасні системи контролю доступу до офісних приміщень покликані забезпечувати надійний захист від несанкціонованого доступу. Для цього використовуються передові технології, які дозволяють ідентифікувати осіб, обмежувати доступ до певних зон і вести облік відвідувань. Основна мета таких систем полягає у забезпеченні високого рівня безпеки, одночасно надаючи зручний і швидкий спосіб для авторизації користувачів. В нашій моделі ми поєднуємо біометричні та RFID-технології, що дозволяє комплексно підійти до питань безпеки та зробити систему більш гнучкою і масштабованою.

Біометрична ідентифікація: сканер відбитків пальців

Однією з найнадійніших технологій для ідентифікації є біометричний метод на основі відбитків пальців. Така технологія є практично невразливою до підробок, адже відбиток пальця містить унікальні фізіологічні риси, які неможливо відтворити або скопіювати. В системі використовується сканер відбитків пальців (наприклад, моделі FPM10A або ZFM60XSA), який здатний швидко і точно здійснити перевірку. Сканер оснащений датчиками для зчитування відбитка, після чого він перетворюється у цифрову модель, яка порівнюється з шаблонами, збереженими в базі даних.

Для кожного користувача відбиток пальця сканується кілька разів, щоб отримати точну ідентифікацію. Це відбувається шляхом аналізу характерних точок малюнка пальця, які згодом порівнюються із записаними шаблонами. У нашій системі алгоритм дозволяє визначити рівень безпеки шляхом встановлення мінімальної кількості точок, що необхідно для успішної ідентифікації. Вибір середньої кількості таких точок дозволяє забезпечити оптимальний баланс між точністю і швидкістю обробки даних.

RFID-зчитувач для безконтактної ідентифікації

Для підвищення гнучкості та зручності використання, система також включає RFID-зчитувач, наприклад, RC522, що дозволяє здійснювати безконтактну ідентифікацію користувачів. RFID-технологія забезпечує швидкий і зручний доступ за допомогою карток або брелоків, що містять унікальні чіпи. RC522 працює на частоті 13,56 МГц і підтримує стандарти ISO 14443A, що робить його універсальним для різних типів RFID-карток.

Перевагою RFID є можливість миттєвої перевірки даних без фізичного контакту з пристроєм. Система здатна розпізнати картку на відстані декількох сантиметрів, що зручно в умовах, коли потрібно забезпечити швидкий доступ великій кількості людей. Коли RFID-зчитувач зчитує дані з картки, він передає їх на контролер, де відбувається їх порівняння з записами бази даних.

Контролер Arduino як центральний елемент системи

Контролер Arduino відіграє центральну роль в системі, адже саме він здійснює управління та координацію всіх компонентів. Arduino обробляє сигнали від сканера відбитків та RFID-зчитувача, передає інформацію до модуля ESP8266 для подальшої відправки даних на сервер і керує іншими процесами. Використання Arduino дозволяє зробити систему гнучкою та легкою для розширення, оскільки Arduino має відкриту архітектуру і підтримує широкий спектр модулів та датчиків.

Інтернет-з’єднання через модуль ESP8266

Для забезпечення віддаленого доступу та можливості моніторингу, система оснащена Wi-Fi модулем ESP8266, який дозволяє підключати систему до мережі Інтернет. ESP8266 підтримує TCP/IP протоколи, що робить можливим передачу даних у режимі реального часу на віддалений сервер. Така структура дає можливість адміністраторам здійснювати моніторинг і керування системою з будь-якого місця, де є доступ до Інтернету, що значно підвищує зручність і ефективність контролю.

База даних та серверна частина

Останнім, але не менш важливим елементом системи є серверна частина з базою даних. База даних зберігає шаблони відбитків пальців, RFID-ідентифікатори та іншу інформацію, необхідну для роботи системи. Крім того, сервер фіксує всі події та відвідування, що дозволяє зберігати журнал подій для подальшого аналізу. Така структура не тільки забезпечує високу безпеку, але й надає інструменти для детального моніторингу та контролю доступу до приміщення.

Завдяки модульному підходу система легко адаптується до змін, що дозволяє додавати нові функції або замінювати старі компоненти без значних витрат.

2.2 Реалізація та інтеграція апаратних компонентів

На етапі розробки системи особлива увага була приділена вибору апаратних компонентів, що забезпечують високу надійність і швидкодію.

Біометричний сканер FPM10A (рис. 2.1): Цей сканер має вбудований процесор ARM Cortex M 32-bit (Synochip AS608), що дозволяє обробляти зображення відбитка пальця менш ніж за секунду. Спочатку сканер зчитує папілярний візерунок, який перетворюється у цифрову модель. Для цього зображення сканер виділяє ключові точки, які використовуються для порівняння з еталонними шаблонами. Визначення ідентифікаційної відповідності досягається шляхом пошуку збігів серед 12-24 точок, що забезпечує оптимальний баланс між швидкістю і точністю.

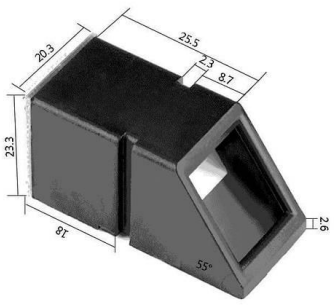


Рисунок 2.1 – Біометричний сканер FPM10A

RFID-зчитувач RC522 (рис. 2.2): Зчитувач дозволяє безконтактно зчитувати дані з RFID-карт, використовуючи частоту 13,56 МГц. Даний модуль працює з картами MIFARE, які є надійними та широко використовуються. Інтерфейс SPI забезпечує швидку передачу даних між зчитувачем та Arduino. Зчитувач використовує команду Request для пошуку карт у радіусі дії, а потім команду Select для зчитування унікального ідентифікатора карти (UID), що передається на Arduino для подальшої обробки.

Рисунок 2.2 – RFID-зчитувач RC522

Модуль ESP8266: Wi-Fi модуль забезпечує передачу даних на віддалений сервер, використовуючи протоколи TCP/IP. Модуль потребує низької напруги живлення (3,3 В), що дозволяє економити енергію. Крім того, ESP8266 підтримує режими сну, що забезпечує енергоефективність у тривалих системах моніторингу. Конфігурація ESP8266 здійснюється за допомогою AT-команд або програмування з використанням мови C++. Це дозволяє передавати дані відбитків пальців або RFID ідентифікаторів на сервер в реальному часі.

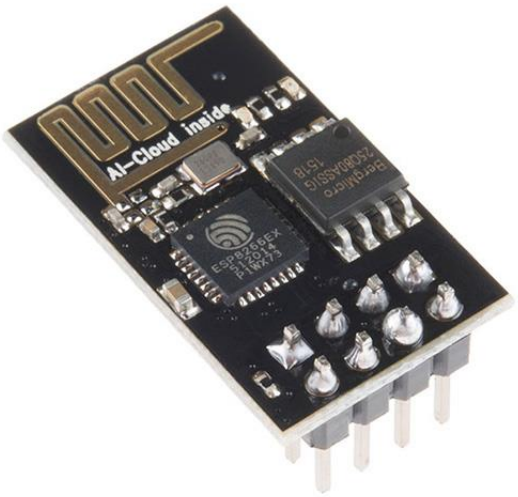


Рисунок 2.3 – Модуль ESP8266

2.3 Програмна архітектура та робота з базою даних

Програмне забезпечення для системи розроблено на основі платформи Arduino IDE, де реалізовані всі основні функції управління доступом. Використовуються бібліотеки Adafruit_Fingerprint, MFRC522 та ESP8266WiFi, що забезпечують взаємодію з апаратними компонентами та керуванням мережею. Основні етапи роботи моделі:

1. Зчитування даних: Arduino отримує відбиток пальця або RFID-картку, обробляє їх та визначає тип запиту (відбиток або RFID).

2. Передача даних: Після обробки дані передаються на сервер через модуль ESP8266. Програмний код налаштовано для передачі даних через HTTP-запити, що дозволяє гнучко керувати з'єднанням та обробляти відповіді сервера.

3. Порівняння даних та управління доступом: Сервер перевіряє отримані дані в базі даних. Якщо відбиток пальця або RFID-картка збігаються з записами в базі, сервер надсилає команду на Arduino для відкриття дверей. Якщо ж дані не відповідають жодному запису, доступ блокується.

