МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Обслуговування комп'ютерних систем і мереж»

Група: 4КС-58

Дипломний проєкт

здобувача освіти денної форми навчання
КС.58.04.000.ДП

ВИТИКАЧА ОЛЕКСАНДРА ДМИТРОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: **«Обслуговування комп'ютерних систем і мереж»**

Група: **4КС-58**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проєкту на тему:

Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу

Проектний матеріал складається з пояснювальної записки на 67 сторінках та графічного (презентаційного) матеріалу на 12 аркушах (слайдах)

Дипломник _____ (Витикач О.Д.)

Керівник _____ (Кільдішев В.Й.)

Консультанти:

з економічного розділу _____ (Канський М.Ю.)

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Краснокутська К.Г.)

Захист «30» червня 2025 р. Протокол ЕК № 8

Оцінка ЕК 4 (добре) / 75 б.

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ПІ*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Обслуговування комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"19" 05 2025 р.

ЗАВДАННЯ

на дипломний проєкт

Здобувачеві освіти *Витикача Олександра Дмитровича*

(прізвище, ім'я, по батькові)

1. Тема проекту *Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу*

затверджена наказом по коледжу від "14" листопада 2025р. № 246

2. Термін здачі закінченого проекту 16.06.25

3. Вихідні данні до проекту *1. Розробка системи контролю доступу на основі Arduino. 2. Інтеграція компонентів у єдину систему на платформі Arduino; 3. Алгоритм роботи багаторівневої системи на основі Arduino; 4. Розробка і опис програмного забезпечення; 5. Тестування програмного і апаратного забезпечення проєкту*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Аналіз існуючих систем захисту приміщень; Розробка багаторівневої системи захисту приміщення на платформі Arduino; Розробка системи контролю доступу на основі Arduino; Розробка багаторівневої системи захисту приміщення; Опис роботи схеми і підключення елементів; Тестування програмного і апаратного забезпечення проєкту

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Типи систем безпеки; Основні технології виявлення диму; Функціональні вимоги до багаторівневої системи захисту приміщення; Схема взаємодії компонентів багаторівневої системи захисту приміщення; Алгоритм авторизації системи контролю доступу; Схема з компонентів системи захисту приміщення з датчиком газу, диму та контролем доступу; Тестування клавіатури та перевірка роботи сервоприводу; Тестування датчика газу та диму

6. Консультанти по проекту, із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	*Кільдішев В.Й.*		
Економічний розділ	*Канський М.Ю.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 16.05.25

Керівник *Кільдішев В.Й.* _____
(підпис)

Завдання прийняв до виконання *Витикач О.Д.* _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	*Вступ. Постановка задачі проектування*	19.05.2025	
2	*Аналіз технічного завдання та пошук літератури*	21.05.2025	
3	*Аналіз існуючих систем захисту приміщень*	22.05.2025	
4	*Системи контролю доступу: принципи роботи та класифікація*	24.05.2025	
5	*Визначення основних вимог до багаторівневої системи захисту*	26.05.2025	
6	*Розробка багаторівневої системи захисту приміщення на платформі Arduino*	28.05.2025	
7	*Розробка системи контролю доступу на основі Arduino*	30.05.2025	
8	*Алгоритм роботи багаторівневої системи на основі Arduino*	02.06.2025	
9	*Оцінка ефективності та перспективи розвитку розробленої системи*	05.06.2025	
10	*Оцінка ефективності розробленої системи на платформі Arduino*	07.06.2025	
11	*Рекомендації щодо покращення системи*	09.06.2025	
12	*Виконання економічних розрахунків*	10.06.2025	
13	*Розробка питань з охорони праці та техніки безпеки*	12.06.2025	
14	*Підготовка мультимедійної презентації проекту*	14.06.2025	

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КС 58. 04 000. 00 ДП	Дипломний проєкт		
А4			КС 58. 04 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КС 58. 04 000. 00 ДП		
Розробив		Кільдішев В.Й.		20.06	Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу	Літ.	Аркуш 4 / Аркушів 67
Перевірив		Витикач О.Д.		20.06		Н Д П	
Н. контр.		Петрашова В.І.		20.06		ВСП "ОТФК ОНТУ" гр.4КС-58	
Затверд.		Кривченко Ю.В.		20.06			

ЗМІСТ

ВСТУП

У сучасному світі проблема безпеки приміщень є надзвичайно актуальною, оскільки зростання кількості випадків пожеж, витоків небезпечних газів та несанкціонованого доступу до об'єктів вимагає застосування сучасних технологій для забезпечення надійного захисту. Захист приміщень, особливо тих, де зберігаються цінні матеріали, інформація або знаходяться люди, потребує комплексного підходу, що включає в себе використання різноманітних сенсорних та інформаційних технологій.

Системи, що використовують датчики газу, диму та контролю доступу, є одними з найбільш ефективних засобів для забезпечення безпеки в приміщеннях. Вони здатні вчасно виявити загрози, запобігти нещасним випадкам і зменшити можливі збитки. Однак, попри наявність численних рішень на ринку, більшість з них обмежуються окремими аспектами безпеки і не забезпечують достатнього рівня комплексного захисту.

Метою цього дипломного проєкту є розробка багаторівневої системи захисту приміщення, яка включає в себе інтеграцію датчиків газу, диму та системи контролю доступу в єдину ефективну структуру.

Актуальність проєкту полягає в необхідності удосконалення технологій безпеки для зменшення ризиків виникнення надзвичайних ситуацій, захисту людей та матеріальних цінностей. Очікується, що розроблена система дозволить підвищити рівень безпеки в різноманітних типах приміщень, таких як офіси, склади, житлові комплекси та інші об'єкти.

Завданням проєкту є розробка ефективної і надійної багаторівневої системи захисту, що поєднує у собі сучасні технології детекції загроз та контролю доступу для забезпечення комплексного захисту приміщень.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Аналіз існуючих систем захисту приміщень

1.1.1 Огляд сучасних систем безпеки

Сучасні системи безпеки активно впроваджуються в житлових, комерційних та промислових об’єктах з метою запобігання несанкціонованому доступу, виявлення небезпек та своєчасного реагування на загрози. Ці системи охоплюють широкий спектр технологій, які дозволяють ефективно контролювати стан об'єкта, забезпечуючи безпеку життя і майна.

До основних типів систем безпеки належать:

1) системи відеоспостереження;

2) системи охоронної сигналізації;

3) пожежна сигналізація та датчики диму;

4) газові сенсори;

5) системи контролю доступу;

6) інтелектуальні (розумні) системи безпеки;

7) інтегровані системи безпеки.

Основні типи систем безпеки представлено на рис. 1.1.

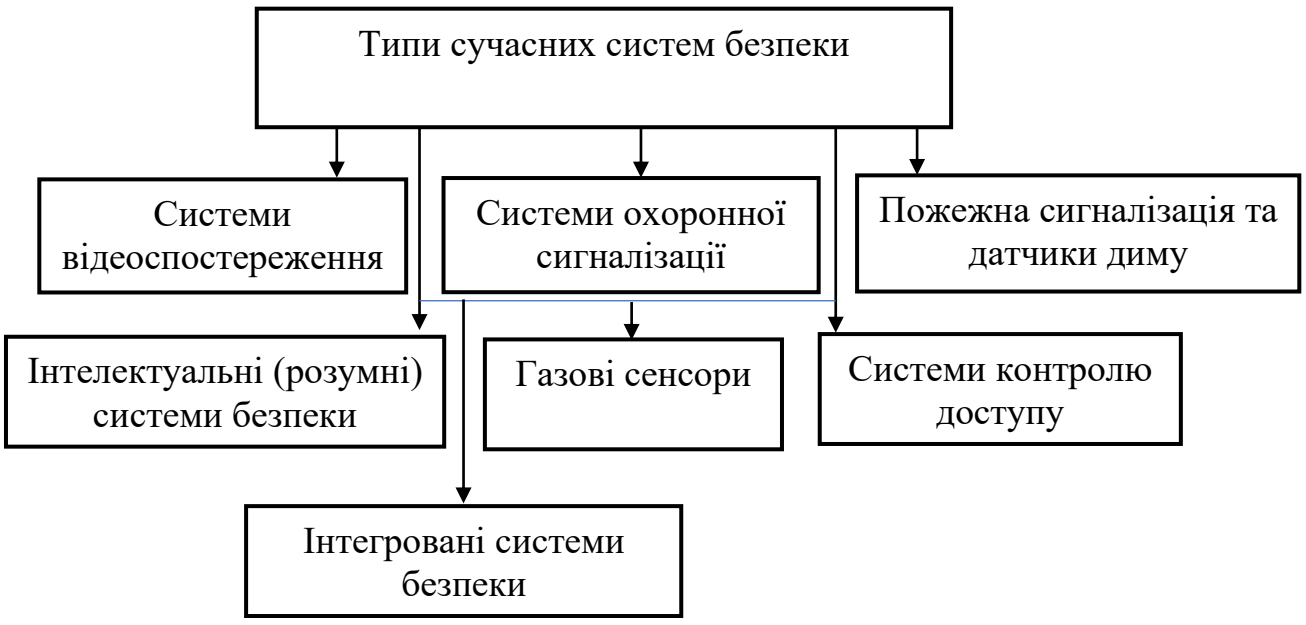


Рисунок 1.1. Типи систем безпеки

Системи відеоспостереження (CCTV) забезпечують візуальний контроль за об'єктом у режимі реального часу. Вони складаються з відеокамер, моніторів та записуючих пристроїв. Сучасні моделі оснащуються функціями розпізнавання обличь, виявлення руху та віддаленого доступу через мережу Інтернет. Відеоспостереження часто інтегрується з іншими системами безпеки для підвищення ефективності охорони.

Системи охоронної сигналізації призначені для виявлення вторгнення в приміщення через двері або вікна. Вони включають датчики руху, магнітні датчики відкриття, інфрачервоні бар’єри та інші сенсори, що реагують на спробу проникнення. У разі виявлення загрози сигналізація активує звукове попередження та/або надсилає сповіщення власнику або охоронній службі.

Пожежна сигналізація та датчики диму дозволяють швидко виявити пожежу або задимлення на ранніх стадіях. Найпоширенішими є оптичні (фотоелектричні) та іонізаційні датчики. У разі фіксації диму або різкого підвищення температури система подає тривожний сигнал або автоматично активує пожежогасіння.

Датчики витоку газу (наприклад, метану, пропану, вуглекислого або чадного газу) використовуються для контролю безпеки у приміщеннях з газовим обладнанням. Вони забезпечують своєчасне попередження про потенційно небезпечні концентрації газів, що дозволяє уникнути вибухів або отруєнь.

Системи контролю доступу (СКД) обмежують доступ до приміщень або об'єктів лише для авторизованих осіб. До таких систем входять: електронні замки, кодові клавіатури, RFID-картки, біометричні сканери (відбитки пальців, розпізнавання обличчя тощо). Вони можуть працювати автономно або бути частиною загальної системи безпеки.

З розвитком технологій «розумного дому» все більшу популярність набирають інтелектуальні системи безпеки. Вони дозволяють дистанційно керувати безпекою об’єкта з мобільного пристрою, автоматизують реакцію на загрози (наприклад, автоматичне увімкнення освітлення, блокування дверей, активація сирен тощо), а також можуть інтегруватися з голосовими помічниками.

Інтегровані системи безпеки – це комплексні рішення, які об’єднують в собі відеоспостереження, пожежну та охоронну сигналізацію, контроль доступу та інші функції. Такі системи забезпечують централізоване керування всіма компонентами безпеки через програмне забезпечення або контролер.

Отже, сучасні системи безпеки характеризуються високим рівнем автоматизації, можливістю інтеграції з іншими технологіями та орієнтацією на швидке реагування. Завдяки цьому вони здатні ефективно забезпечити захист житлових і комерційних приміщень, мінімізуючи ризики для людей і майна. У контексті даної дипломної роботи особливий інтерес становлять компактні та доступні рішення на основі платформ типу Arduino, які дозволяють створювати адаптивні та персоналізовані системи безпеки.

1.1.2 Технології датчиків газу та диму

У сучасних системах безпеки важливу роль відіграють датчики газу та диму, що забезпечують раннє виявлення пожеж, витоків небезпечних газів або підвищення концентрації чадного газу. Вчасна реакція на ці загрози дає змогу уникнути серйозних наслідків для життя, здоров’я людей і матеріальних цінностей. Розглянемо основні типи сенсорів, принципи їх роботи, особливості застосування та приклади реалізації на платформі Arduino.

Існує кілька основних технологій виявлення диму:

– оптичні (фотоелектричні) датчики;

– іонізаційні датчики;

– комбіновані датчики;

– датчики газу;

– інфрачервоні (NDIR) датчики.

Основні технології виявлення диму надано на рис. 1.2.

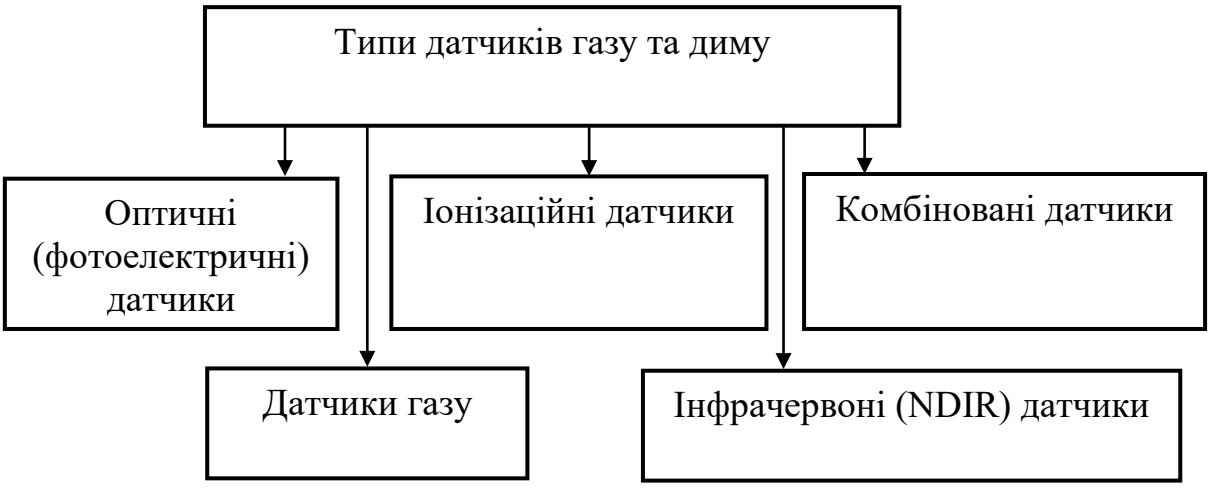


Рисунок 1.2. Основні технології виявлення диму

Оптичні (фотоелектричні) датчики працюють на основі розсіювання світла. Усередині сенсора розташоване джерело світла (зазвичай ІЧ-світлодіод) та фотоприймач, які за нормальних умов не взаємодіють. Коли в камеру потрапляє дим, частинки змінюють напрямок світла, і частина його досягає фотодатчика, що спричиняє спрацьовування тривоги. Їх перевагами є: ефективність при тлінні матеріалів (великі частинки диму); низький рівень хибних спрацювань.

Іонізаційні датчики працюють за рахунок зміни електричної провідності повітря, викликаної наявністю диму. Усередині сенсора є радіоактивний елемент (наприклад, америцій-241), який іонізує повітря. Коли з’являється дим, іонізація порушується, що реєструється як сигнал тривоги. Такі датчики краще реагують на вогонь із полум’ям та чутливі до дрібних частинок. До недоліків можна віднести наступне: можуть викликати суперечності через використання радіоактивних елементів та складніші в утилізації.

Комбіновані датчики поєднують в собі кілька принципів виявлення (оптичний + іонізаційний), що підвищує надійність та точність спрацювання.

Датчики газу призначені для виявлення наявності у повітрі вибухонебезпечних або токсичних газів. Найпоширеніші типи є MQ-серія наприклад, MQ-2, MQ-5, MQ-7, MQ-135. Зображення таких датчиків подано на рис. 1.3.

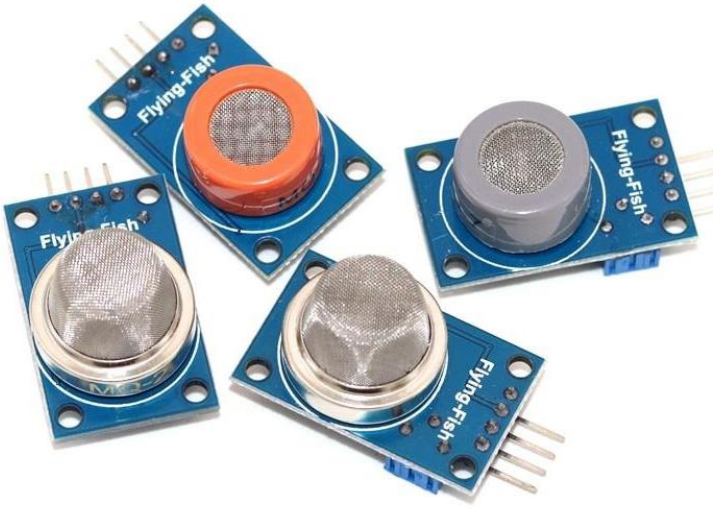


Рисунок 1.3. Плати датчиків газу

Це напівпровідникові датчики на основі чутливого елемента, зазвичай оксиду олова (SnO_2), який змінює свою провідність у присутності певного газу.

Характеристики датчиків MQ-серії наступні:

– MQ-2: виявлення диму, пропану, бутану, метану, водню, алкоголю;

– MQ-5: детекція природного газу, CH4, LPG;

– MQ-7: виявлення чадного газу (CO);

– MQ-135: контроль якості повітря (CO_2, аміак, бензол, дим).

До їх переваг можна віднести наступне: доступність і простота використання; широкий спектр застосування; сумісність з мікроконтролерами (Arduino, ESP32 тощо). До недоліків можна віднести: потрібен час на прогрів (до 1 хв); схильність до хибних спрацювань при зміні температури або вологості.

Інфрачервоні (NDIR) датчики застосовуються для виявлення вуглекислого газу (CO_2). Принцип роботи ґрунтується на поглинанні інфрачервоного випромінювання молекулами газу. Такі датчики забезпечують: високу точність; малу чутливість до інших газів; довгий термін служби. До їх недоліків слід віднести високу вартість і необхідність регулярного калібрування.

Arduino є зручною платформою для побудови прототипів систем безпеки. Для роботи з датчиками диму та газу зазвичай використовуються плати типу Arduino Uno або Arduino Nano, які дозволяють легко зчитувати аналогові або цифрові сигнали з сенсорів та передавати їх на інші модулі або виводити на

дисплей. Наведемо приклад підключення датчиків до мікроконтролера:

– MQ-2 до аналогового входу A0;

– живлення: 5V і GND;

– контроль порогових значень через програмний код.

Також можливе розширення функціоналу за допомогою:

– звукових та світлових сигналізаторів (бузер, світлодіоди);

– модулів зв’язку (GSM, Wi-Fi) для надсилання сповіщень;

– реле для відключення подачі газу або живлення.

Отже, технології датчиків газу та диму постійно вдосконалюються, забезпечуючи високий рівень надійності виявлення загроз. У поєднанні з платформою Arduino вони дозволяють створювати доступні, гнучкі та ефективні системи безпеки, що легко адаптуються під конкретні потреби користувача.

1.1.3 Системи контролю доступу: принципи роботи та класифікація

Системи контролю доступу (СКД) відіграють ключову роль у забезпеченні фізичної безпеки об’єктів, обмежуючи або дозволяючи вхід на територію або до приміщення тільки авторизованим особам. У контексті багаторівневої системи захисту приміщення на основі платформи Arduino, застосування СКД дозволяє реалізувати прості, але ефективні механізми ідентифікації та допуску.

СКД функціонують за принципом «ідентифікація – перевірка – рішення». Це означає, що особа або об’єкт спочатку ідентифікується, потім відбувається перевірка наданих даних із базою дозволених, і система ухвалює рішення — надати або заборонити доступ.

Основні компоненти типової СКД:

– ідентифікаційний пристрій (зчитувач карти, клавіатура, біометричний сенсор, NFC-модуль тощо);

– контролер (центральний елемент, що обробляє інформацію; в нашому випадку – Arduino);

– виконавчі пристрої (електромагнітні замки, реле, дверні приводи);

– програмне забезпечення (або скетч Arduino), яке реалізує логіку доступу.

СКД класифікуються за різними ознаками:

– за типом ідентифікації;

– за масштабністю;

– за рівнем захисту.

Компоненти типової СКД надано на рис. 1.4.

За типом ідентифікації розняють наступні варіанти: кодові (PIN-код); Карточні (RFID/NFC); біометричні (відбитки пальців, обличчя, райдужка ока); мобільні (Bluetooth, Wi-Fi, GSM).

Кодові (PIN-код) методи є найпростіший типом і реалізується за допомогою клавіатури. Цей метод дешевий і простий. Проте недоліком є те, що код досить легко перехопити або вгадати.

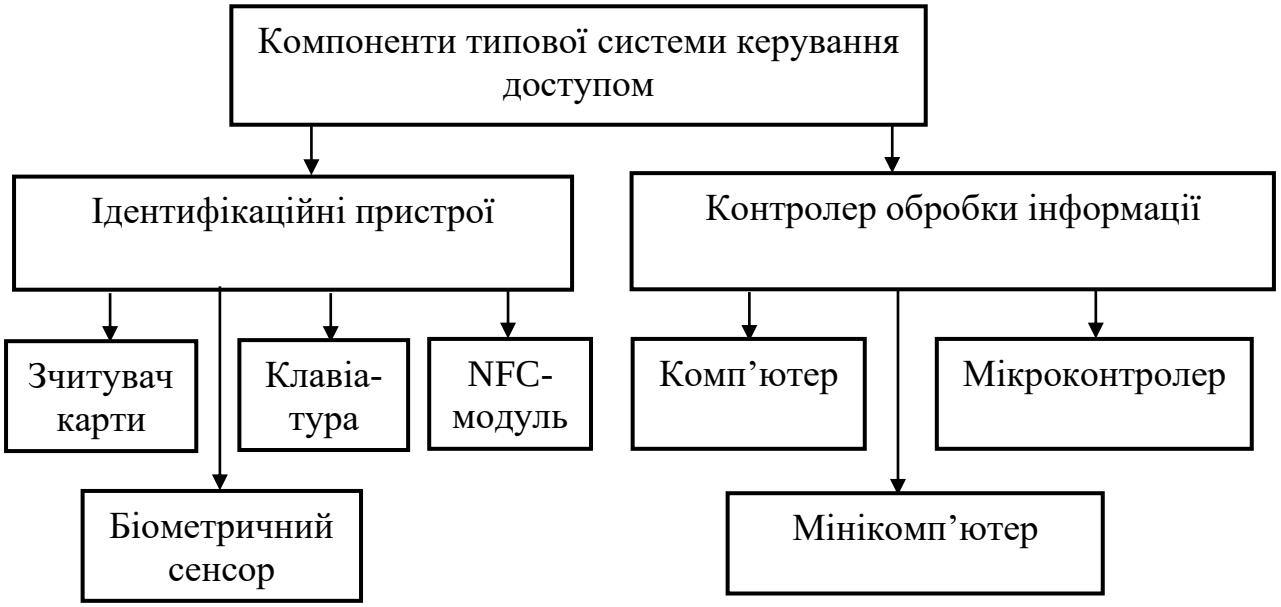


Рисунок 1.4. Основні компоненти типової СКД

Карточні (RFID/NFC) використовують безконтактні ідентифікатори (брелоки, карти). Вони популярні у системах на Arduino з RFID-модулями (наприклад, RC522). Їх перевагами є: зручність, широка підтримка. До недоліків можна віднести клонованість дешевих міток.

Зображення радіочастотних RFID/NFC ідентифікаторів надано на рис. 1.5.

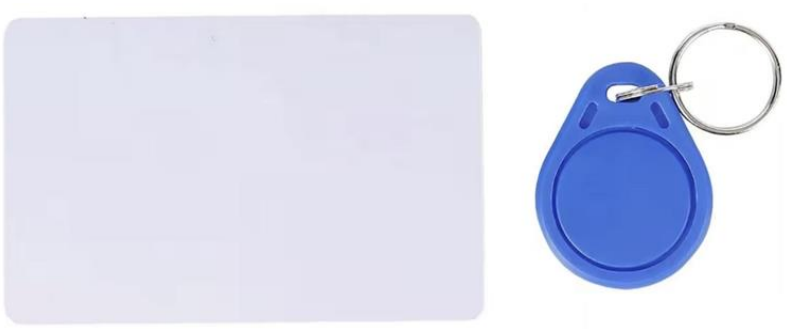


Рисунок 1.5. Зображення радіочастотних RFID/NFC ідентифікаторів

Біометричні (відбитки пальців, обличчя, райдужка ока) реалізуються за допомогою спеціалізованих модулів (наприклад, R305, AS608). Такі метод забезпечують високу надійність і складність підробки. Проте ці методи мають вищу вартість та їх складніше підключити.

Приклад зображення сканера відбитків пальців ZKTeco FR1300 надано на рис. 1.6. Також цей сканер має клавіатуру для додаткової ідентифікації суб'єкта.

На рис 1.7 надано зображення пристрою RFID зчитувач DHI-ASR1102A (V2).

Рисунок 1.6. Сканер відбитків пальців ZKTeco FR1300

Мобільні (Bluetooth, Wi-Fi, GSM) методи ідентифікації забезпечують доступ за допомогою мобільних пристроїв. Їх можна реалізувати з використанням модулів HC-05 (Bluetooth), ESP8266 (Wi-Fi).

Рисунок 1.7. RFID зчитувач DHI-ASR1102A (V2)

За масштабністю СКД розрізняють автономні та мережеві. Автономні СКД працюють без зовнішнього сервера або комп'ютера (наприклад, Arduino з локальною базою користувачів). Мережеві СКД з'єднані у мережу з можливістю централізованого управління (наприклад, з ESP32 і сервером).

За рівнем захисту СКД розрізняють базовій, середній та високий рівень. Базові СКД мають одну точку контролю та використовують прості механізми (Arduino + RFID). Середній рівень захисту СКД реалізується за допомогою багаторівневої авторизації, реєстрації подій, зберігання логів. Високий рівень захисту використовує шифрування даних, багатофакторну автентифікацію, інтеграція з системами відеоспостереження та сигналізації.

Розглянемо приклади реалізації СКД на базі Arduino.

RFID-контроль доступу потребує: використання модуля RC522 та карт MIFARE; зчитування UID картки та порівняння з "білим списком"; відкриття замка за допомогою реле.

Кодовий доступ вимагає наявність: клавіатуру 4x4 + LCD-дисплей; введення PIN-коду, перевірка правильності.

Біометричний доступ потребує наявність: модуля відбитків пальців R305; ідентифікації користувача за шаблоном у пам'яті модуля.

Мобільний контроль можливий через Bluetooth з додатком на телефоні та надсилання команд відкриття замка з мобільного пристрою.

Отже, системи контролю доступу є невід'ємною складовою сучасних

систем безпеки. Завдяки гнучкості та доступності платформи Arduino, можливе створення простих, надійних і персоналізованих рішень контролю доступу для квартир, офісів і промислових об’єктів. Правильний вибір типу ідентифікації та реалізація логіки роботи дозволяє досягти високого рівня захищеності з мінімальними витратами.

1.1.4 Оцінка ефективності існуючих рішень

На сучасному ринку існує велика кількість систем безпеки, що поєднують в собі функції виявлення небезпечних факторів (дим, газ, рух) та контролю доступу. Для оцінки ефективності таких рішень слід враховувати кілька ключових критеріїв: надійність, масштабованість, вартість, енергоефективність, простота інтеграції, а також адаптивність до конкретних умов експлуатації (житло, офіс, склад тощо). В табл. 1.1 надано порівняльний аналіз типових систем.

Проведемо аналіз недоліків існуючих систем. Комерційні системи мають високу ціну обладнання. Також вони часто потребують підписки або зв’язку з центральним сервером. Для них характерно обмежені можливості кастомізації та залежність від виробника (закрите ПЗ та протоколи).