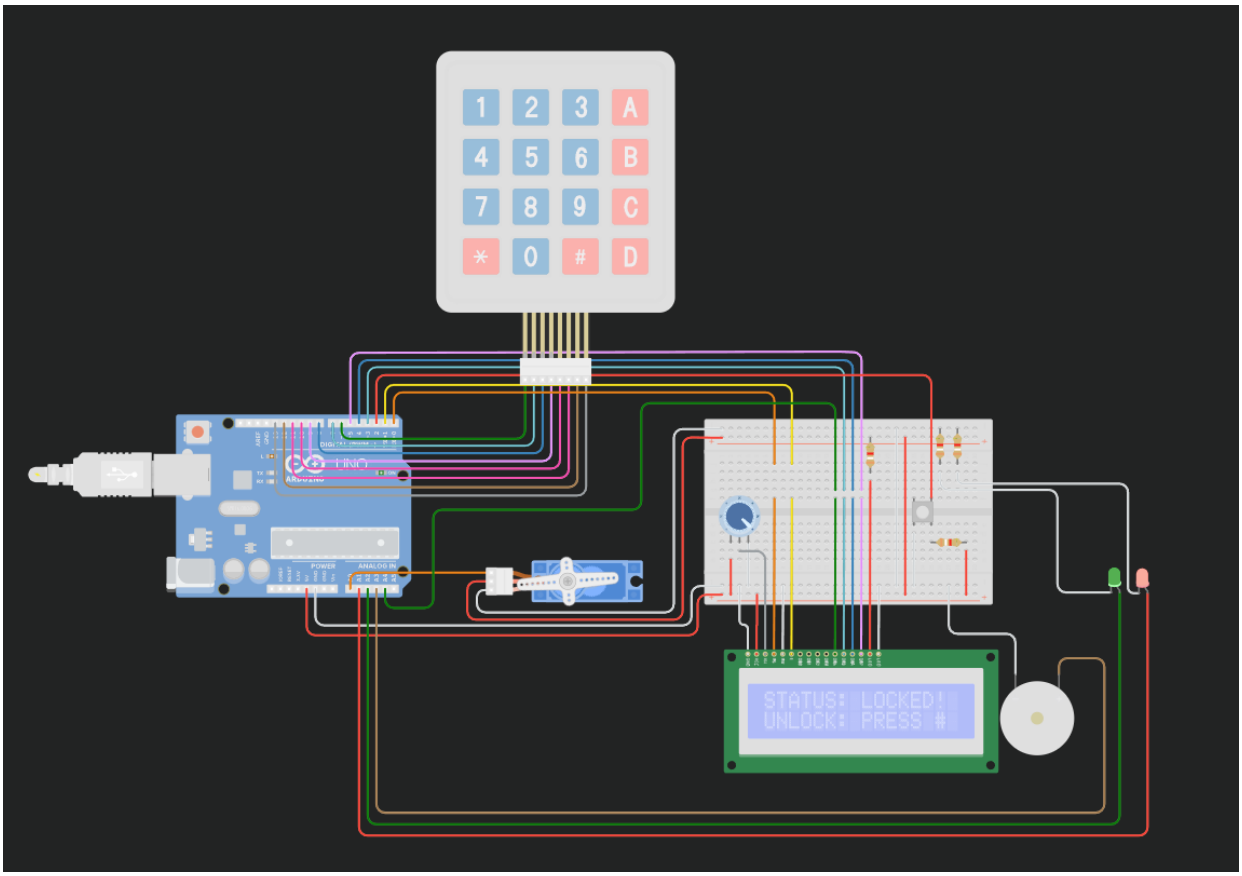


Рисунок 2.4 – Модель системи контролю доступу

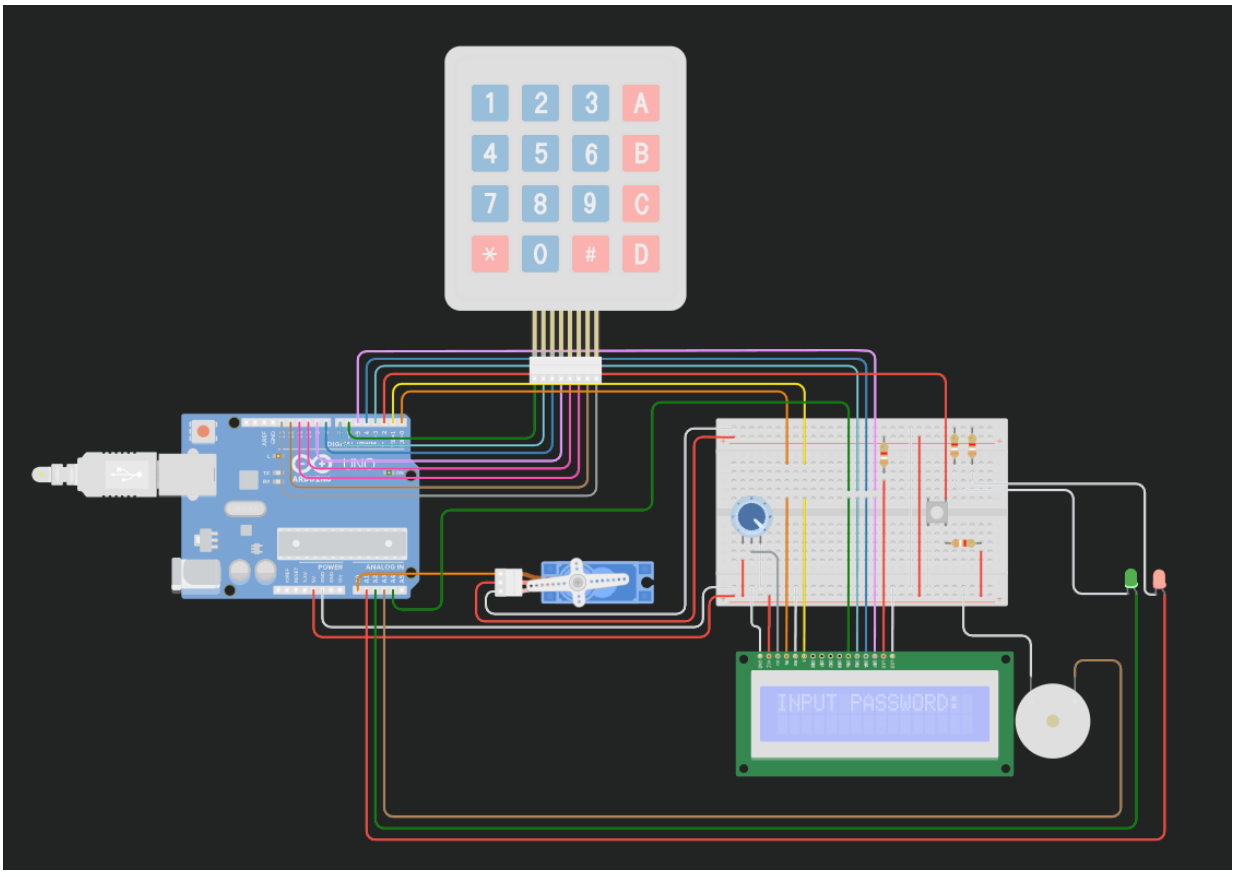


Рисунок 2.5 – Ввод коду доступу

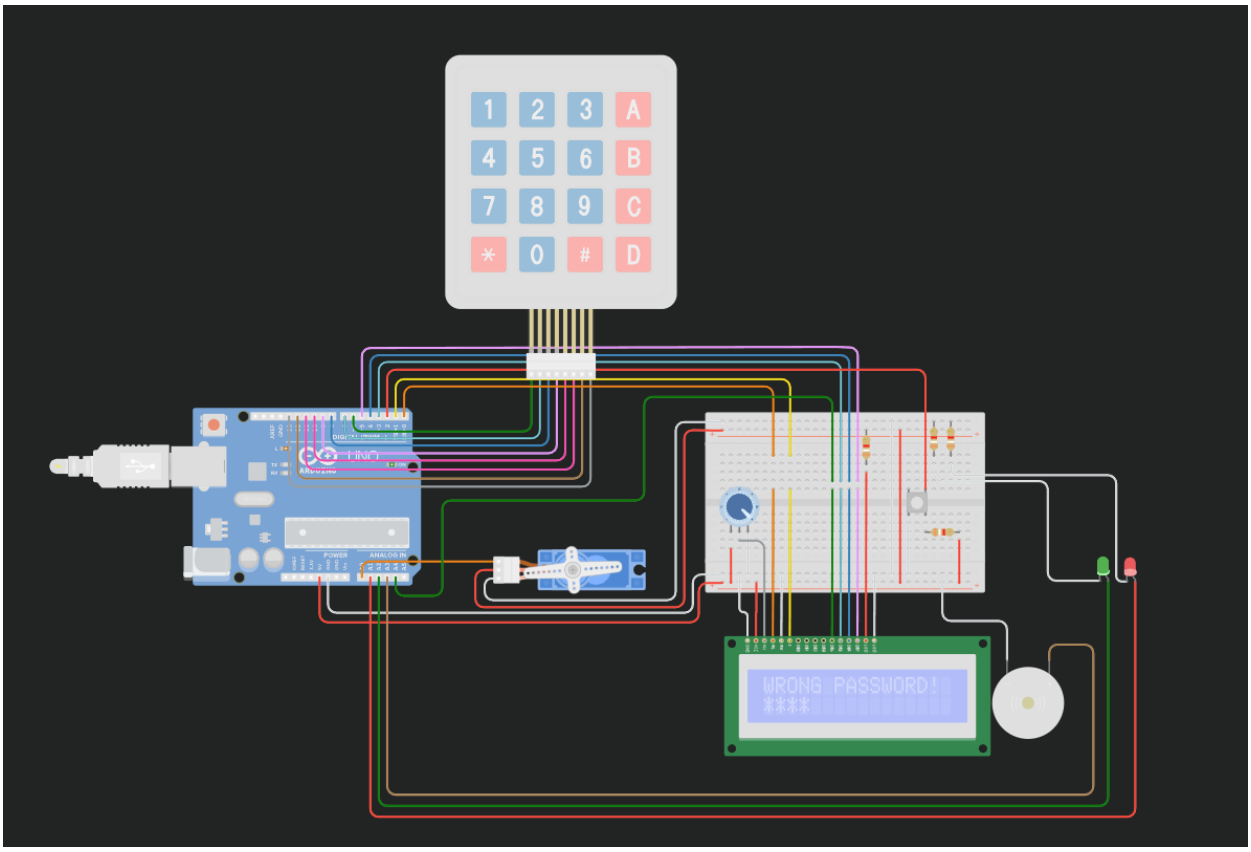


Рисунок 2.6 – Код доступу невірний, доступ заблоковано

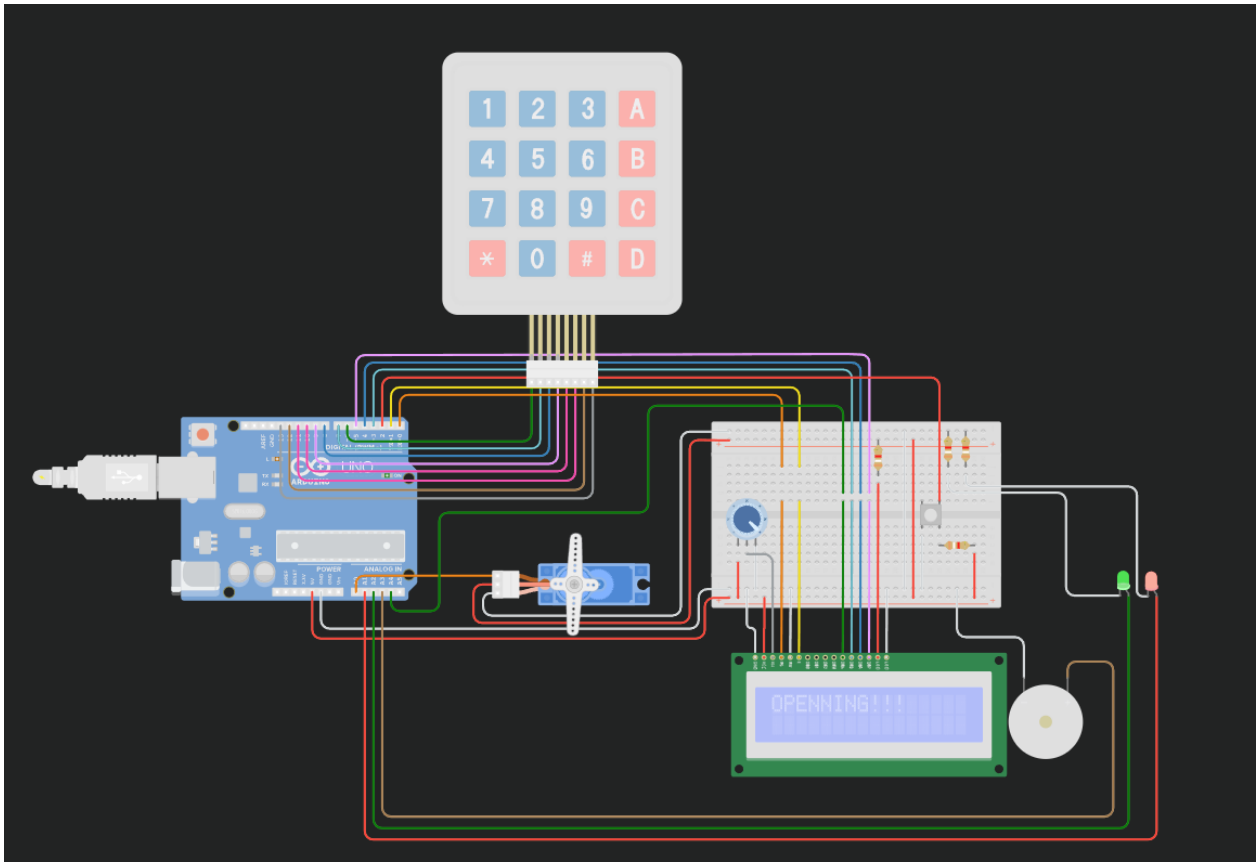


Рисунок 2.7 – Код доступу вірний, відчинення дверей

Висновки за розділом 2

Розроблена модель системи контролю доступу об'єднує сучасні технології ідентифікації, що дозволяє забезпечити надійний контроль доступу. Програмна та апаратна частини системи синхронізовані для швидкої та ефективної обробки запитів, тоді як використання інтернет-з'єднання розширює функціонал до віддаленого контролю. Дана модель здатна забезпечити високий рівень безпеки та є гнучкою у налаштуванні і масштабуванні, що робить її придатною для широкого використання в різних офісних приміщеннях.

РОЗДІЛ 3
ОПИС МОДЕЛІ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА БАЗІ ARDUINO З ВИКОРИСТАННЯМ ІНТЕРНЕТ МОДУЛЮ

3.1. Опис моделі системи контролю доступу

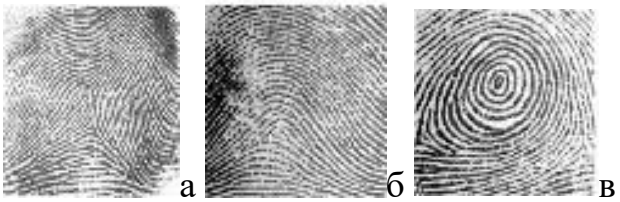
В даній моделі для ідентифікації суб’єкта пропонується використання біометричні даних, а також зчитувач RFID чипів. Найпоширенішою біометричною технологією автентифікації користувача є ідентифікація за відбитком пальця. Основою методу цієї ідентифікації є використання унікального малюнка папілярних візерунків на пальцях людей. Відбиток можна отримати застосовуючи сканер відбитків пальців. Сканер зчитує папілярний візерунок, перетворює його в цифрову модель і потім проводить порівняння з раніше введеним малюнком, який прийнято вважати еталонним.

Основні види папілярних візерунків (рис. 3.1):

– дуговий (рис. 3.1а);

– петльовий (рис. 3.1б);

– завитковий (рис. 3.1в).



а б в

Рисунок 3.1 – Основні види папілярних візерунків

В зв’язку з тим, що відбиток досить малий, необхідне застосування вузько направлених методів. Алгоритм розпізнавання відбитків пальців реалізується наступним чином: після отримання рисунка відбитка за допомогою сканера, він перетворюється в цифрову модель. З графічного зображення виділяються ключові характерні точки з яких формується цифрова модель відбитка. У сучасних системах береться від 12- 24 ключових точок.

При виборі більшої кількості ключових точок, сучасних обчислювальних ресурсів не вистачає для нормальної експлуатації системи в зв'язку з низькою швидкістю ідентифікації. При виборі меншої кількості точок, існує велика ймовірність допуску чужого відбитку пальця. Тому необхідно брати певне середнє значення для задоволення обох вимог.