Саморобні системи на Arduino мають наступні особливості:

– потребують навичок програмування та електроніки;

– відсутність готового інтерфейсу для користувача (потрібно розробляти самостійно);

– можливі проблеми з електроживленням, помилки у коді.

Таблиця 1.1. Порівняльний аналіз типових систем

Характеристика	Комерційні рішення (Ajax, Jablotron)	DIY-рішення на базі Arduino
Надійність	Висока, сертифіковані	Залежить від реалізації
Вартість	Висока	Низька/помірна
Можливість модифікації	Обмежена	Висока

продовження таблиці 1.1.

Зручність налаштування	Інтуїтивна, через мобільні застосунки	Потребує програмування
Підтримка кількох типів сенсорів	Зазвичай вбудована	Гнучка, ручне налаштування
Контроль доступу	NFC, брелоки, мобільні додатки	RFID, клавіатури, Bluetooth
Підтримка автономної роботи	Так (з резервним живленням)	Так, за умови налаштування

Можна зазначити наступні переваги Arduino-рішень у побудові багаторівневого захисту СКД:

– гнучкість і розширюваність: можливість підключення будь-якої кількості сенсорів та модулів;

– інтеграція з інтернетом речей (IoT): через модулі ESP8266, ESP32;

– локальна обробка даних: не вимагає зовнішнього серверу, що підвищує безпеку;

– низька вартість компонентів;

– швидке прототипування та тестування.

Отже, оцінка існуючих рішень демонструє, що для побудови ефективної, доступної та адаптивної системи захисту приміщення найдоцільнішим підходом є використання платформи Arduino. Вона забезпечує належний рівень функціональності при мінімальних витратах і дозволяє реалізувати індивідуальну багаторівневу архітектуру безпеки, яка може включати в себе:

– сенсори диму й газу;

– засоби контролю доступу (RFID, PIN-код, Bluetooth);

– систему оповіщення;

– можливість зв’язку з мобільним додатком або сервером.

Таким чином, розробка такої системи на базі Arduino є перспективним напрямком, особливо для малих об'єктів, приватних помешкань або стартапів у сфері охоронних технологій.

1.1.5 Визначення основних вимог до багаторівневої системи захисту

Перед початком проєктування багаторівневої системи захисту приміщення важливо визначити перелік основних функціональних, технічних та експлуатаційних вимог, яким вона має відповідати. Це дозволить сформувати чітку архітектуру рішення, обрати відповідні компоненти, уникнути надмірної складності та забезпечити ефективну і стабільну роботу системи.

Функціональні вимоги потребують:

1) виявлення загроз природного походження;

2) контроль фізичного доступу;

3) оповіщення про загрози;

4) багаторівнева логіка захисту.

Функціональні вимоги до багаторівневої системи захисту приміщення надано на рис. 1.8.

Виявлення загроз природного походження потребує: реагування на витік побутового газу (природний газ, метан); детекція диму, пов’язаного із займанням.

Контроль фізичного доступу вимагає: ідентифікацію користувачів за RFID-картками, PIN-кодом або мобільним пристроєм; ведення журналу доступу (опційно – за допомогою SD-карти або Wi-Fi).

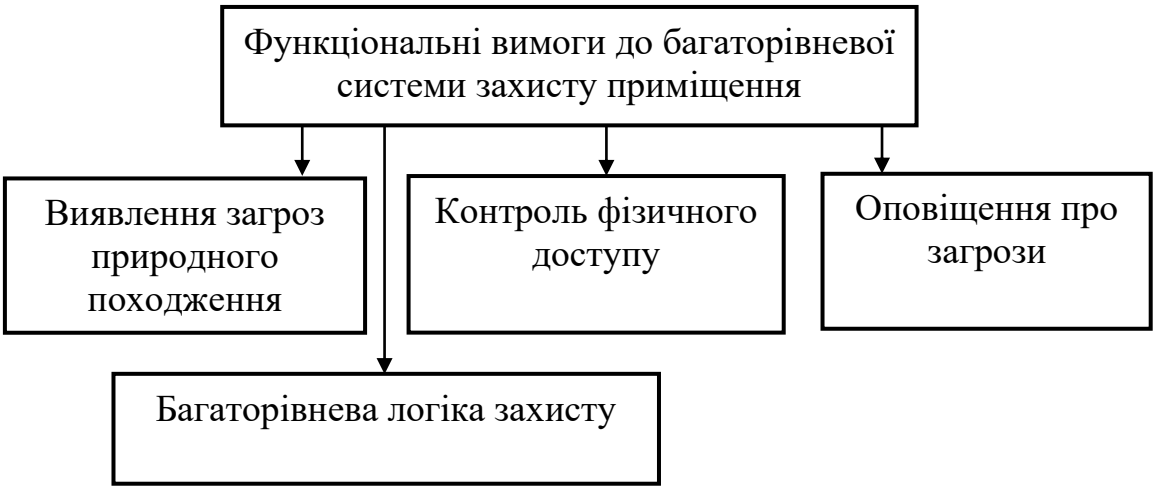


Рисунок 1.8. Функціональні вимоги до багаторівневої системи захисту приміщення

Оповіщення про загрози вимагає: звукову та світлову сигналізацію при

спрацюванні сенсорів; віддалене повідомлення (через GSM, Wi-Fi або Bluetooth).

Багаторівнева логіка захисту потребує: об'єднання кількох способів перевірки (наприклад, газ + рух + доступ); можливість задавати різні рівні тривоги.

Технічні вимоги вимагає наявність:

1) платформи керування;

2) сенсорів;

3) живлення;

4) захист даних.

Платформа керування потребує використання: Arduino Uno/Nano/Mega або ESP32 для розширених можливостей; мінімум 6 вхідних/вихідних портів для підключення сенсорів, замків, сигналізаторів.

Сенсори побудовані на використання: датчиків диму (наприклад, MQ-2, MQ-135); датчиків газу (наприклад, MQ-5 або MQ-9); реле або електромагнітний замок для блокування доступу; RFID-модуля (RC522), клавіатури або Bluetooth-модуля.

Живлення забезпечує можливість автономної роботи з джерела резервного живлення (акумулятор або power bank) та захист від перепадів напруги.

Захист даних потребує використання: базова шифрування ідентифікаторів доступу (хешування паролів); забезпечення стійкості до збоїв (watchdog, перезапуск системи).

Експлуатаційні вимоги вимагає:

1) надійність і безвідмовність;

2) простота користування;

3) можливість оновлення.

Надійність і безвідмовність орієнтується на: можливість роботи в автономному режимі без підключення до ПК; самодіагностику основних вузлів (наприклад, перевірка наявності сенсорів при запуску).

Простота користування потребує наявність інтуїтивного інтерфейсу взаємодії з користувачем (екран, індикатори) та можливість додавання нових

RFID-карт або зміни PIN-кодів.

Можливість оновлення орієнтується на перепрограмування через USB або Wi-Fi та розширення кількості модулів без повної реконструкції системи.

Узагальнена структура багаторівневої системи має наступні рівні:

1) рівень 1: виявлення небезпеки (дим, газ);

2) рівень 2: контроль фізичного доступу (ідентифікація користувача);

3) рівень 3: активна реакція (блокування, сигналізація, повідомлення).

Отже, визначення чітких вимог дозволяє закласти основу для розробки ефективної багаторівневої системи безпеки. Система на базі Arduino повинна бути модульною, гнучкою до налаштувань, енергоефективною та надійною в роботі. Такий підхід дозволить забезпечити охорону приміщень з мінімальними витратами та високим рівнем адаптації до змін у середовищі чи вимогах користувача.

1.2 Розробка багаторівневої системи захисту приміщення на платформі Arduino

1.2.1 Архітектура системи та її компоненти

Багаторівнева система захисту приміщення, побудована на основі платформи Arduino, має модульну архітектуру, яка дозволяє легко масштабувати, модернізувати та адаптувати систему до конкретних потреб користувача. У цій підсистемі інтегруються три основні функціональні напрями: виявлення загроз (газ/дим), контроль доступу, та система оповіщення. Загальна архітектура системи умовно поділяється на такі рівні: рівень сенсорів; рівень обробки даних; рівень взаємодії; рівень управління/реакції.

Рівень сенсорів призначений для виявлення небезпечних факторів (дим, газ) та спроб несанкціонованого доступу. Рівень обробки даних використовує центральний контролер (Arduino), який обробляє сигнали з сенсорів, аналізує логіку подій та приймає рішення. Рівень взаємодії реалізується за допомогою модулів ідентифікації (RFID, клавіатура) сигналізації (бузер, світлодіоди, GSM). Рівень управління/реакції забезпечує активацію сирени, блокування дверей та

надсилання повідомлення користувачу. В табл. 1.2 представлено основні компоненти багаторівневої системи захисту приміщення.

Таблиця 1.2. Компоненти багаторівневої системи захисту приміщення

Компонент	**Призначення**
Arduino Uno / Mega	Головний контролер для обробки сигналів та управління логікою системи.
Датчик газу MQ-5 / MQ-9	Виявлення витоку побутового або чадного газу.
Датчик диму MQ-2 / MQ-135	Реєстрація наявності диму у приміщенні.
Модуль RFID RC522	Ідентифікація користувача для контролю доступу.
Клавіатура 4x4	Альтернативний метод автентифікації (введення PIN-коду).
Бузер / сирена	Звукова сигналізація при виявленні загрози.
Світлодіоди (LED)	Візуальна індикація станів системи (норма/тривога/помилка).
GSM-модуль (SIM800L)	Надсилання SMS-повідомлень у випадку тривоги (опціонально).
Електромагнітний замок	Блокування доступу до приміщення.
Блок живлення / АКБ	Живлення системи; резервне живлення у разі відключення електроенергії.

Схема взаємодії компонентів багаторівневої системи захисту приміщення надано на рис. 1.9.

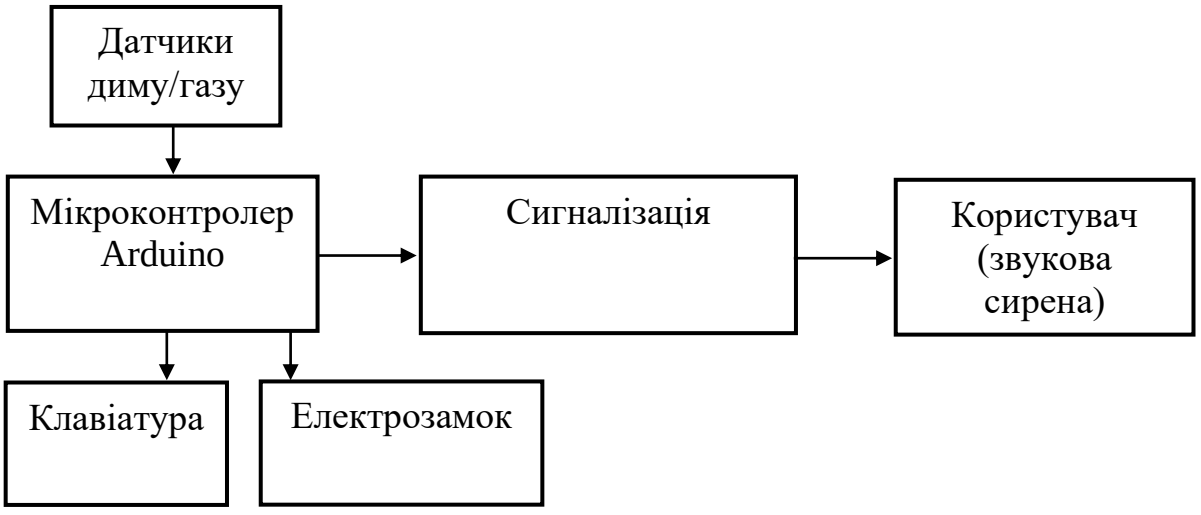


Рисунок 1.9. Схема взаємодії компонентів багаторівневої системи захисту приміщення

Можна відзначити наступні переваги такої архітектури: модульність; гнучкість; економічність; надійність; інформативність. Модульність дозволяє легко додавати або замінювати компоненти. Гнучкість забезпечує підтримку кількох методів ідентифікації. Економічність обгрунтовується: використанням недорогих модулів. Надійність забезпечується за рахунок автономної роботи, відсутності залежності від хмарних сервісів. Інформативність характеризує наявність візуальної та звукової індикації, а також SMS-повідомлень.

Отже, архітектура розробленої багаторівневої системи забезпечує високий рівень адаптивності, безпеки та автономності, що є важливими факторами для ефективного захисту приміщень. Завдяки використанню платформи Arduino та сумісних модулів досягається баланс між функціональністю, вартістю та простотою реалізації. У наступному розділі буде детально описано процес реалізації кожного з компонентів системи.

1.2.2 Вибір датчиків газу та диму для платформи Arduino

Однією з ключових задач при розробці багаторівневої системи захисту приміщення є вибір відповідних сенсорів для виявлення диму та газу. Вони мають бути сумісні з платформою Arduino, забезпечувати достатню чутливість, стабільність роботи, а також бути доступними за ціною для побудови прототипу або реального пристрою.

При виборі сенсорів газу та диму враховуються наступні технічні параметри: тип виявлюваних речовин (метан, пропан, чадний газ, дим тощо); чутливість та точність вимірювання; час спрацювання та відновлення; робоча напруга та сумісність із Arduino; температурний діапазон роботи; споживання енергії; наявність аналогового або цифрового виходу.

Розглянемо популярні моделі датчиків для мікроконтролера Arduino. Датчик газу MQ-2 забезпечує виявлення диму, пропану, бутану, метану, алкоголю. Цей датчик аналоговий тим виходу. Його перевагами є: універсальність, доступність та широке використання в аматорських проєктах. До недоліків можна віднести: потребує калібрування, чутливий до вологості.

Датчик газу MQ-5 призначений для виявлення метану, природного газу, зрідженого газу. Має аналоговий тип виходу. Його перевагою є добра чутливість до побутових газів. Недоліком цього датчика є тривалий час прогріву перед роботою (~20 сек).