Для реалізації функції зчитування біометричних даних використовується оптичний сканер відбитків FPM10A(ZFM60XSA) (рис. 3.2).

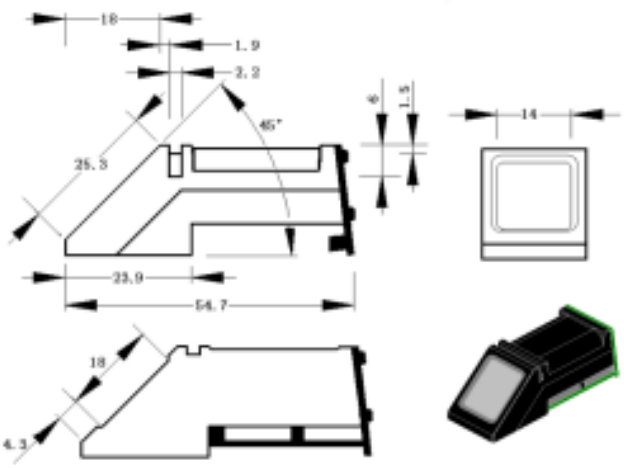


Рисунок 3.2 – Оптичний сканер відбитків FPM10A

Сканер відбитків побудовано на процесорі ARM Cortex M 32-bit - Synochip AS608, завдяки якому забезпечується підтримка алгоритмів шифрування даних, створюється база відбитків у внутрішній пам'яті та порівняння по шаблону. Сканер може керуватися, як комп'ютером так і самою платформою Arduino. Останній варіант дозволяє використовувати сканер в автономних пристроях. Живлення модулю складає 3,6-6 В, споживання струму 120 мА. Час, який необхідний для опрацювання відбитку, менше 1 секунди.

Взаємодія з модулем відбувається за допомогою пакетів, які мають в собі контрольну суму. Модуль складається з камери, кількох буферів та флеш пам’яті де зберігаються шаблони (рис. 3.3).

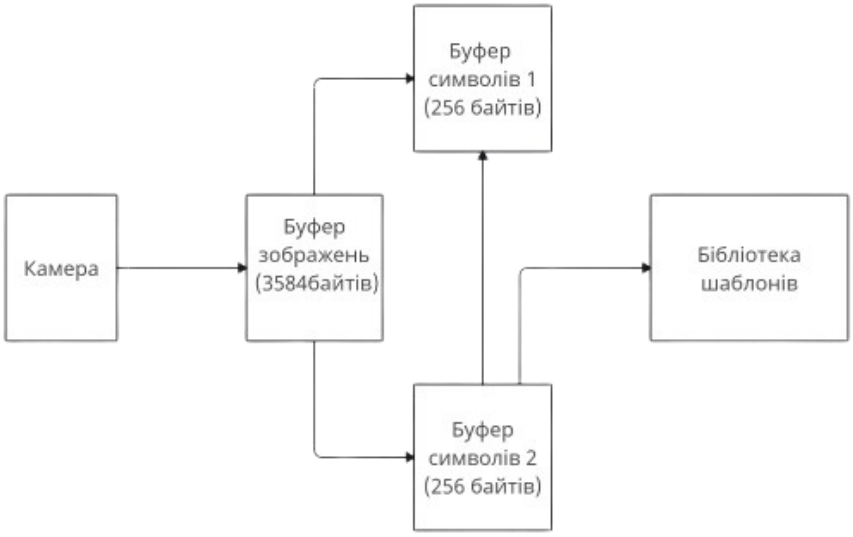


Рисунок 3.3 – Схема роботи модуля

При способі авторизації від сенсору циклічно надсилається команда Genimg, до моменту фіксації відбитку, в буфер обміну, що має роздільну здатність 256 на 288 точок з 16 градаціями сірого. До буферу надсилається команда img2TZ, яка виконує функцію згортання – алгоритм, який перетворює вхідні 35 кБайт в зображення розміром 256 байт із збереженням унікальних рис відбитку. Після цього виконується команда search – пошук та порівняння з шаблонами бібліотеки або з певним діапазоном бібліотеки. Як результат порівняння повертається номер шаблону, результат операції авторизації та коефіцієнт співпадіння. Рівень співпадіння залежить від характеристики порогу співпадіння. Поріг може бути відредаговано за допомогою програмного забезпечення шляхом встановлення одного з п’яти рівнів безпеки. Перший рівень – найменший рівень безпеки, п’ятий – найвищий.

При внесені відбитків у базу шаблонів, фіксація відбитків відбувається двічі. Перше зображення зберігається в першому буфері обміну, другий результат сканування - в другому. Зображення згортаються та відбувається операція RegModel, що дозволяє отримати усереднене значення з двох результатів. Кінцевий результат зберігається у вигляді шаблону в бібліотеці.

Для реалізації функції зчитування RFID-міток використовується зчитувач RFID-міток RC522 (рис 3.4).

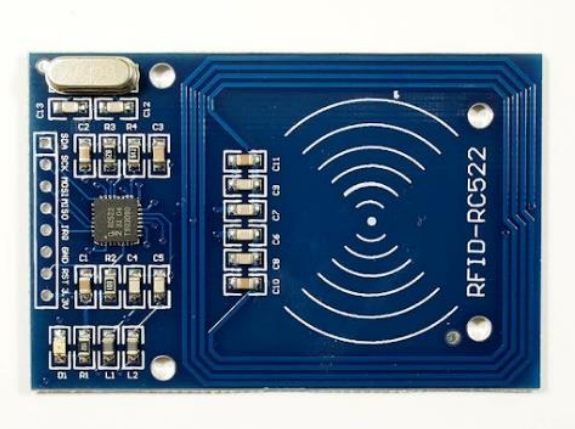


Рисунок 3.4 – RFID-зчитувач RC522

Зчитувач RC522 працює на частоті 13,56 МГц і підтримує стандарти ISO 14443A/MIFARE. Він має високу швидкість зчитування та низьке енергоспоживання, що робить його ідеальним для автономних пристроїв на базі платформи Arduino.

Живлення модуля складає 2,5-3,3 В, споживання струму - близько 13 мА в режимі очікування та 50 мА в режимі роботи. Модуль оснащений SPI інтерфейсом, що забезпечує просте підключення до Arduino.

Процес зчитування відбувається наступним чином: після наближення RFID картки або брелока до зчитувача, модуль RC522 зчитує дані з чіпа та передає їх на мікроконтролер для подальшої обробки і порівняння з базою даних.

В якості модулю бездротового зв’язку використовується мікроконтролер ESP8266 з підтримкою Wi-Fi інтерфейсу.

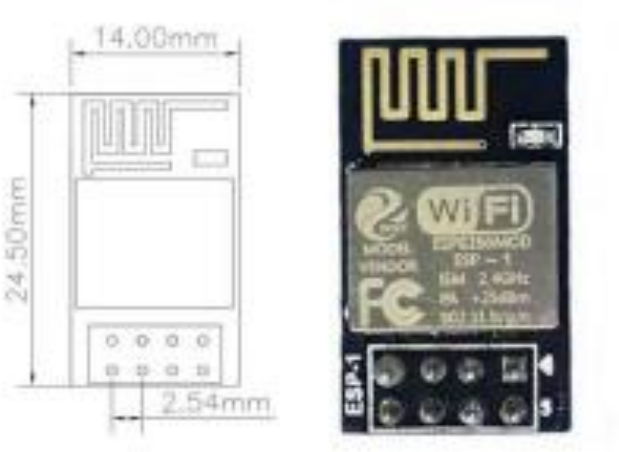


Рисунок 3.5 – Мікроконтролер ESP8266-01S

Мікроконтролер, в даному випадку хоч і використовується лише як модуль бездротового зв’язку, може також використовуватися як окремий контролер для реалізації проектів в системах автоматизації побуту та IoT. На сьогодні існує велика кількість різновидів моделей даного контролеру, від ESP-01 до ESP-12. Моделі мають відмінності головним чином в роз’ємах та кількості флеш пам’яті.

Модель мікроконтролеру ESP-01S має 8 контактів та PCB-антену (друкований передавач на самій платі) (рис. 3.5). В модельному ряду ESP8266 використовується 32 бітний процесор Tensilica L106, що може бути «розігнаний» до частоти 160 МГц. Споживання енергоживлення в режимі передавання даних складає 220 мА. Модуль потребує живлення в межах 2,5-3,6 В, для забезпечення стабільної напруги використовується мікросхема AMS1117-3,3, тобто, лінійний стабілізатор з малим падінням напруги. Модуль ESP8266 працює за протоколом IPv4, TCP/UDP, HTTP, та підтримує протоколи передавання 802.11 b/g/n, протоколи WPA/WPA2 та шифрування WEP/TKIP/AES.