Датчик газу MQ-9 призначений для виявлення чадного газу (CO), метану, пропану. Має аналоговий тип виходу. Перевагою є: хороша стабільність, придатність для систем безпеки. Цей датчик може бути використаний як для CO, так і для легких вуглеводнів.

Датчик газу MQ-135 призначений для виявлення аміаку, бензолу, дим, CO_2. Його перевагою є широкий спектр виявлюваних речовин. Недоліком є менш точний процес виявлення для CO у порівнянні з MQ-9.

Таблиця 1.3. Порівняльна таблиця датчиків газу

Модель	**Виявлювані речовини**	**Підходить для диму**	**Підходить для газу**	**Тип виходу**	**Сумісність з Arduino**
MQ-2	Дим, пропан, метан, LPG	Так	Так	Аналоговий	Висока
MQ-5	Природний газ, LPG	Ні	Так	Аналоговий	Висока
MQ-9	CO, метан, пропан	Ні	Так	Аналоговий	Висока
MQ-135	CO_2, дим, аміак, бензол	Так	Так	Аналоговий	Висока

Зважаючи на вимоги багаторівневої системи, доцільно використовувати комбінацію з двох сенсорів: MQ-2 і MQ-5 або MQ-9. Датчик MQ-2 буде призначеним для виявлення диму та ряду легкозаймистих газів. Датчики MQ-5 або MQ-9 буде використовуватися як спеціалізований сенсор газу (в залежності від типу приміщення та ймовірної загрози витоку).

Таке поєднання дозволить підвищити надійність та точність реагування системи, а також зменшити ймовірність хибних спрацювань за рахунок перехресного контролю.

Отже, обрані сенсори MQ-2 та MQ-9 (або MQ-5) забезпечують надійне та доступне рішення для виявлення загроз, пов’язаних із димом і газом. Вони повністю сумісні з Arduino, мають просте підключення та налаштування, що робить їх ідеальними для використання у прототипах систем безпеки. У наступному підрозділі буде розглянуто принцип роботи та вибір системи контролю доступу.

1.3 Розробка системи контролю доступу на основі Arduino

Система контролю доступу є одним із ключових елементів багаторівневої охоронної системи. Вона відповідає за ідентифікацію та авторизацію користувача, а також за блокування або розблокування доступу до приміщення. У цьому підрозділі розглядається реалізація такої системи на основі платформи Arduino з використанням RFID-модуля та клавіатури для введення PIN-коду.

Система контролю доступу працює за наступним алгоритмом:

1) Користувач прикладає RFID-картку або вводить PIN-код через клавіатуру;

2) Arduino зчитує дані з модуля та перевіряє їх на відповідність збереженим у пам’яті кодам;

3) У разі успішної ідентифікації:

– увімкнення зеленої індикації (LED).

– активація реле або транзистора, що керує електромагнітним замком.

– надсилання інформації про вхід до журналу подій (опціонально).

4) у разі невдалої спроби:

– активація червоної індикації;

– запуск звукової сигналізації після кількох невдалих спроб;

– можливість надсилання SMS-попередження через GSM-модуль.

В табл. 1.4 надано основні апаратні компоненти система контролю доступу.

Програма реалізується на мові C/C++ з використанням Arduino IDE. Для взаємодії з RFID-модулем застосовується бібліотека MFRC522, а для клавіатури – Keypad.h.

Ключові етапи в коді наступні:

- ініціалізація компонентів;
- зчитування UID картки;
- порівняння з масивом авторизованих UID;
- зчитування коду з клавіатури та перевірка відповідності;
- керування замком та індикацією.

Таблиця 1.4. Основні апаратні компоненти система контролю доступу

Компонент	**Призначення**
Arduino Uno/Mega	Центр обробки введених даних та керування доступом.
RFID-модуль RC522	Зчитування UID RFID-карт для авторизації.
Клавіатура 4x4 Keypad	Введення PIN-коду як альтернативного методу доступу.
Серводвигун / реле	Активація електрозамка при авторизації.
Електромагнітний замок	Блокування/розблокування дверей.
Світлодіоди (LED)	Візуальна індикація результату авторизації.
Бузер	Звукова сигналізація про неправильний вхід або помилку.

Алгоритм авторизації (блок-схема) системи контролю доступу надано на рис. 1.10.

Для підвищення безпеки можливі такі доповнення:

– дворівнева авторизація: поєднання RFID і PIN-коду;

– ведення журналу подій: збереження UID та часу спроб входу4

– GSM-оповіщення: надсилання повідомлення власнику при підозрілих діях;

– Wi-Fi підключення: моніторинг через мобільний додаток або веб-інтерфейс.

Таким чином, система контролю доступу, реалізована на базі Arduino, забезпечує ефективну перевірку прав доступу до приміщення. Використання RFID та клавіатури робить її гнучкою, а додаткові засоби безпеки – стійкою до несанкціонованих дій. У наступному підрозділі буде розглянуто реалізацію підсистеми виявлення загроз та сигналізації.

1.3.1 Інтеграція компонентів у єдину систему на платформі Arduino

Інтеграція компонентів в єдину багаторівневу систему безпеки на базі Arduino передбачає поєднання різних підсистем – виявлення загроз (газ, дим), контролю доступу, сигналізації та централізованого керування — в один цілісний комплекс, що забезпечує автономну та взаємозалежну роботу усіх елементів.

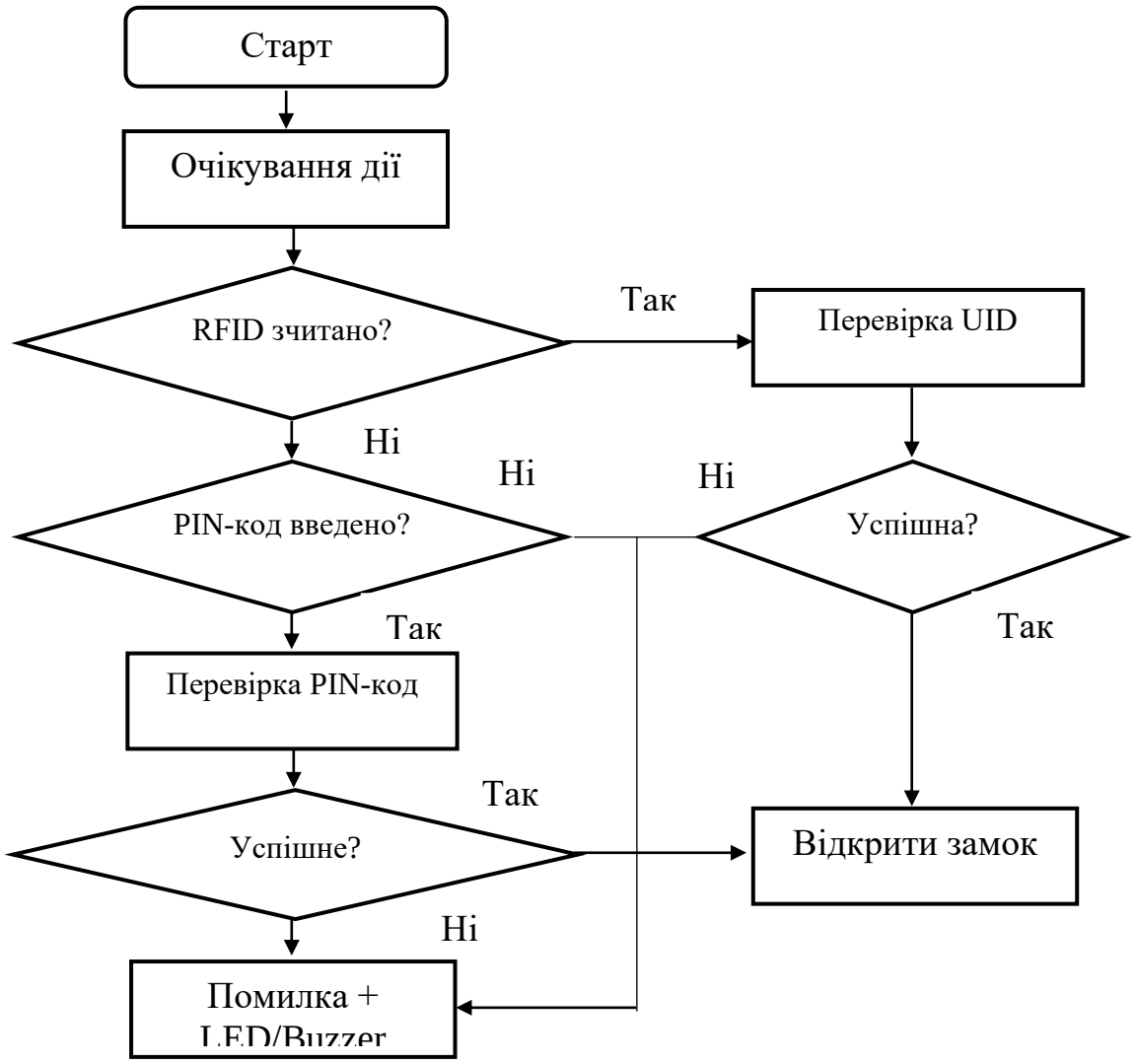


Рисунок 1.10 – Алгоритм авторизації системи контролю доступу

До складу інтегрованої системи входять:

– підсистема – моніторингу середовища: газові та димові датчики;

– підсистема доступу: RFID-модуль, клавіатура, сервопривід/електрозамок;

– підсистема індикації та сигналізації: LED, бузер;

– контролер: Arduino Uno або Mega як центр управління;

– модулі зв’язку (опціонально): GSM, Wi-Fi (ESP8266) для віддаленого сповіщення.

Всі ці елементи взаємодіють між собою через Arduino, де реалізовано логіку прийняття рішень. Електричне з'єднання компонентів схеми системи доступу надано в табл. 1.5.

Таблиця 1.5. Електричне з'єднання компонентів схеми системи доступу

Компонент	**Arduino Pin**
MQ-2 (газ/дим)	A0
RFID-модуль RC522	SPI (10, 11, 12, 13)
Клавіатура 4x4	Цифрові 2–9
Серводвигун / реле	Цифровий 3
LED (зелений/червоний)	Цифрові 4, 5
Бузер	Цифровий 6
GSM-модуль (опціонально)	TX/RX або Serial1 (Mega)
LCD-дисплей (опціонально)	I2C (A4 SDA, A5 SCL)

При використанні великої кількості компонентів рекомендується Arduino Mega з розширеним числом входів/виходів.

Логіка роботи інтегрованої системи включає такі етапи:

1) моніторинг стану датчиків (газ, дим);

2) у разі перевищення порогу – активація сигналізації та блокування доступу;

3) очікування дій користувача: зчитування RFID або введення PIN-коду;

4) авторизація: при успіху – відкриття замка; при помилці – сигнал тривоги;

5) реєстрація подій у журналі (опційно);

6) відправлення SMS або повідомлення через Wi-Fi при тривозі (опційно);

7) виведення стану системи на дисплей (опціонально).

Програмне забезпечення повинно враховувати пріоритети подій:

– події тривоги (дим/газ) мають найвищий пріоритет і переривають доступ;

– контроль доступу активний лише у безпечному стані;

– періодичне опитування датчиків реалізовано через таймери або millis();

– використання структурованого коду, функцій та станів (state machine) забезпечує стабільну роботу.

Для забезпечення надійності інтегрованої системи варто врахувати:

– захист живлення (додаткові стабілізатори та конденсатори);

– обробка помилок (наприклад, втрати сигналу з RFID);

– тестування сценаріїв надзвичайних ситуацій (одночасна тривога і доступ);

– використання EEPROM для збереження авторизованих UID/PIN-кодів.

Отже, інтеграція всіх підсистем на базі Arduino дозволяє створити функціональну, автономну та гнучку систему захисту приміщення. Така система здатна реагувати на загрози в режимі реального часу, обмежувати доступ та забезпечувати високий рівень захисту. У наступному розділі буде проведено тестування, аналіз ефективності та оцінка надійності розробленого рішення.

1.3.2 Алгоритм роботи багаторівневої системи на основі Arduino

Алгоритм функціонування багаторівневої системи захисту приміщення на базі Arduino є ключовим елементом, що забезпечує злагоджену роботу усіх компонентів: датчиків газу, диму, засобів контролю доступу та сигналізації. Він реалізує послідовну перевірку умов, реагування на події та виконання відповідних дій згідно з обраною логікою безпеки.

Основні принципи побудови алгоритму передбачає:

– постійний моніторинг параметрів навколишнього середовища (газ, дим);

– реагування на перевищення порогових значень;

– контроль авторизації користувачів (RFID або клавіатура);

– визначення пріоритетів у разі кількох одночасних подій;

– візуальна та звукова сигналізація;

– можливість відправки повідомлення (опціонально);

– захист від несанкціонованого доступу.

Таким чином, розроблений алгоритм забезпечує поетапну обробку інформації від сенсорів і пристроїв введення, гарантує пріоритетність безпеки у разі виявлення небезпеки та дозволяє гнучко реалізувати різні рівні доступу. Така структура забезпечує ефективне та безпечне функціонування системи в умовах реального використання. У наступному розділі буде проведено тестування та аналіз ефективності розробленої системи.

1.4 Розробка багаторівневої системи захисту приміщення

1.4.1 Завдання на розробку системи захисту приміщення з датчиком газу, диму та контролем доступу

Завдання на розробку полягає в наступному: розробити макет багаторівневої системи захисту приміщення на платформі Arduino, що дозволяє здійснювати контроль доступу за допомогою клавіатури, відкривати двері сервоприводом та виявляти наявність диму і газу за допомогою відповідних сенсорів.

Вимоги до функціональних можливостей:

1) контроль доступу за допомогою PIN-коду, введеного через матричну клавіатуру;

2) привід дверей: відкривання дверей сервоприводом (SG90 або аналогічним) після успішної авторизації;

3) виявлення загроз: диму; горючого газу;

4) аварійне сповіщення (звукове або вивід на екран);

5) індикація стану системи за допомогою світлодіодів.

Апаратним компонентами для проєкту є:

1) плата керування на основі мікроконтролера Arduino Uno;

2) клавіатура: 4×4 або 3×4 матрична клавіатура;

3) сервопривід: SG90 або аналогічний;

4) сенсори датчик диму (наприклад, аналог MQ-2); датчик газу (може бути симуляція тим самим MQ-2 у Tinkercad);

5) світлодіоди для індикації стану (зелений – доступ дозволено, червоний – заборонено, жовтий – небезпека);

6) звуковий сигналізатор: buzzer (опційно);

7) дисплей (опційно): LCD1602 або OLED – для виведення повідомлень.

Програмне забезпечення передбачає наступні кроки:

1) розробка коду в середовищі Arduino IDE;

2) логіка роботи полягає в наступному: обробка введення PIN-коду; перевірка значень з датчиків;

3) керування сервоприводом та сигналізацією;

4) коментарі в коді для пояснення функціональності;

Пропонуються наступні етапи виконання:

1) аналіз вимог і вибір компонентів;

2) проєктування логіки системи;

3) моделювання схеми у Tinkercad Circuits;

4) написання програмного забезпечення;

Тестування роботи системи в різних режимах (нормальний, тривожний, спроба несанкціонованого доступу);

Оформлення звітної документації.

Вимоги до ефективності полягають в наступному:

1) час реакції системи: не більше 1 секунди з моменту введення правильного PIN-коду або виявлення загрози;

2) надійність: стійка робота компонентів при імітації подій;

3) просте та інтуїтивне керування через клавіатуру.

https://www.tinkercad.com/things/hPyGtbQwOFn/editel?returnTo=%2Fdashboard%2Fdesigns%2F3d&sharecode=o8lsO9HX4dnCiI3_oM5HPyBfEfygGslnB4BX5tj3ikM

1.4.2 Апаратні компоненти проєкту

Для реалізації багаторівневої системи захисту приміщення з контролем доступу, виявленням газу, сигналізацією та світловою індикацією, використано такі апаратні компоненти:

1) мікроконтролер Arduino Uno R3;

2) клавіатура 4×4;

3) сервопривод SG90;

4) газовий сенсор типу MQ;

5) пасивний п'єзодинамік;

6) світлодіоди для індикації стану;

7) блок живлення або USB-кабель.

Мікроконтролер Arduino Uno R3 – це основний контролер, який керує усіма підключеними елементами, обробляє дані з клавіатури та сенсорів, приймає рішення про доступ і керує виконавчими пристроями (сервопривод, сигналізація, світлодіоди).

Зовнішній вид плати мікроконтролер Arduino Uno R3 надано на рис. 1.11.

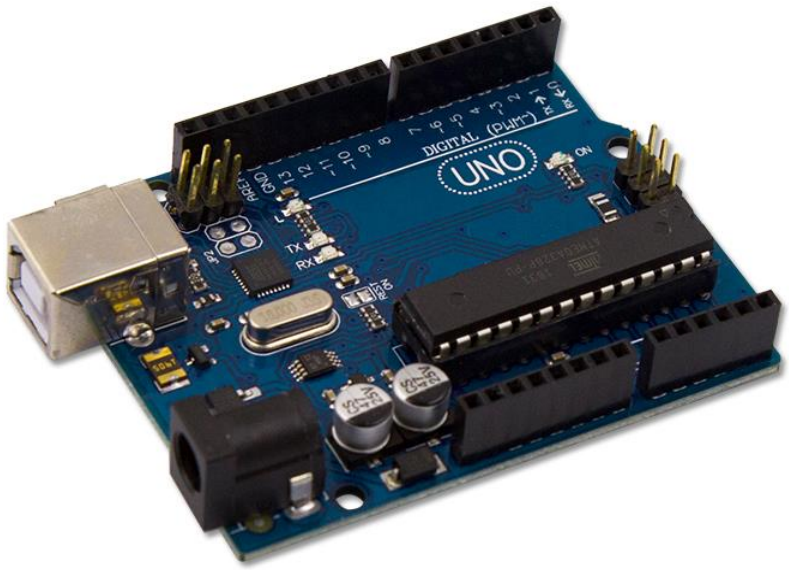


Рисунок 1.11. Зовнішній вигляд плати мікроконтролера Arduino Uno R3

Клавіатура 4×4 (Keypad 4×4) Використовується для введення паролю доступу. Клавіатура підключена до цифрових пінів D2–D9 та дозволяє реалізувати механізм авторизації користувача. Зовнішній вигляд клавіатури 4×4

надано на рис 1.12.

Рисунок 1.12. Зовнішній вигляд клавіатури 4×4

Сервопривод SG90 застосовується як імітація механізму відкривання/закривання дверей. Підключений до цифрового піна D10. Керується за допомогою PWM-сигналу. Поворот сервопривода виконується при правильному введенні пароля. Зовнішній вигляд сервоприводу SG90 надано на рис 1.13.

Рисунок 1.13. Зовнішній вигляд сервоприводу SG90

Газовий сенсор типу MQ (Gas Sensor) підключається до аналогового входу A0 та живлення. Виявляє наявність горючих газів у повітрі (наприклад, метану,

пропану). При перевищенні заданого порогу (наприклад, значення >600) активується тривожний сигнал та світлодіодна індикація. Цей пристрій має шість дротів. Підключіть нагрівач, підключивши +5 В до H1 або H2, а заземлення до іншого. Опір між A та B змінюється залежно від кількості виявленого газу. Підключіть один кінець вашої схеми виявлення до A1 або A2, а інший до B1 або B2.

Принцип роботи полягає в наступному: виберіть пристрій під час моделювання, щоб відобразити хмару, що представляє концентрацію газу. Пересуньте ціль, щоб змінити рівень змодельованого газу. Перетягніть схему стартера нижче у свій проект, щоб отримати робочий приклад використання цієї деталі. На рис. 1.14 надано зовнішній вигляд газового сенсору MQ135.

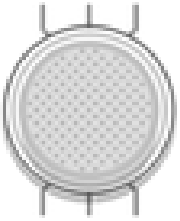


Рисунок 1.14. Зовнішній вигляд газового сенсору MQ135

На рис. 1.15 представлено призначення пінів газового сенсору MQ135.

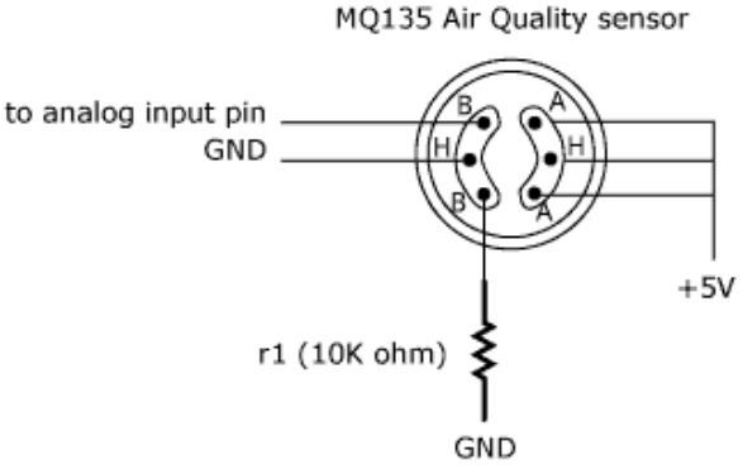


Рисунок 1.15. Призначення пінів газового сенсору MQ135

Програмний код газовий сенсор MQ135 виглядає наступним чином:

```
int sensorValue;
```

```
void setup()
{
  Serial.begin(9600);      // sets the serial port to 9600
}

void loop()
{
  sensorValue = analogRead(0);       // read analog input pin 0
  Serial.println(sensorValue, DEC);  // prints the value read
  delay(100);                        // wait 100ms for next reading
}
```

Пасивний п'єзодинамік (Buzzer) підключається до піна D11. Використовується для генерування звукових сигналів при тривозі або неправильному введенні паролю. Генерує звук за допомогою команди tone(). На рис. 1.16 представлено зовнішній вигляд пасивного п'єзодинаміка.

Рисунок 1.16. Зовнішній вигляд пасивного п'єзодинаміка

Світлодіоди призначені для індикації стану. Червоний світлодіод (індикація тривоги через газ) – підключений до піна D13. Зелений світлодіод (індикація успішного доступу) – підключений до піна D12. Кожен світлодіод з’єднаний через резистор номіналом 220 Ом. На рис. 1.17 представлено зовнішній вигляд світлодіодів. Зовнішній вигляд резистора надано на рис. 1.18.

Рисунок 1.17. Зовнішній вигляд світлодіодів

Рисунок 1.18. Зовнішній вигляд резистора

Блок живлення для плати Arduino призначений для перетворення напруги 220В в напругу постійного струпу 9 вольт (струм 1 ампер). Для подачі живлення на Arduino Uno та всі компоненти проєкту. На рис. 1.19 представлено зовнішній вигляд блоку перетворення напруги 220В в напругу постійного струпу 9 вольт.

Рисунок 1.19. Зовнішній вигляд блоку перетворення напруги 220В в напругу постійного струпу 9 вольт

USB-кабель призначений для підключення плати Arduino до комп’ютера для задачі програмування, роботи та подачі живлення 5 вольт. На рис. 1.20 представлено зовнішній вигляд USB-кабелю.

Рисунок 1.20. Зовнішній вигляд USB-кабелю

Цей набір компонентів дозволяє побудувати просту, але функціональну систему контролю доступу з вбудованими функціями виявлення газу, звукового та світлового оповіщення, що може бути використана для навчальних або демонстраційних цілей.

1.5 Опис роботи схеми і підключення елементів

На рис. 1.21 представлена схема електрична принципіальна системи захисту приміщення з датчиком газу, диму та контролем доступу Загальний принцип роботи системи полягає в наступному. Розроблена система захисту приміщення виконує такі основні функції:

1) очікує введення паролю з клавіатури;

2) у разі правильного паролю відкриває двері (керує сервоприводом) та вмикає зелений індикатор доступу;

3) у разі неправильного паролю або при виявленні газу активує звукову сигналізацію;

4) безперервно контролює рівень газу в приміщенні через аналоговий газовий сенсор;

5) у разі виявлення перевищення порогового рівня газу вмикає червоний індикатор тривоги та звук.

В табл. 1.6 надано підключення елементів схеми до плати мікроконтролера Arduino Uno R3.

Таблиця 1.6. Підключення елементів до плати мікроконтролера Arduino Uno R3

№	Компонент	Підключення до Arduino
1	Keypad 4×4	Рядки: D9, D8, D7, D6Стовпці: D5, D4, D3, D2
2	Сервопривод SG90	Сигнальний пін до D10Живлення: +5V, GND
3	Газовий сенсор типу MQ	A1 → +5V (через нагрівач H1)B1 → GND (через H2)A0 → Analog A0 для зчитування
4	П'єзодинамік (Buzzer)	D11 – сигнал Живлення: +5V, GND
5	Червоний світлодіод (тривога)	Анод через резистор 220 Ом до D13, катод – GND
6	Зелений світлодіод (доступ)	Анод через резистор 220 Ом до D12, катод – GND

Розглянемо принцип роботи кожного елемента.

Клавіатура Keypad дозволяє користувачу ввести пароль. При натисканні клавіш дані зчитуються та накопичуються у змінній. Якщо введено правильний пароль (1234) і натиснуто #, сервопривод відкриває двері, і загоряється зелений світлодіод на піні D12. Якщо пароль неправильний – вмикається сирена.

Сервопривод після введення правильного паролю повертається на 90°, імітуючи відкривання дверей, через 5 секунд повертається назад (0°), закриваючи їх.

Газовий сенсор безперервно зчитує рівень газу через аналоговий пін A0. Якщо рівень перевищує 600, спрацьовує тривога: вмикається сирена та червоний світлодіод.

Buzzer використовується для сигналізації в разі помилкового доступу або при підвищеному рівні газу. Генерує звук триразово при тривозі.

Світлодіоди візуально інформують про стан системи. Червоний світлодіод (D13) вмикається при тривозі (газ). Зелений світлодіод (D12) вмикається при успішному доступі.

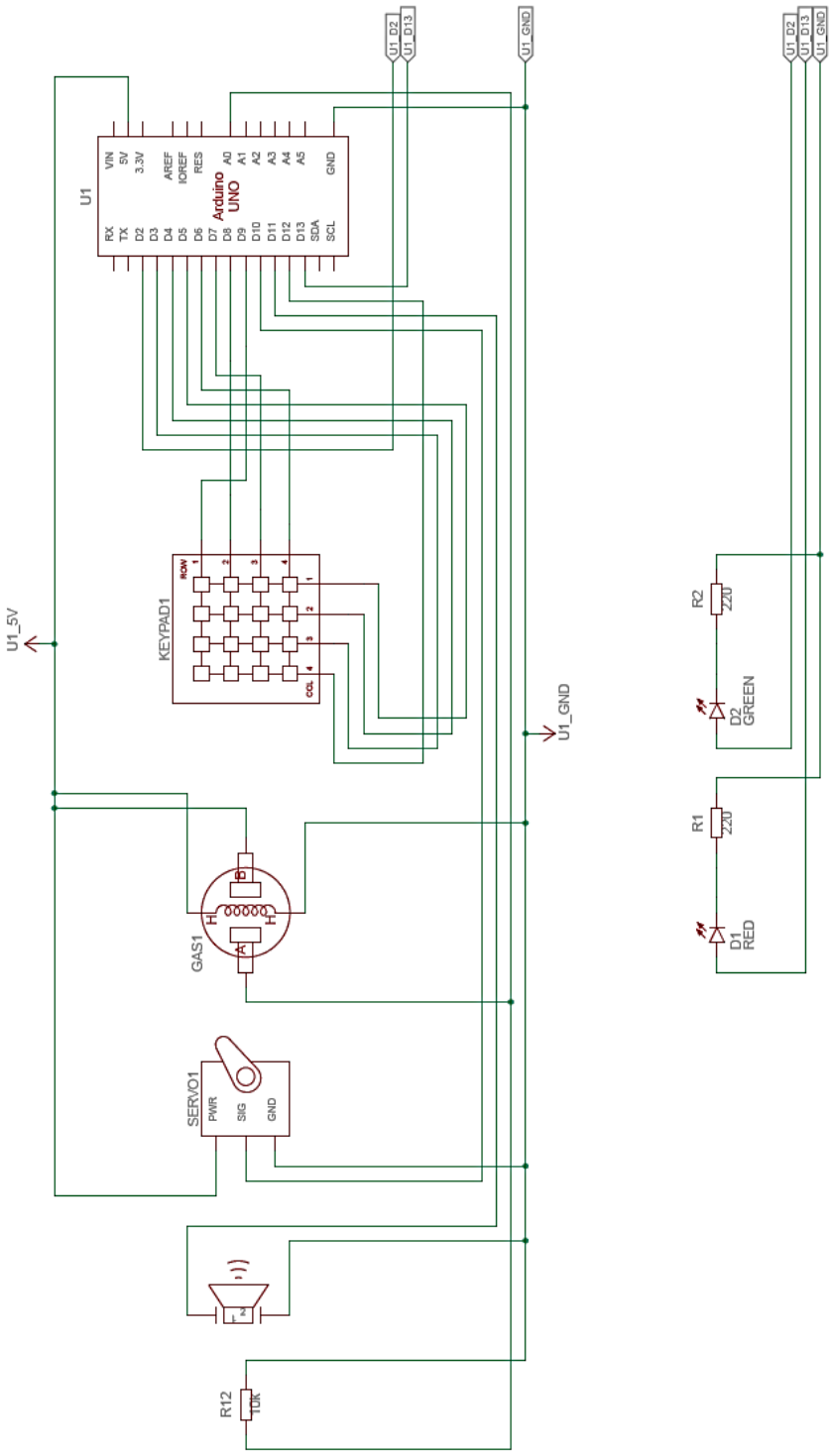


Рисунок 1.21. Схема електрична принципіальна системи захисту приміщення з датчиком газу, диму та контролем доступу

На рис. 1.22 представлена схема з компонентів системи захисту приміщення з датчиком газу, диму та контролем доступу. В табл. 1.7 надано перелік елементів схеми системи захисту приміщення з датчиком газу, диму та контролем доступу.