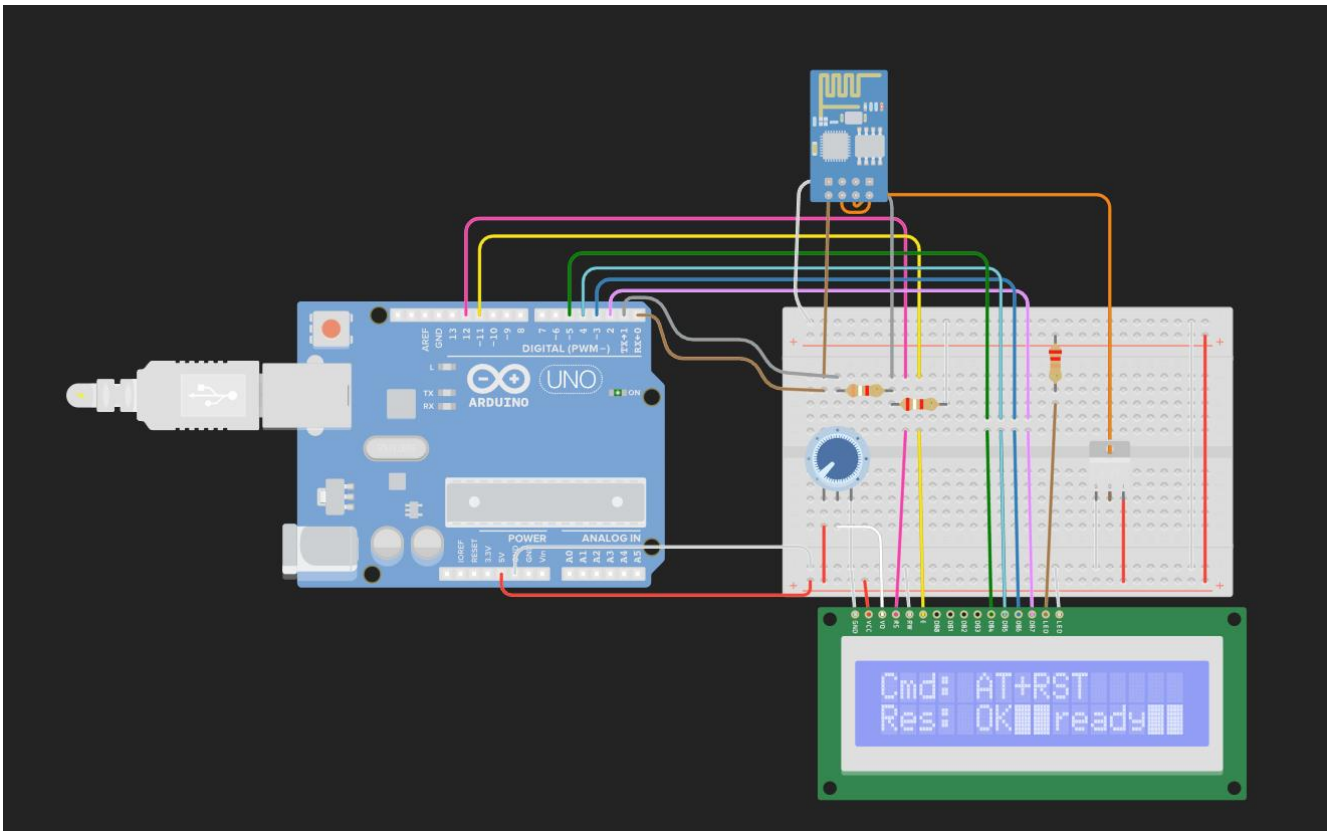


Рисунок 3.6 – Приклад роботи ESP8266-01S

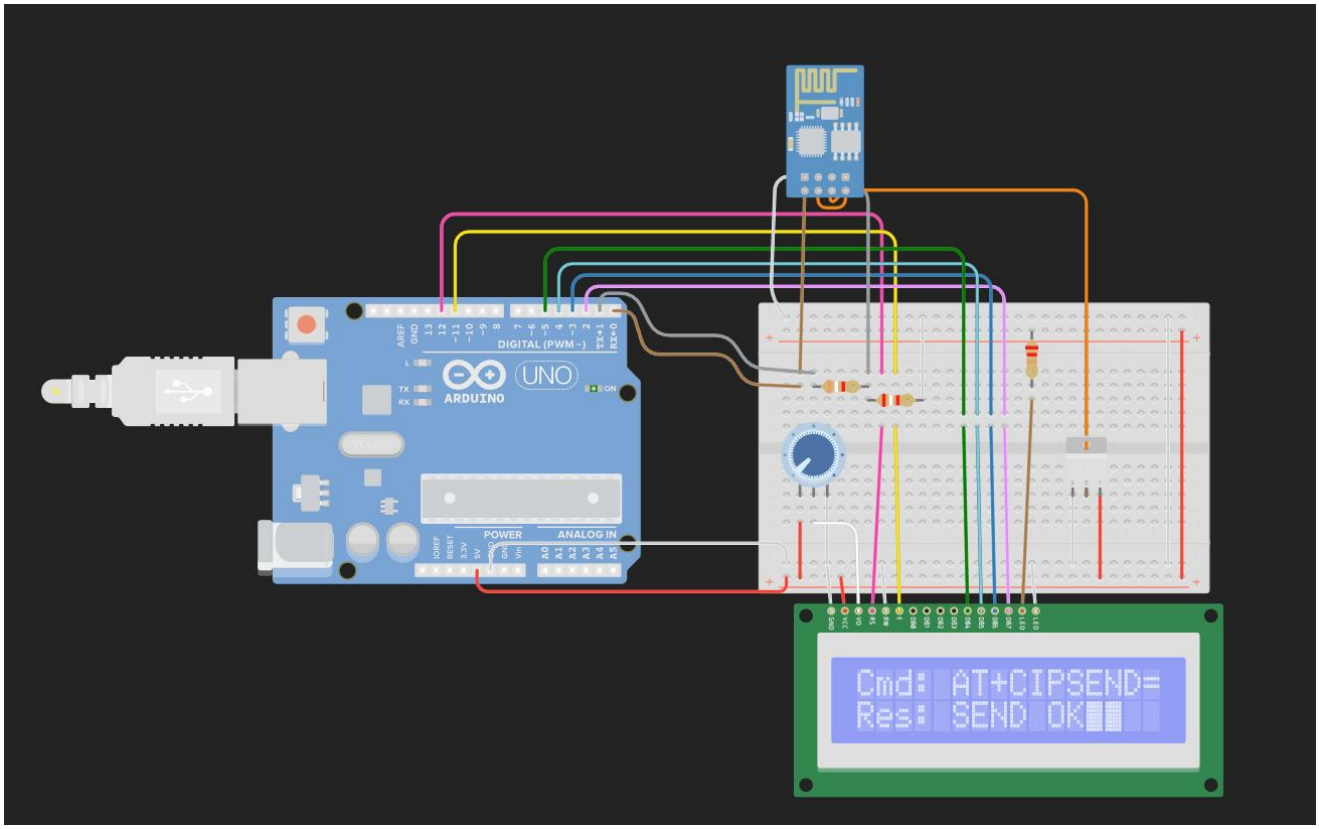


Рисунок 3.7 – Відправка даних

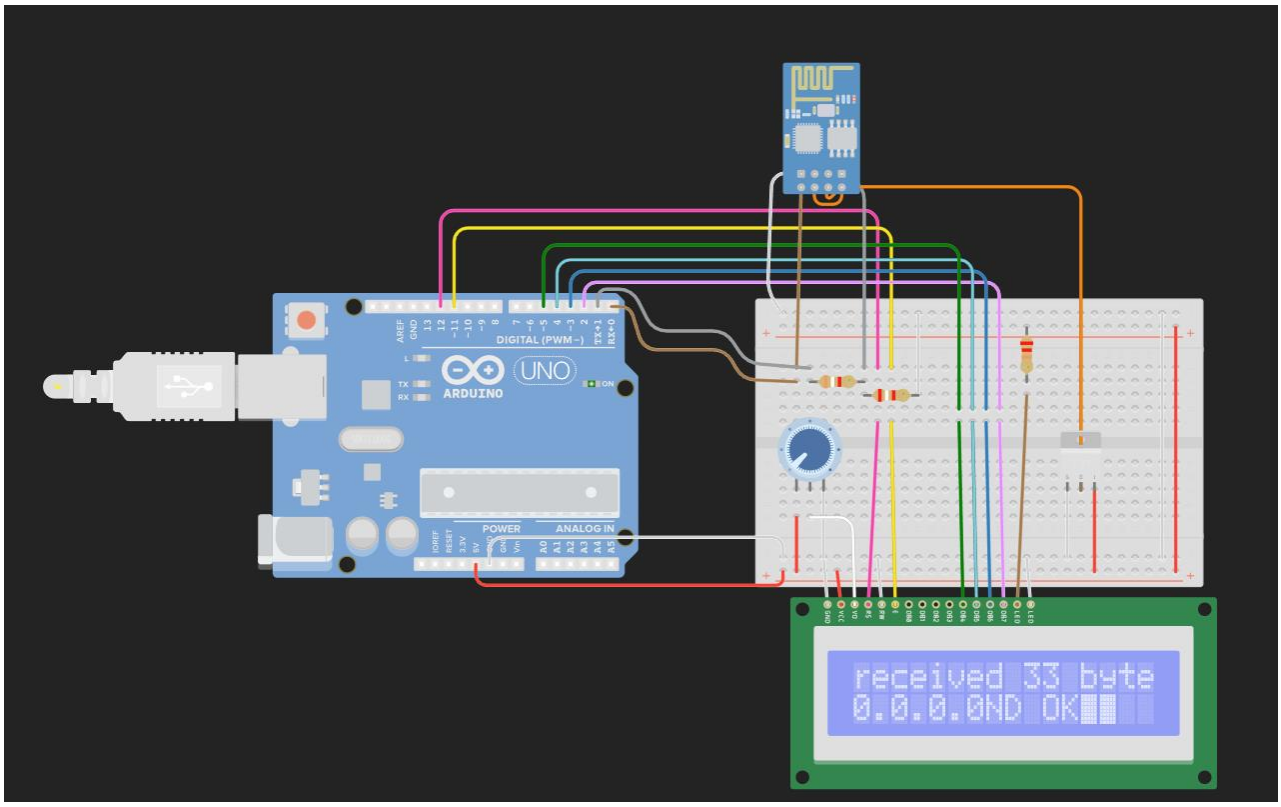


Рисунок 3.8 – Дані отримані

Для керування контролером використовуються, як браузери, так і програмне забезпечення для Android/iOS/Desktop.

В якості контролера системи пропонується застосувати платформу Arduino - відкриту програмовану апаратну платформу для роботи з різними фізичними об'єктами. Платформа являє собою просту плату з мікроконтролером та спеціальне середовище розробки для створення програмного забезпечення мікроконтролера.

Arduino може використовуватися для розробки інтерактивних систем, керованих різними датчиками і перемикачами. Такі системи, в свою чергу, можуть управляти роботою різних індикаторів, двигунів та інших пристроїв. Проекти Arduino можуть бути як самостійними, так і взаємодіючими з програмним забезпеченням, що встановлене на персональному комп'ютері (наприклад, додатками Flash, Processing, MaxMSP). Середовище розробки для програмування такої плати має відкритий вихідний код. Плата Arduino

складається з мікроконтролеру Atmel AVR та елементів обв'язки для програмування та інтеграції з іншими схемами.

3.2 Пояснення роботи моделі

Схема системи контролю доступу

1. Ідентифікація та аутентифікація користувачів

- Біометричний сканер: Зчитує відбитки пальців.
- Безконтактний зчитувач: Використовує RFID карти або брелоки.

2. Обробка даних

- Arduino: Центральний контролер для обробки даних з біометричного сканера та безконтактного зчитувача.
- Інтернет модуль (ESP8266): Відправляє дані на сервер.

3. База даних

- Зберігання шаблонів: Збереження шаблонів відбитків та RFID даних.
- Сервер: Ведення журналу відвідувань.

```
#include <Adafruit_Fingerprint.h>
#include <SPI.h>
#include <MFRC522.h>
#include <ESP8266WiFi.h>

const char* ssid = "your_SSID";
const char* password = "your_PASSWORD";
const char* server = "your_server_address";
const int fingerprintPin = 2;
const int rfidPin = 10;
WiFiClient client;

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&Serial);
MFRC522 rfid(rfidPin, SS_PIN);

void setup() {
  Serial.begin(9600);
  // Підключення до WiFi
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("Connected to WiFi");

  // Ініціалізація компонентів
```

```
  finger.begin();
  if (finger.verifyPassword()) {
    Serial.println("Fingerprint sensor connected");
  } else {
    Serial.println("Fingerprint sensor connection failed");
    while (1);
  }
  SPI.begin();
  rfid.PCD_Init();
  Serial.println("RFID reader initialized");
}

void loop() {
  if (checkFingerprint()) {
    int id = finger.fingerID;
    sendDataToServer("fingerprint", id);
  }
  if (checkRFID()) {
    String uid = getUID();
    sendDataToServer("rfid", uid);
  }
  delay(2000);
}

bool checkFingerprint() {
  finger.getImage();
  if (finger.image2Tz() == FINGERPRINT_OK) {
    if (finger.fingerFastSearch() == FINGERPRINT_OK) {
      Serial.print("Fingerprint ID: ");
      Serial.println(finger.fingerID);
      return true;
    }
  }
  return false;
}

bool checkRFID() {
  if (rfid.PICC_IsNewCardPresent() && rfid.PICC_ReadCardSerial()) {
    Serial.print("RFID UID: ");
    for (byte i = 0; i < rfid.uid.size; i++) {
      Serial.print(rfid.uid.uidByte[i] < 0x10 ? " 0" : " ");
      Serial.print(rfid.uid.uidByte[i], HEX);
    }
    Serial.println();
    return true;
  }
  return false;
}

void sendDataToServer(String type, int id) {
  if (client.connect(server, 80)) {
    client.print("GET /auth?type=");
    client.print(type);
    client.print("&id=");
    client.print(id);
    client.println(" HTTP/1.1");
    client.println("Host: " + String(server));
    client.println("Connection: close");
    client.println();
  }
  client.stop();
}
```

Рисунок 3.9 – Лістинг програмного коду на C++

Загальна схема роботи системи (рис. 3.10):