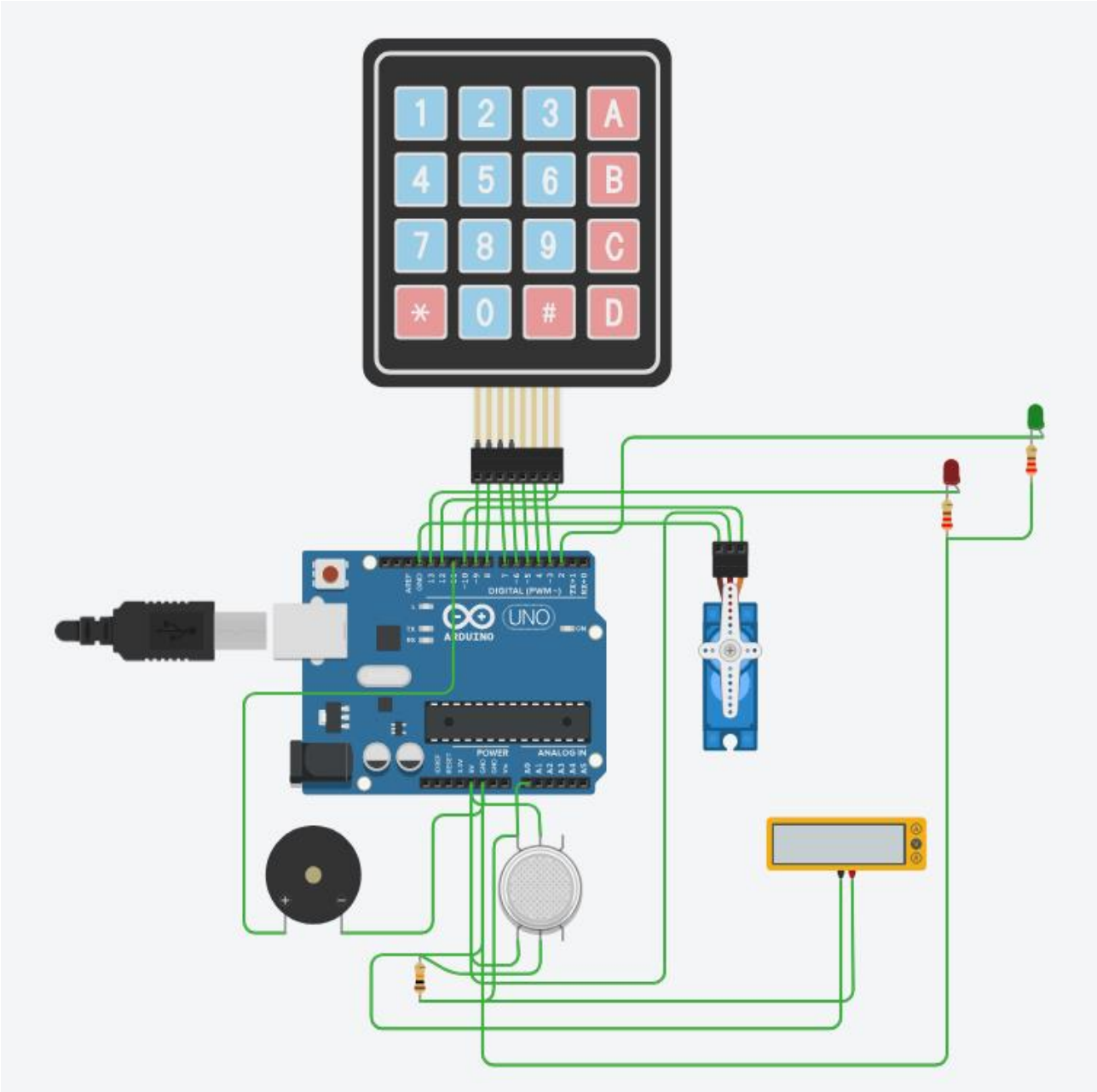


Рисунок 1.22. Схема з компонентів системи захисту приміщення з датчиком газу, диму та контролем доступу

Таблиця 1.7. Перелік елементів схеми системи захисту приміщення з датчиком газу, диму та контролем доступу

Позначення на схемі	**Кількість радіоелементів**	**Назва радіоелемента**
U1	1	Arduino Uno R3
KEYPAD1	1	Keypad 4x4
GAS1	1	Gas Sensor

продовження таблиці 1.7.

SERVO1	1	Positional Micro Servo
PIEZO1	1	Piezo
Meter1	1	Voltage Multimeter
R12	1	10 kΩ Resistor
R1, R2	1	10 kΩ Resistor
D1	1	Red LED
D2	1	Green LED

1.6 Розробка і опис програмного забезпечення

Програмне забезпечення для мікроконтролера Arduino Uno було розроблено мовою програмування C++ із використанням середовища розробки Arduino IDE. Програма забезпечує інтеграцію з клавіатурою, сервоприводом, газовим сенсором, звуковим сигналізатором та індикаторами, реалізуючи логіку роботи системи захисту приміщення.

Основні функціональні модулі програми наступні:

1) обробка введення з клавіатури:

2) контроль газового сенсора;

3) робота сервоприводу;

4) активація звукової тривоги;

5) індикація станів.

Модуль обробки введення з клавіатури виконує наступні дії. Програма зчитує натиснення клавіш із 4×4 Keypad і формує введений пароль. Після натискання клавіші # введений пароль порівнюється з коректним паролем (1234). У разі збігу надається доступ та сервопривод відкриває двері, вмикається зелений індикатор доступу, після чого двері автоматично зачиняються. У разі помилки активується тривога.

Модуль контролю газового сенсора виконує наступні дії. На аналоговому вході A0 постійно зчитуються значення напруги з газового сенсора. Якщо значення перевищує встановлений поріг (у програмі – 600), система сприймає це

як витік газу, активує звукову сигналізацію та червоний індикатор тривоги.

Робота сервоприводу виконує наступні дії. Сервомотор підключено до цифрового піну D10. При правильному введенні паролю сервопривод повертається на 90 градусів, що імітує відкривання дверей. Через 5 секунд він повертається у початкове положення (0 градусів), двері зачиняються.

Активація звукової тривоги виконує наступні дії. У разі неправильного паролю або при виявленні газу активується функція triggerAlarm(), яка генерує звуковий сигнал через п'єзодинамік на піні D11. Сигнал подається триразово із паузами.

Індикація станів виконує наступні дії. D12 (зелений світлодіод) вмикається при успішному доступі. D13 (червоний світлодіод) сигналізує про перевищення рівня газу.

В програмі використовуються наступні бібліотеки:

1) Keypad.h – для обробки введення з клавіатури 4×4;

2) Servo.h – для керування сервоприводом SG90.

Основні переваги реалізації програми наступні:

1) простий та надійний алгоритм перевірки доступу;

2) безперервний контроль за станом середовища;

3) чітка індикація різних станів (нормальний режим, тривога, доступ).

Простота адаптації до більш складних систем (наприклад, додавання GSM-модуля або дисплея).

Програма проєкта має наступний вид:

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

// === Function declaration ===
void triggerAlarm();

// === Keypad settings ===
const byte ROWS = 4;
```

```
const byte COLS = 4;
char keys[ROWS][COLS] = {
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};
byte rowPins[ROWS] = {9, 8, 7, 6};     // Піни рядків
byte colPins[COLS] = {5, 4, 3, 2};     // Піни стовпців

Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);

// === Pins ===
const int servoPin = 10;
const int buzzerPin = 11;
const int gasSensorPin = A0;
const int gasLedPin = 13;     // LED — газ
const int accessLedPin = 12;  // LED — успішний доступ

// === Variables ===
Servo doorServo;
String inputPassword = "";
String correctPassword = "1234";
bool accessGranted = false;

void setup() {
  Serial.begin(9600);
  doorServo.attach(servoPin);
  doorServo.write(0);  // Двері закриті
```

```
  pinMode(buzzerPin, OUTPUT);
  pinMode(gasLedPin, OUTPUT);
  pinMode(accessLedPin, OUTPUT);

  digitalWrite(gasLedPin, LOW);
  digitalWrite(accessLedPin, LOW);

  Serial.println("System ready. Enter password.");
}

void loop() {
  // === Gas sensor monitoring ===
  int gasLevel = analogRead(gasSensorPin);
  Serial.print("Gas level: ");
  Serial.println(gasLevel);

  if (gasLevel > 600) {
    Serial.println("Gas detected! Triggering alarm!");
    digitalWrite(gasLedPin, HIGH);   // Увімкнути LED
    triggerAlarm();
  } else {
    digitalWrite(gasLedPin, LOW);    // Вимкнути LED
  }

  // === Keypad input ===
  char key = keypad.getKey();
  if (key) {
    Serial.print("Key pressed: ");
    Serial.println(key);
```

```
    if (key == '#') {
      if (inputPassword == correctPassword) {
        Serial.println("Access granted.");
        accessGranted = true;
        digitalWrite(accessLedPin, HIGH);  // Ввімкнути LED доступу
        doorServo.write(90);              // Відчинити двері
        delay(5000);                      // Тримати відкритими 5 секунд
        doorServo.write(0);               // Закрити двері
        digitalWrite(accessLedPin, LOW);   // Вимкнути LED доступу
        accessGranted = false;
      } else {
        Serial.println("Access denied. Wrong password.");
        triggerAlarm();
      }
      inputPassword = "";  // Очистити введення
    } else if (key == '*') {
      inputPassword = "";  // Очистити вручну
      Serial.println("Input cleared.");
    } else {
      inputPassword += key;
    }
  }

  delay(100); // Невелика затримка для стабільності
}

void triggerAlarm() {
  for (int i = 0; i < 3; i++) {
    tone(buzzerPin, 1000);
```