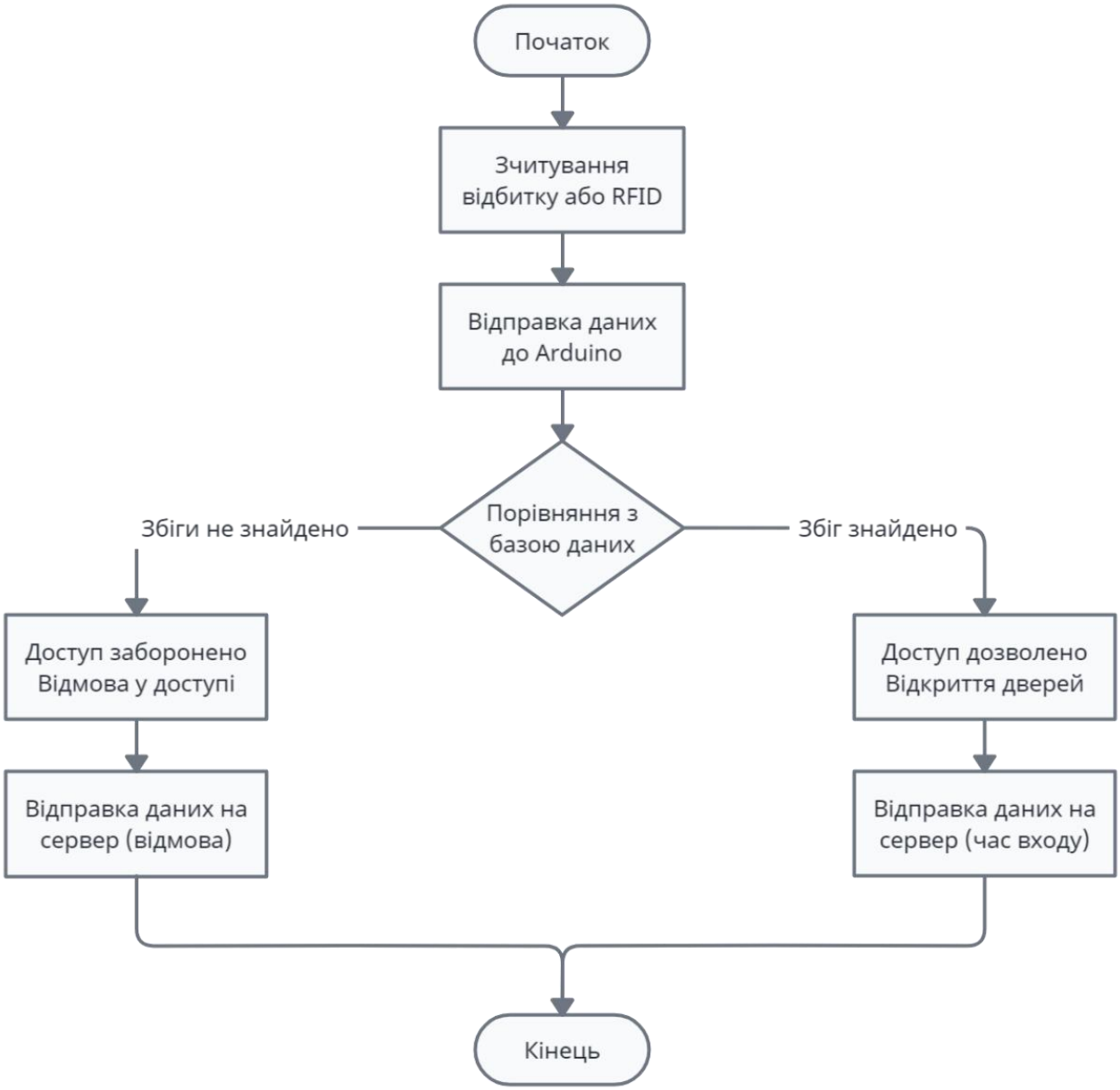


Рисунок 3.10 – Блок-схема роботи системи

Рис 3.11 – Блок-схема додавання шаблону відбитку до бази даних

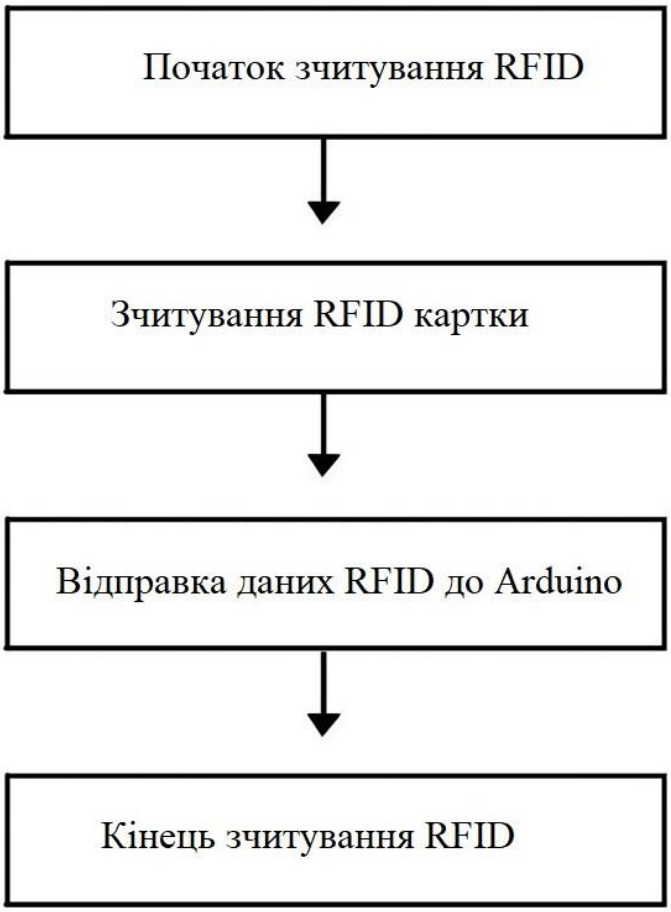


Рис 3.12 – Блок-схема зчитування RFID

Після передачі даних до Arduino, вони проходять перевірку у базі даних. Таким чином повністю виключається можливість потрапляння сторонніх людей до офісного приміщення.

Висновки за розділом 3

У цьому розділі було розглянуто процес розробки біометричної системи контролю доступу на базі платформи Arduino з використанням інтернет модуля. Система поєднує в собі використання біометричних сканерів та RFID-зчитувачів для забезпечення надійної ідентифікації користувачів та ведення журналу відвідувань. Такий підхід дозволяє забезпечити високий рівень безпеки завдяки використанню сучасних алгоритмів розпізнавання відбитків пальців та RFID-технологій.

Застосування оптичного сканера відбитків FPM10A та RFID-зчитувача RC522 дозволяє досягти швидкої та точної ідентифікації користувачів. Всі

дані про відвідування передаються на віддалений сервер через інтернет модуль, де зберігаються та аналізуються, що забезпечує можливість віддаленого моніторингу та управління системою доступу.

Важливою перевагою такої системи є можливість гнучкого налаштування політик доступу, додавання нових користувачів, а також інтеграція з іншими системами безпеки та автоматизації. Це дозволяє створити комплексну систему безпеки для офісного приміщення, яка відповідає сучасним вимогам та стандартам.

ВИСНОВКИ

У даній роботі виконано аналіз та розробку моделі системи контролю доступу до офісного приміщення через Інтернет. Проведено всебічне дослідження сучасних платформ для розробки подібних систем, включаючи Arduino, Raspberry Pi та інші мікроконтролери, та обґрунтовано вибір платформи Arduino для реалізації проекту.

Було розглянуто апаратні та програмні компоненти системи, включаючи зчитувач відбитків пальців FPM10A, RFID-зчитувач RC522, мікроконтролер ESP8266 для бездротового зв’язку, та інші ключові елементи. Запропоновано та реалізовано модель системи, що забезпечує високу безпеку, гнучкість та надійність управління доступом до офісних приміщень.

Особливу увагу приділено аутентифікації на основі біометричних даних, RFID-чипів, перевірці даних згідно з базою даних для надання доступу. Впроваджено функціональність відправки ідентифікаторів користувачів через Інтернет для реєстрації наявності осіб на об’єкті, що дозволяє інтегрувати систему з іншими безпековими та управлінськими платформами.

Запропонована модель демонструє високу ефективність, простоту в реалізації та низькі витрати, що робить її привабливою для малих та середніх підприємств, які прагнуть підвищити рівень безпеки та контролю доступу до своїх приміщень. Розроблена модель може бути основою для подальших досліджень та вдосконалення систем контролю доступу з використанням більш складних та надійних методів аутентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Системи контролю доступу: що це таке і як працює [Електронний ресурс] , [Веб-сайт] URL: https://zakarpattya.net.ua/News/200909-Systemy-kontroliu-dostupu-shcho-tse-take-i-iak-pratsiuie (Дата звернення: 05.09.2024) – назва з екрану
2. Що таке системи контролю доступу і як вони працюють [Електронний ресурс] , [Веб-сайт] URL: https://l-vorota.com.ua/ua/a422469-chto-takoe-sistemy.html?srsltid=AfmBOorWHFumSZVGg4dBR0E4M8NHxskWgE-oF0NMU2kLJmPxMY_pY52Q (Дата звернення: 06.09.2024) – назва з екрану
3. Система контролю доступу. Види та відмінності СКУД. Особливості вибору СКД. [Електронний ресурс] , [Веб-сайт] URL: https://revel.com.ua/info/articles/skud-vidy-i-otlichiya/?lang=ua (Дата звернення: 19.09.2024) – назва з екрану
4. Контролери СКУД: види, призначення, складові [Електронний ресурс] , [Веб-сайт] URL: https://nadzor.ua/uk/blog/kontrol-dostupa/kontrollery-skud-vidy-naznacenie-sostavlausie (Дата звернення: 21.09.2024) – назва з екрану
5. Вивчаємо Raspberry Pi. #1. Знайомство [Електронний ресурс] , [Веб-сайт] URL: https://evo.net.ua/ru/izuchaem-raspberry-pi.-chast-1.-znakomstvo/ (Дата звернення: 22.09.2024) – назва з екрану
6. ESP32 vs ESP8266 Порівняння контролерів [Електронний ресурс] , URL: [Веб-сайт] https://artificer.com.ua/esp32-vs-esp8266-sravnenie-kontrollerov/ (Дата звернення: 22.09.2024) – назва з екрану
7. Мікроконтролер Arduino [Електронний ресурс] , [Веб-сайт] URL: https://bitkit.com.ua/shho-take-arduino (Дата звернення: 22.09.2024) – назва з екрану

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна

Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Кафедра комп'ютерних систем та робототехніки
Рівень вищої освіти (освітньо-кваліфікаційний рівень) **Бакалавр**
Галузь знань: 12 – Інформаційні технології
Спеціальність: 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних
систем та робототехнікики
к. ф.-м. н., доц. ХРУСЛОВ М. М.
« 05» вересня 2024року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Папуші Руслана Олександровича
(прізвище, ім'я, по батькові студента)

1. Тема роботи «Модель комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет»

керівник роботи Лабенко Дмитро Петрович , к.т.н, доцент кафедри КСР
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «___»_____2024 року
№_____

2. Строк подання студентом роботи **30 листопада 2024**

3. Перелік питань, які потрібно розробити
1. Аналіз існуючих моделей систем контролю доступу до офісного приміщення через Інтернет.

2. Вивчення основних принципів роботи системи контролю доступу до офісного приміщення через Інтернет.
3. Вибір платформи для розробки моделі системи контролю доступу до офісного приміщення.
4. Розробка моделі комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет.
5. Розробка пояснювальної записки.

4. План роботи

№ з/п	Назви етапів роботи	Термін виконання етапів роботи
1	Аналіз та пошук методичної літератури щодо побудови моделі комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет	05.09.2024 - 17.09.2024
2	Огляд і аналіз існуючих систем контролю доступу	18.09.2024 - 24.09.2024
3	Побудова моделі системи контролю доступу до офісного приміщення через Інтернет	25.09.2024 - 09.10.2024
4	Програмна реалізація моделі комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет	10.10.2024 - 24.10.2024
5	Проведення тестування розробленої моделі	25.10.2024 - 08.11.2024
6	Розробка та оформлення пояснювальної записки	09.11.2024 - 29.11.2024
7	Представлення роботи	30.11.2024

5. Дата видачі завдання ***05 вересня 2024року.***

Студент Папуша Р.О
ініціали, прізвище
підпис

Керівник роботи Лабенко Д.П
ініціали, прізвище
підпис

ДОДАТОК Б

Затверджую
_____
«_____»_____2024 р.