```
    delay(300);
    noTone(buzzerPin);
    delay(200);
  }
}
```

Розроблений проєкт представлено за наступним посиланням:

https://www.tinkercad.com/things/hPyGtbQwOFn-smooth-rottis-1/editel?returnTo=https%3A%2F%2Fwww.tinkercad.com%2Fdashboard&sharecode=o8lsO9HX4dnCiI3_oM5HPyBfEfygGslnB4BX5tj3ikM

1.7 Тестування програмного і апаратного забезпечення проєкту

Після завершення розробки апаратної частини системи та програмного забезпечення було проведено тестування для перевірки коректності роботи всіх функціональних елементів. Метою тестування було виявити можливі помилки у логіці програми, перевірити відповідність фізичних підключень і впевнитися в стабільній роботі всієї системи в реальних умовах.

Розглянемо тестування різних модулів окремо.

Клавіатура (Keypad) тестуємо шляхом перевірки кожної клавіши на коректність зчитування. Тестувалася логіка введення пароля, обробка символів * (очищення) та # (перевірка пароля). Встановлено, що система правильно реагує на вірний та невірний пароль.

Сервопривід тестуємо наступним чином. При правильному паролі сервопривід повертався на 90° (відкриття дверей), після затримки повертався у вихідне положення (0°). Тестувалося декілька циклів відкриття/закриття.

На рис. 1.23 надано зображення процесу тестування клавіатури та перевірка роботи сервоприводу.

Газовий датчик проводимо таким чином: зчитувалося значення з аналогового виходу; порогове значення було встановлено на рівні 600. При

перевищенні запускалася сигналізація. Для імітації витоку газу використовувалася функція зміни значення в симуляторі. На рис. 3.14 представлено зображення тестування датчика газу та диму. Для наглядно к датчику підключено вольтметр, по якому можна побачити збільшення напруги до значення 4,05 вольт, що свідчить про його роботу.

П'єзодинамік (Buzzer) тестуємо наступним чином: перевіряємо звуковий сигнал при спрацюванні сигналізації (як при неправильному паролі, так і при витоку газу). Частота звуку та тривалість були підібрані для чіткої ідентифікації тривоги.

Світлодіоди тестуємо наступним чином: червоний (пін 13) активувався при перевищенні рівня газу; зелений (пін 12) вмикався при правильному введенні пароля та відкритті дверей.

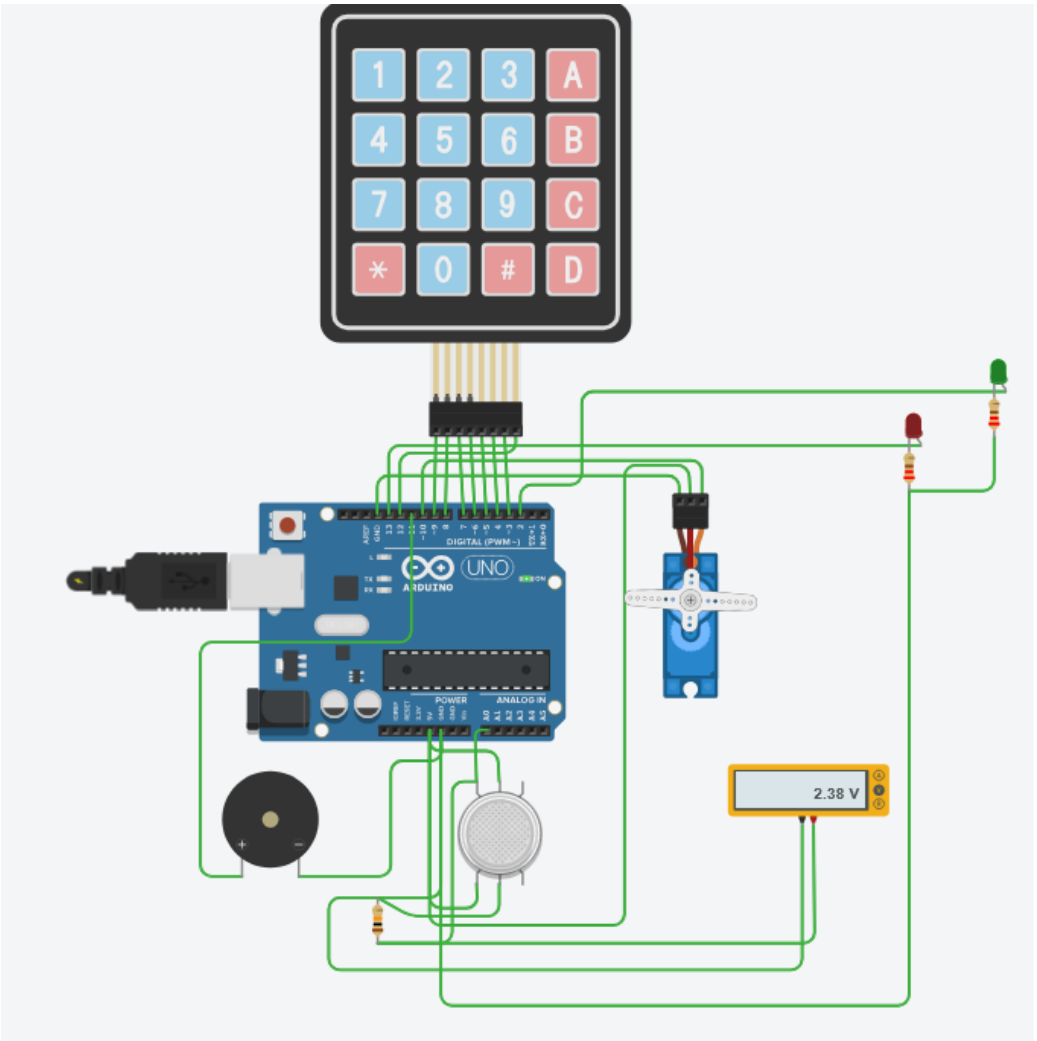


Рисунок 1.23. Тестування клавіатури та перевірка роботи сервоприводу

Системне тестування полягає в наступному. Після перевірки окремих компонентів було виконано інтегроване тестування всієї системи. Основні сценарії:

1) введення вірного пароля → відкриття дверей → активація зеленого світлодіода;

2) введення неправильного пароля → запуск сигналізації (біпер) без відкриття дверей;

3) виявлення підвищеного рівня газу → запуск сигналізації + активація червоного світлодіода;

4) паралельне спрацювання: якщо під час відкритих дверей спрацьовує датчик газу – обидва світлодіоди активуються, і система правильно обробляє обидві події.

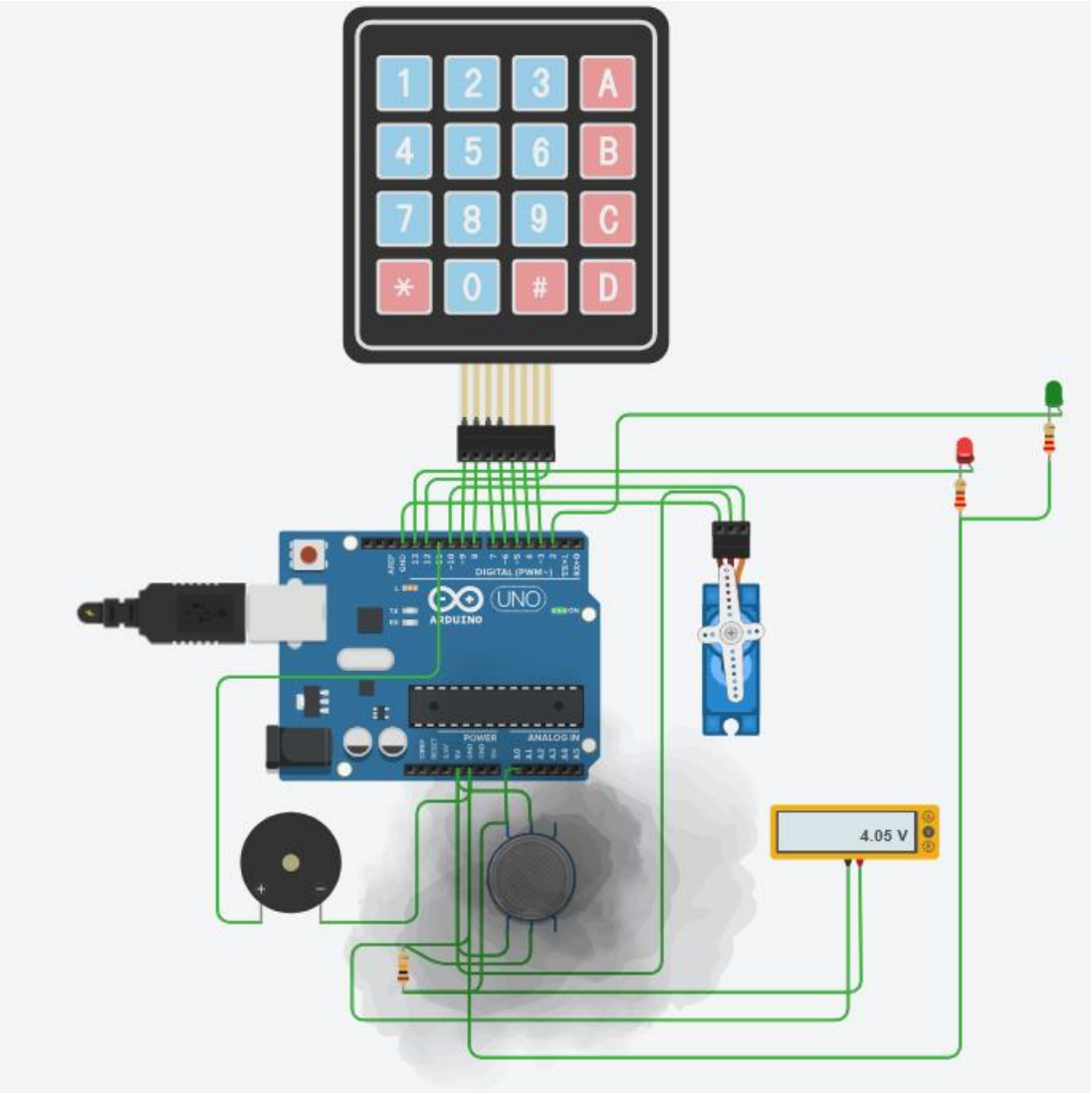


Рисунок 1.24. Тестування датчика газу та диму

Результати тестування дали наступні результати:

1) всі апаратні компоненти працюють стабільно;

2) програмне забезпечення виконує поставлені задачі;

3) Система коректно реагує на всі передбачені події.

Таким чином, розроблена система пройшла успішне тестування і може бути використана як багаторівнева система захисту приміщення.

2 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даних розрахунків є обчислення вартості виконання науково-дослідної розробки «Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу».

Цей проєкт є науково-дослідницькою розробкою. Щоб оцінити його якість, ми визначаємо трудомісткість та вартість створення. Повний перелік етапів і робіт, що виконуються під час цієї НДР, ви знайдете в табл. 2.1.

Таблиця 2.1. Розподіл робіт по етапах і видах виконавців

Етап проведення НДР	Вигляд робіт	Посада виконавця
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР по розробці «Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу»	Дипломник, керівник
Вибір напряму дослідження	1. Збір і вивчення науково-технічної літератури. 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняння. 3. Розробка плану проведення досліджень для подальшої розробки.	Дипломник керівник
Теоретичні і експериментальні дослідження	1. Аналіз існуючих систем захисту приміщень 2. Аналіз існуючих систем захисту приміщень 3. Оцінка ефективності та перспективи розвитку розробленої системи	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1. Узагальнення результатів попередніхетапів. 2. Оцінка повноти вирішення завдань. 3. Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття	Дипломник керівник консультанти

За відсутності належної нормативної бази, тривалість виконання окремих робіт визначається на основі ймовірнісних оцінок, наданих самими виконавцями.

Таблиця 2.2. Очікувана трудомісткість робіт

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР по розробці «Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу»	1
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	2
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	2
4. Розробка плану проведення досліджень для подальшої розробки.	2
5. Аналіз існуючих систем захисту приміщень	3
6. Аналіз існуючих систем захисту приміщень	5
7. Оцінка ефективності та перспективи розвитку розробленої системи	5
8.Узагальнення і оцінка результатів досліджень	3
Всього:	23

Через значну роль інтелектуальної праці у створенні науково-технічної продукції, собівартість та ціна виконання науково-дослідних робіт (НДР) формуються з таких основних статей витрат:

1. Витрати на матеріали –380 грн.

2. До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної заробітної плати для науково-дослідних робіт (НДР) розраховується з

урахуванням кількості залучених фахівців різних категорій, обсягу роботи, яку вони виконують, а також їхньої середньоденної заробітної плати.Згідно зі статтею 8 Закону України «Про Державний бюджет України на 2025 рік», встановлено такі показники:

Мінімальна місячна заробітна плата з 1 січня 2025 року становить 8000 гривень. Мінімальна погодинна тарифна ставка – 48 гривень.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

Зден= п.т.с. * 8;

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня,год.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в табл. 2.3.

Таблиця 2.3. Витрати на основну заробітну плату

Виконавець	Погодинна тарифна ставка, грн	Денна ставка, грн	Трудомісткість робочих днів	Сума основної зарплати,грн
Дипломник	48,00	364	23	8464
Керівник	80,50	644	1	644
Консультант по економіч. част.	70,50	564	0,25	141
Консультант по охороні праці	70,50	564	0,25	141
Нормоконтроль	70,50	564	0,25	141
Всього (Зо)				9531

3. Додаткова заробітна плата розраховується як відсоток від основної заробітної плати**.** У наукових установах цей показник зазвичай становить 10-12% від суми основної заробітної плати.

Зд=10%Зо= 9531*0,1 = 953,1грн

4. До собівартості науково-дослідних робіт (НДР) включаються

відрахування до єдиного соціального внеску (ЄСВ)**,** які для більшості роботодавців в Україні становлять 22% від бази нарахування

Зєсв=0,22*(Зо+Зд)=0,22*(9531+953,1) = 2306,50 грн.

5. Накладні витрати — це кошти, що йдуть на управління та господарське обслуговування всіх науково-дослідних робіт (НДР), які виконує організація. У наукових установах їхня частка зазвичай коливається від 40% до 120% від загальної суми основної та додаткової заробітної плати**.**

Рнакл= (З0+Зд)*0,5= (9531+953,1) * 0,6 = 6290,46 грн.

На основі даних, отриманих по кожній статті витрат, ми сформували калькуляцію планової собівартості всієї науково-дослідної роботи (НДР)**.** Ця калькуляція представлена у формі, наведеній у табл. 2.4.

Таблиця 2.4. Калькуляція планової собівартості

Статті витрат	Сума, грн.
1. Матеріали	380,00
2. Основна заробітна плата	9531
3. Додаткова заробітна плата	953,1
4. Відрахування до єдиного соціального внеску	2306,50
5. Накладні витрати	6290,46
Планова собівартість (Спл)	19461,06

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл= 0,1*19461,06= 1946,11грн

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції..

Договірна ціна визначається по формулі:

Цндр = Спл + Ппл = 19461,06+ 1946,11= 21407,17 грн.

Звідси ціна реалізації НДР становить:

Цр = Цнір + ПДВ = 21407,17 + 21407,17 *0,2= 25688,60 грн.

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Закон України «Про охорону праці» є одним із ключових нормативних актів, що регламентує захист життя та здоров'я громадян у процесі трудової діяльності. Він визначає основні принципи організації безпечних умов праці, регулює відносини між роботодавцем і працівником у питаннях гігієни, охорони праці та виробничого середовища, а також встановлює єдині стандарти охорони праці на території України.

У дипломному проєкті розглядається процес розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу.

У рамках проєкту буде проведено аналіз існуючих систем безпеки, розроблено архітектуру багаторівневої системи та визначено її основні компоненти. Особливу увагу буде приділено алгоритмам роботи системи та її інтеграції, що дозволить досягти високого рівня надійності та ефективності.

3.1 Аналіз небезпечних і шкідливих факторів

У процесі розробки пристрою для калібрування комп'ютерних моніторів важливо враховувати фактори, що можуть впливати на безпеку працівника. До таких належать електромагнітне випромінювання, можливі перепади електричної напруги, інтенсивність освітлення робочого місця, а також тепловий вплив при проведенні пайки електронних компонентів. Робоче середовище має бути організоване таким чином, щоб мінімізувати вплив шкідливих чинників та забезпечити комфортні умови праці.

3.2 Гігієнічні вимоги до виробничого середовища

Для забезпечення ефективної роботи над калібрувальним пристроєм необхідно враховувати умови виробничого середовища. Освітлення має відповідати нормам (300–400 лк згідно з ДБН В.2.5-28:2018), а робоче приміщення повинно бути обладнане вентиляцією для регулювання температури та рівня вологості. Важливо забезпечити зручне розташування робочого місця, захист від шуму та оптимальні санітарні умови.