Технічне завдання
на розробку програмного вироби
«Модель комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет»

Назва розділу	Назва і зміст підрозділу
1. Введення	1.1. Назва програмного вироби – Модель комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет 1.2. Галузь застосування – системи безпеки та контролю доступу.
2. Підстава для розробки	2.1. Навчальний план за спеціальністю 123 – Комп'ютерна інженерія 2.2. Завдання на кваліфікаційну роботу бакалавра № _____ від «___» _____2024 (представити як Додаток А до пояснювальної записки до кваліфікаційної роботи).
3. Призначення розробки	3.1. Мета розробки: створення ефективного та надійного інструменту для управління доступом до офісних приміщень, що забезпечить високий рівень безпеки та зручність використання. 3.2. Призначення розробки: полягає в створенні інструменту, який забезпечить безпечний та контрольований доступ до офісних приміщень, зменшить ризики несанкціонованого проникнення та підвищить загальний рівень безпеки. 3.3. Початкові дані для розробки: дані про користувачів та їх рівні доступу, технічні характеристики обладнання, вимоги до безпеки та інтеграції з існуючими системами.
4. Технічні вимоги до програмного виробу	4.1. Вимоги до функціональних характеристик: 1) Аутентифікація користувачів за відбитками пальців 2) Аутентифікація користувачів за RFID-чипами у брелоках 3) Перевірка даних згідно з базою даних 4) Відправка даних про доступ через Інтернет 4.2. Вимоги до надійності: Забезпечення стабільної роботи системи навіть при великому навантаженні. 4.3. Вимоги до умов експлуатації: немає

<table>
<tr><td></td><td colspan="2">4.4. Вимоги до складу і параметрів технічних засобів:
Персональний комп’ютер або мікроконтролер Arduino з відповідними модулями (FPM10A, ESP8266 тощо).
4.5. Вимоги до інформаційної та програмної сумісності:
Забезпечення сумісності з усіма основними обчислювальними засобами та мережевими протоколами.
4.6. Вимоги до маркування та упаковки: відсутні.
4.7. Вимоги до транспортування і зберігання: відсутні.
4.8. Спеціальні вимоги: відсутні.</td></tr>
<tr><td>5. Вимоги до програмної документації.</td><td colspan="2">Програмною документацією до виробу «Модель комп’ютеризованої системи контролю доступу до офісного приміщення через Інтернет» вважати:
1) Справжнє Технічне завдання на розробку програмного вироби (представити у вигляді Додатку Б до пояснювальної записки до дипломної роботи).
2) Програму і методику випробувань розробленого програмного вироби (представити у вигляді Додатку В до пояснювальної записки до дипломної роботи).
3) Опис програмного вироби (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи).</td></tr>
<tr><td>6. Техніко-економічні показники</td><td colspan="2">В даному розділі можуть бути представлені:

1) Справжнє Технічне завдання на розробку програмного вироби (представити у вигляді Додатку Б до пояснювальної записки до дипломної роботи).

2) Методику розрахунку інформативності змінних стану (у вигляді глав 3.2 та 3.3 пояснювальної записки до кваліфікаційної роботи).
3) Опис виробу (представити в розділі 3 пояснювальної записки до кваліфікаційної роботи)</td></tr>
<tr><td>7. Стадії і етапи розробки</td><td>Дата</td><td>Назва етапу</td></tr>
<tr><td></td><td>05.09.2024 - 17.09.2024</td><td>Аналіз та пошук методичної літератури щодо побудови моделі комп’ютеризованої системи контролю доступу до офісного приміщення через Інтернет</td></tr>
<tr><td></td><td>18.09.2024 - 24.09.2024</td><td>Огляд і аналіз існуючих систем контролю доступу</td></tr>
</table>

	25.09.2024 - 09.10.2024	Побудова моделі системи контролю доступу до офісного приміщення через Інтернет
	10.10.2024 - 24.10.2024	Програмна реалізація моделі комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет
	25.10.2024 - 08.11.2024	Проведення тестування розробленої моделі
	09.11.2024 - 29.11.2024	Розробка та оформлення пояснювальної записки
	30.11.2024	Представлення роботи
8. Порядок контролю і приймання	1) Перевірку ходу розробки програмного виробу керівнику робіт виконувати раз в 3 тижні. 2) Випробування програмного продукту провести відповідно до програми та методики випробувань на базі комп'ютерного класу. 3) Захист розробленої моделі провести на засіданні Атестаційної комісії. 4) Пояснювальну записку подати в електронному вигляді в 1 примірнику.	

Виконавець
студент групи К1-41
Папуша Р.О.
_____

Замовник
канд. техн. наук, доц.
Лабенко Д.П.
_____

Додаток В

Програма і методика випробувань програмного виробу

«Модель комп’ютеризованої системи контролю доступу до офісного приміщення через Інтернет»

1. **Об'єкт випробувань**
    1. Назва програмного виробу : «Модель комп’ютеризованої системи контролю доступу до офісного приміщення через Інтернет»
    2. Галузь застосування : Контроль доступу до приміщень
    3. Перераховані відомості запозичуються з відповідних розділів Технічного завдання.
2. **Мета випробувань**

Перевірка відповідності функціональності програмної реалізації системи заявленим функціональним можливостям в технічному завданні (Додаток Б до пояснювальної записки до кваліфікаційної роботи).

3. **Загальні положення**
    1. **Підстави для проведення випробувань**

        Підставою для проведення випробувань є наказ про призначення атестаційної комісії.

    2. **Місце і тривалість випробувань**

        Приймальні (приймально-здавальні) випробування проводяться на базі комп'ютерного класу кафедри в період роботи атестаційної комісії.

    3. **Обсяг випробувань**

        Приймальні випробування програмного вироби проводяться в обсязі відповідному цієї програми і методики випробувань.

    4. **Організації, які беруть участь у випробуваннях**

        Приймальні випробування проводяться атестаційною комісією напередодні засідання (або в процесі засідання) за участю Замовника, Виконавця та інших осіб, присутніх на засіданні.

4. **Вимоги до програми або програмного виробу**

Модель повинна задовольняти наступним вимогам:

1. персональний комп’ютер або мікроконтролер Arduino з відповідними модулями (FPM10A, ESP8266 тощо).

2. вимоги до надійності;
3. передбачити захист від некоректних дій користувача;
4. сумісність з іншими програмними продуктами;
5. забезпечення стабільної роботи системи навіть при великому навантаженні.
6. забезпечення сумісності з усіма основними обчислювальними засобами та мережевими протоколами.
7. вимоги до складу і параметрів технічних засобів;
8. вимоги до маркування та упаковки (не висуваються);
9. вимоги до транспортування і зберігання (не висуваються).

Спеціальні вимоги (не пред'являються).

5. Вимоги до програмної документації

Програмною документацією до виробу «Модель комп'ютеризованої системи контролю доступу до офісного приміщення через Інтернет» вважати:

1. Програмною документацією щодо розроблюваного програмного продукту вважати:
2. справжнє технічне завдання на розробку програми (представити як Додаток Б до пояснювальної записки до кваліфікаційної роботи);
3. Програму і методику випробувань розробленої програми (представити як Додаток В до пояснювальної записки до кваліфікаційної роботи);
4. рекомендацій щодо застосування створеної програмної стандартизації у проєктах (представити в Розділі 3 пояснювальної записки до кваліфікаційної роботи).

6. Засоби і порядок випробувань

6.1 Засоби випробувань

Для проведення випробувань необхідний персональний комп'ютер або мікроконтролер Arduino з відповідними модулями (FPM10A, ESP8266 тощо)

6.2 Порядок проведення випробувань

Як правило, випробування проводяться в два етапи:
-ознайомчий (1-й етап);
-випробування програмного виробу (2-й етап).
Перелік перевірок, що проводяться на 1 етапі випробувань, включає в себе:

1. Перевірку комплектності програмної документації.
2. Перевірка комплектності складу програмної документації здійснюється за критерієм наявності зазначеної в ТЗ документації.
3. Перевірку комплектності складу технічних і програмних засобів.
4. Методику проведення перевірок на 1 етапі випробувань.

5. Якість програмної документації перевіряється на відповідність вимогам стандартів ДСТУ.

Перелік перевірок, що проводяться на 2 етапі випробувань, включає в себе:

1. перевірку відповідності технічних характеристик програми вимогам технічного завдання;
2. перевірку ступеня виконання функціональних вимог до програми;
3. методику проведення перевірок, що входять до переліку по 2 етапу випробувань.

1. Програма працює відповідно до умов експлуатації персонального комп'ютера або мікроконтролера Arduino.
2. Для роботи необхідний персональний комп'ютер або мікроконтролер Arduino з відповідними модулями (FPM10A, ESP8266 тощо).
3. Порядок проведення випробувань:
   3.1. Перевірка роботи модулю FPM10A за допомогою SFG Demo.
   3.2. При прикладанні пальця до сканеру відбитку буде відбуватися перевірка відбитку з існуючими у базі.
   3.3. У разі наявності відбитку дозвіл буде надано. У разі відсутності – не буде надано.

   Для проведення випробувань пропонується тест 1 та тест 2.

Тест 1

1. Перевірка роботи сканера відбитків у разі наявності відбитку у базі.

2. Отримання дозволу.

Рисунок В.1 Тест 1

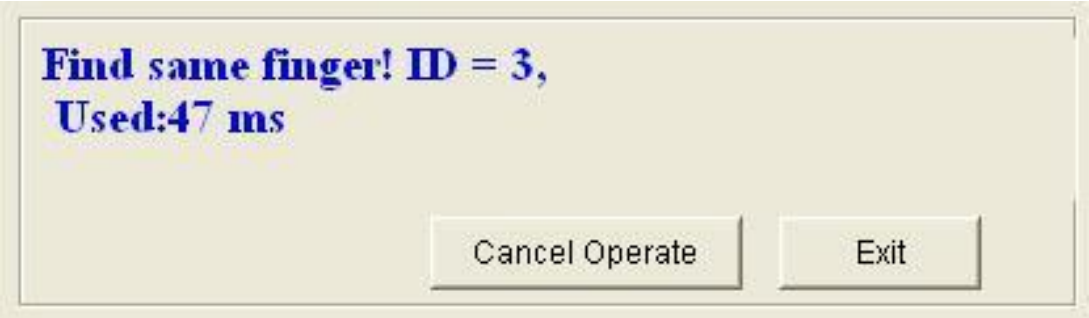


Рисунок В.2 Тест 1

Тест 2

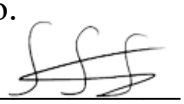
1. Перевірка роботи сканера відбитків у разі наявності відбитку у базі.
2. Видача помилки.

Рисунок В.3 Тест 2

Рисунок В.4 Тест 2

Тест вважається пройденим, якщо відбуваються вказані операції і їх відображення у програмному продукті.

Висновки: тест 1 успішно пройшов випробування і тест 2 успішно пройшов випробування. Випробування пройшло успішно.

Виконавець: студент групи КІ-41, Папуша Р.О. 

Додаток Г

Програмний код моделі

```
#include <LiquidCrystal.h>
LiquidCrystal lcd(12, 11, 5, 4, 3, 2);

const String host = «https://httpbin.org/»;
const String red = «Simulator Wifi»;
const String pass = «»;

char buf[80];
int i;
int e = 1;

void setup() {
  Serial.begin(115200);
  lcd.begin(16, 2);
  delay(500);
  connectWiFi();
}

void loop() {
  request();
  while (true) {
  }
}

void connectWiFi() {
  comando(«AT+RST»);
  delay(100);
  respuesta();
  delay(1000);
  comando(«AT+CWJAP_CUR=\»» + red + «\»,\»» + pass + «\»»);
  delay(100);
  respuesta();
  delay(1000);
  comando(«AT+CWJAP_CUR?»);
  delay(100);
  respuesta();
}

void comando(String cmd) {
  lcd.clear();
  lcd.home();
  lcd.print(«Cmd: « + cmd);
  Serial.println(cmd);
}

void respuesta() {
  while (Serial.available() == 0) {
    ;
  }
  i = 0;
  while (Serial.available() > 0) {
    char x = Serial.read();
    buf[i] = x;
    i++;
  }
  lcd.setCursor(0, 1);
  lcd.print(«Res: «);
```

```
        lcd.print(buf);
        memset(buf, 0, sizeof(buf));
      }

      void connectToPage() {
        String cmd = «AT+CIPSTART=\»TCP\»,\»»;
        cmd += String(host);
        cmd += «\»,80»;
        comando(cmd);
        delay(100);
        respuesta();
        delay(1000);
        bool p = strstr(buf, «ERROR»);
        if (p) {
          e = 1;
        } else {
          e = 0;
        }
      }

      void request() {
        while (e == 1) {
          connectToPage();
          if (e == 1) {
            lcd.home();
            lcd.print(«Connection Error»);
            lcd.setCursor(0, 1);
            lcd.print(«Reconnecting…»);
          }
        }
        String getStr = «GET «;
        getStr += «/ip»;
        getStr += « HTTP/1.1\r\n»;
        getStr += «Host: « + host + «\r\n»;
        getStr += «\r\n\r\n»;
        if (sendGetCmd(getStr) == «error») {
          e = 1;
        }
      }

      String sendGetCmd(String getStr) {
        String cmd = «AT+CIPSEND=»;
        cmd += String(getStr.length());
        comando(cmd);
        delay(100);
        if (Serial.find(«>»)) {
          Serial.print(getStr);
          delay(10);
          respuesta();
          delay(500);
          readSite();
        } else {
          Serial.println(«AT+CIPCLOSE»);
          lcd.print(«CIPSEND ERROR»);
          return «error»;
        }
      }

      void readSite() {
        Serial.find(«+IPD»);
        int len = Serial.parseInt();
        Serial.find(«200 success»);
        Serial.find(«Content-Length»);
```

```
  int contentlen = Serial.parseInt();
  Serial.find(«Content-Type»);
  int ip1 = Serial.parseInt();
  int ip2 = Serial.parseInt();
  int ip3 = Serial.parseInt();
  int ip4 = Serial.parseInt();
  while (Serial.available() > 0) {
    char page[contentlen];
    Serial.readBytes(page, contentlen);
    for (int i = 0; i < len; i++) {
      Serial.write(page[i]);
    }
  }
  lcd.home();
  lcd.print(«received «);
  lcd.print(contentlen);
  lcd.print(« bytes»);
  lcd.setCursor(0, 1);
  lcd.print(ip1);
  lcd.print(«.»);
  lcd.print(ip2);
  lcd.print(«.»);
  lcd.print(ip3);
  lcd.print(«.»);
  lcd.print(ip4);
}

void desplaza(int n) {
  for (int i = 0; i < n; i++) {
    lcd.scrollDisplayLeft();
    delay(300);
  }
  for (int i = 0; i < n; i++) {
    lcd.scrollDisplayRight();
    delay(300);
  }
}
```

Рисунок Г.1 – Лістинг програмного коду для тестування ESP8266

```
#include <Keypad.h>
#include <Servo.h>
#include <string.h>
#include <LiquidCrystal.h>

const byte rows = 4;
const byte columns = 4;
int holdDelay = 700;
int n = 3;
int state = 0;
char key = 0;
int pos = 0;
int buzzer = A3;
int redled = A1;
int greenled = A2;
int button = 2;
int btnState;
int statebtn = 0;
String default_passwd = "0000";
String input_passwd = "";
char lock_key = '*';
```

```
      char unlock_key = '#';
      char change_pass_key = '*';
      Servo servo_A0;

      char keys[rows][columns] = {
        {'1', '2', '3', 'A'},
        {'4', '5', '6', 'B'},
        {'7', '8', '9', 'C'},
        {'*', '0', '#', 'D'},
      };

      byte rowPins[rows] = {6, 7, 8, 9};
      byte columnPins[columns] = {10, 11, 12, 13};
      Keypad keypad = Keypad(makeKeymap(keys), rowPins, columnPins, rows,
columns);
      LiquidCrystal lcd(0, 1, A4, 3, 4, 5);

      char function_key(int n) {
        char temp = keypad.getKey();
        if ((int)keypad.getState() == PRESSED) {
          if (temp != 0) { key = temp; }
        }
        if ((int)keypad.getState() == HOLD) {
          state++;
          state = constrain(state, 1, n);
          delay(holdDelay);
        }
        if ((int)keypad.getState() == RELEASED) {
          key += state;
          state = 0;
        }
        delay(100);
        return key;
      }

      String input_password(int num_char) {
        String passwd = "";
        do {
          char temp = keypad.getKey();
          if (temp != 0) {
            LCD_display(passwd.length(), 1, "*");
            passwd += temp;
          }
          delay(100);
        } while (passwd.length() < num_char);
        return passwd;
      }

      String Change_password(int num_char, String current_passwd) {
        LCD_display(0, 0, "OLD PASSWORD:");
        String old_passwd = input_password(num_char);
        if (old_passwd != current_passwd) {
          lcd.clear();
          LCD_display(0, 0, "WRONG PASSWORD!");
          return current_passwd;
        }
        lcd.clear();
        LCD_display(0, 0, "NEW PASSWORD:");
        String new_passwd = input_password(num_char);
        lcd.clear();
        LCD_display(0, 0, "CONFIRM PASSWORD");
        String confirm_passwd = input_password(num_char);
        if (confirm_passwd == new_passwd) {
```

```
      lcd.clear();
      LCD_display(0, 0, "CHANGED PASSWORD");
      return confirm_passwd;
    } else {
      lcd.clear();
      LCD_display(0, 0, "NOTHING CHANGES!");
      return current_passwd;
    }
  }

  void Unlock() {
    lcd.clear();
    LCD_display(0, 0, "INPUT PASSWORD:");
    input_passwd = input_password(4);
    if (input_passwd == default_passwd) {
      lcd.clear();
      LCD_display(0, 0, "OPENNING!!!");
      digitalWrite(greenled, HIGH);
      digitalWrite(redled, LOW);
      for (pos = 0; pos <= 180; pos += 1) {
        servo_A0.write(pos);
        delay(15);
      }
      delay(3000);
      lcd.clear();
      LCD_display(0, 0, "CLOSING!!!");
      for (pos = 180; pos >= 0; pos -= 1) {
        servo_A0.write(pos);
        delay(15);
      }
    } else {
      LCD_display(0, 0, "WRONG PASSWORD!");
      tone(buzzer, 900, 2000);
      digitalWrite(greenled, LOW);
      digitalWrite(redled, HIGH);
      delay(2000);
    }
    input_passwd = "";
    key = 0;
  }

  void LCD_display(int column, int line, String message) {
    lcd.setCursor(column, line);
    lcd.print(message);
  }

  void setup() {
    servo_A0.attach(A0);
    servo_A0.write(pos);
    pinMode(redled, OUTPUT);
    pinMode(greenled, OUTPUT);
    pinMode(buzzer, OUTPUT);
    pinMode(button, INPUT);
    lcd.begin(16, 2);
    LCD_display(4, 0, "Welcome!");
    delay(2000);
    lcd.clear();
  }

  void loop() {
    btnState = digitalRead(button);
    digitalWrite(greenled, LOW);
    digitalWrite(redled, LOW);
```

```
        char tempKey = keypad.getKey();
        LCD_display(0, 0, "STATUS: LOCKED!");
        LCD_display(0, 1, "UNLOCK: PRESS #");
        if (btnState == LOW) {
          statebtn = 1;
        }
        if (tempKey == '#' || tempKey == '*') {
          statebtn = 2;
        }
        if (statebtn == 1) {
          lcd.clear();
          LCD_display(0, 0, "OPENNING!!!");
          digitalWrite(greenled, HIGH);
          digitalWrite(redled, LOW);
          for (pos = 0; pos <= 180; pos += 1) {
            servo_A0.write(pos);
            delay(15);
          }
          delay(3000);
          lcd.clear();
          LCD_display(0, 0, "CLOSING!!!");
          for (pos = 180; pos >= 0; pos -= 1) {
            servo_A0.write(pos);
            delay(15);
          }
          statebtn = 0;
        } else if (statebtn == 2) {
          if (tempKey == unlock_key) {
            Unlock();
          }
          if (tempKey == change_pass_key) {
            default_passwd = Change_password(4, default_passwd);
            delay(2000);
            key = 0;
          }
        }
      }
```

Рисунок Г.2 – Лістинг програмного коду моделі