Створення сприятливого робочого середовища є важливим аспектом продуктивної діяльності персоналу. Гігієнічні вимоги передбачають низку умов, які мають бути забезпечені у приміщенні, де здійснюється розробка та тестування пристрою.

Освітлення Освітлення робочого місця повинно відповідати встановленим нормативам. Згідно з ДБН В.2.5-28:2018, необхідно забезпечити рівень освітленості 300–400 лк, що дозволить зменшити навантаження на зір та покращити точність роботи з дрібними компонентами пристрою.

Вентиляція та якість повітря Робоче приміщення повинно мати ефективну вентиляцію, щоб усувати шкідливі пари та забезпечувати доступ свіжого повітря. У холодну пору року рекомендована температура 18–20°C, у теплу – 22–25°C. Оптимальний рівень вологості складає 40–60%, що сприяє комфортному перебуванню у приміщенні.

Захист від шуму та вібрацій У місцях, де проводяться пайкові роботи та тестування пристрою, слід мінімізувати рівень шуму та вібрацій, які можуть негативно впливати на продуктивність працівників. Для цього застосовують шумоізолюючі матеріали та спеціальні амортизаційні конструкції.

3.3 Вимоги безпеки праці працівника

Безпека працівника під час роботи з паяльними інструментами та електронними пристроями є першочерговим завданням. Необхідно дотримуватися таких заходів:

Використання індивідуальних засобів захисту – працівник повинен працювати у захисних рукавичках, спеціальному одязі та з використанням ізоляційного покриття на робочій поверхні.

Дотримання правильного розташування робочого місця – важливо розташувати технічне обладнання таким чином, щоб уникнути ризику перекидання чи випадкового контакту з нагрітими частинами.

Контроль електробезпеки – всі пристрої, які використовуються в роботі,

повинні мати заземлення та відповідати технічним стандартам безпеки.

Дотримання правил експлуатації обладнання – працівник повинен перевіряти справність інструментів перед початком роботи та уникати використання пошкодженого обладнання.

3.4 Правила безпеки праці при паянні

При виконанні паяльних робіт слід дотримуватися таких правил:

- Забороняється використання несправних інструментів.
- Не можна торкатися до нагрітих частин паяльника, щоб уникнути опіків.
- Обов’язкове використання витяжки для видалення шкідливих парів припою.
- Деталі утримувати плоскогубцями або спеціальними інструментами, щоб уникнути прямого контакту з гарячими компонентами.
- Регулярно провітрювати приміщення та дотримуватися санітарних норм після завершення роботи.

3.5 Пожежна безпека

Пожежна безпека є одним із критичних аспектів організації робочого місця, особливо при роботі з електронними пристроями, такими як система калібрування моніторів.

Основними причинами виникнення пожеж у виробничому приміщенні можуть бути:

- Несправність електрообладнання – коротке замикання, перевантаження електромережі та механічні пошкодження електрокабелів.
- Неправильне зберігання легкозаймистих матеріалів – відкриті ємності з хімічними речовинами, займисті припої та ізоляційні матеріали.
- Порушення техніки безпеки при пайці – попадання розплавленого припою на горючі матеріали, перегрів електропаяльників та залишення нагрітого обладнання без нагляду.

– Недотримання правил експлуатації електромереж – використання несправних розеток, відсутність захисного заземлення та неправильне підключення обладнання.
– Необережне поводження з вогнем – використання відкритого полум’я у робочому приміщенні, паління та неправильне поводження з нагрітими предметами.

Для запобігання пожежам необхідно дотримуватися ряду заходів безпеки:

– Систематичний контроль електромережі – перед початком роботи слід перевірити справність розеток, проводів та електроприладів.
– Забезпечення робочого приміщення засобами пожежогасіння – кожне місце роботи повинно бути оснащене необхідними протипожежними засобами, такими як:
– Вогнегасник (порошковий або вуглекислотний, залежно від специфіки приміщення).
– Азбестове покриття для гасіння невеликих локальних займання.
– Ящик з піском об’ємом не менше 0,5 м³ для ліквідації розливів рідких займистих речовин.
– Лопати та відра для ефективного використання піску.

Рисунок 3.1. Пожежні щити

Пожежні щити (рис. 3.1) мають бути розміщені на видимих місцях та містити необхідний набір засобів для оперативної ліквідації займання.

Щоб мінімізувати ризик виникнення пожеж, робоче місце має відповідати наступним вимогам:

– Запасні виходи повинні бути позначені світловими покажчиками із написом «Запасний вихід», видимими навіть при недостатньому освітленні.

– Пожежні крани повинні бути доступними на кожному поверсі, у коридорах та біля сходових клітин.

– Вогнегасники слід розміщувати на видимих місцях, на висоті не більше 1,5 м від підлоги для швидкого доступу.

– Евакуаційний план повинен бути розміщений у головному вході приміщення та містити детальний маршрут виходу при пожежі.

– Будівлі та приміщення повинні бути оснащені пожежними щитами з необхідним інструментом для ліквідації загоряння.

– Електромережа повинна відповідати нормам захисту – дроти та розетки повинні бути ізольованими та не перевантаженими.

– Забезпечення контрольованого доступу до виробничих приміщень – стороннім особам забороняється перебувати в робочій зоні без відповідного дозволу.

Додаткові заходи безпеки:

- Регулярні навчання—проведення інструктажів для працівників щодо дій у надзвичайних ситуаціях.
- Моніторинг пожежної безпеки—періодичне тестування пожежної сигналізації та огляд стану вогнегасників.
- Організація шляхів евакуації—забезпечення безперешкодного проходу до аварійних виходів без зайвих перешкод.
- Перевірка вентиляційних систем.

ВИСНОВКИ

В ході роботи було розроблено та реалізовано багаторівневу систему захисту приміщення на базі мікроконтролера Arduino, яка поєднує контроль доступу, виявлення загроз у вигляді витоку газу та аудіовізуальне сповіщення про небезпеку.

На основі аналізу технічних вимог та обраної архітектури було спроєктовано апаратну частину, що включає: клавіатурний модуль для введення пароля, газовий сенсор для моніторингу навколишнього середовища, сервопривід для імітації механізму відкриття дверей, п'єзодинамік для звукової сигналізації, а також світлодіоди для візуальної індикації подій.

Програмне забезпечення системи забезпечує надійну логіку роботи: здійснює перевірку пароля, керує сервоприводом, зчитує дані з газового датчика, формує тривожний сигнал у разі перевищення безпечного рівня газу або неправильно введеного пароля.

У результаті тестування було підтверджено працездатність усіх компонентів як окремо, так і в складі інтегрованої системи. Система реагує на події в режимі реального часу та виконує функції згідно з поставленими вимогами.

Отже, поставлену мету дипломної роботи досягнуто. Розроблена система може бути застосована в побуті або як основа для створення більш складних систем охорони із розширеними функціями моніторингу та віддаленого управління.

Платформа Arduino, застосована в процесі розробки, забезпечує можливість подальшого внесення змін до функціонування пристрою в разі виникнення нових вимог або потреб. Крім того, дана апаратна основа є актуальною й широко розповсюдженою, що значно спрощує її супровід, оновлення та технічне обслуговування в перспективі.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Іванченко С.О. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник/ С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.

2. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.

3. Луценко В.М., Прогонов Д.О. Методи та засоби технічного захисту інформації [Електронний ресурс]: навч. посіб. / КПІ ім. Ігоря Сікорського – Київ: КПІ ім. Ігоря Сікорського, 2021. – 289 с.

4. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

5. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

6. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів./А.М. Олейніков. –Харків: НТМТ, 2014. –298с.

7. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань “Нормативний документ”).

8. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с.

9. Строкань О.В, Прийма С.М., Литвин Ю.О. Комп’ютерна схемотехніка та архітектура комп’ютерів: лабораторний практикум. – Мелітополь, 2019. – 186 с.

10. Авраменко В. С., Авраменко А. С. Основи операційних систем. Навчальний посібник. – Черкаси: ЧНУ імені Богдана Хмельницького, 2018. – 524 с.: іл.

ДОДАТОК А

Слайди мультимедійної презентації

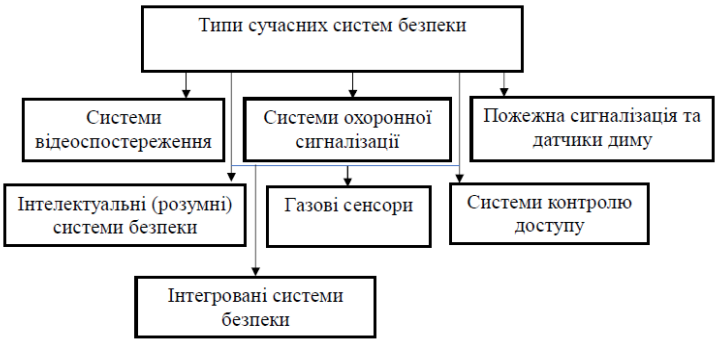
РОЗРОБКА БАГАТОРІВНЕВОЇ СИСТЕМИ ЗАХИСТУ ПРИМІЩЕННЯ З ДАТЧИКАМИ ГАЗУ, ДИМУ ТА КОНТРОЛЕМ ДОСТУПУ

ДИПЛОМНИЙ ПРОЄКТ

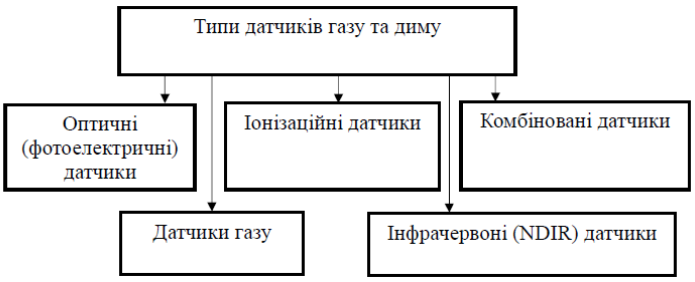
Дипломник: Витикач О.Д.
Керівник: Кільдішев В.Й.

2025

Типи систем безпеки



Основні технології виявлення диму



Основні компоненти типової СКД

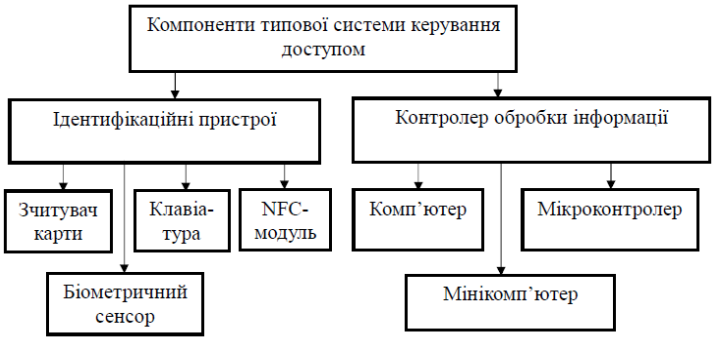


Схема взаємодії компонентів багаторівневої системи захисту приміщення

Порівняльна таблиця датчиків газу

Модель	Виявлювані речовини	Підходить для диму	Підходить для газу	Тип виходу	Сумісність з Arduino
MQ-2	Дим, пропан, метан, LPG	Так	Так	Аналоговий	Висока
MQ-5	Природний газ, LPG	Ні	Так	Аналоговий	Висока
MQ-9	CO, метан, пропан	Ні	Так	Аналоговий	Висока
MQ-135	CO_2, дим, аміак, бензол	Так	Так	Аналоговий	Висока

Основні апаратні компоненти система контролю доступу

Компонент	Призначення
Arduino Uno/Mega	Центр обробки введених даних та керування доступом.
RFID-модуль RC522	Зчитування UID RFID-карт для авторизації.
Клавіатура 4x4 Keypad	Введення PIN-коду як альтернативного методу доступу.
Серводвигун / реле	Активація електрозамка при авторизації.
Електромагнітний замок	Блокування/розблокування дверей.
Світлодіоди (LED)	Візуальна індикація результату авторизації.
Бузер	Звукова сигналізація про неправильний вхід або помилку.

Алгоритм авторизації системи контролю доступу

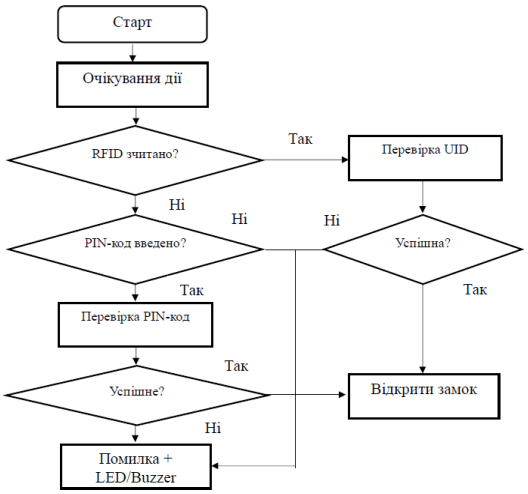
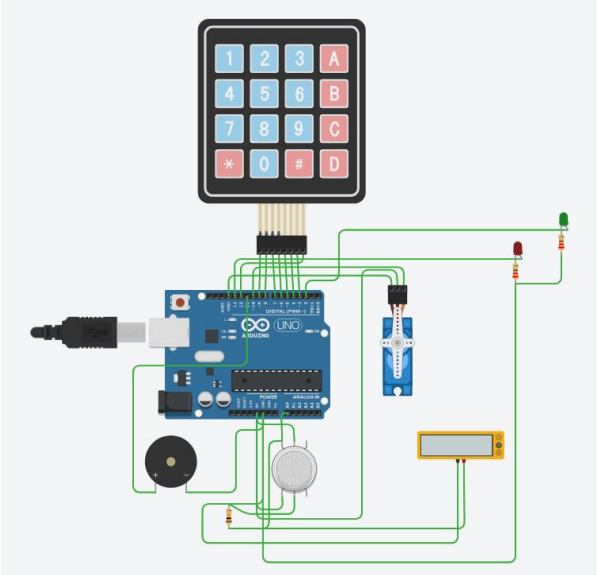
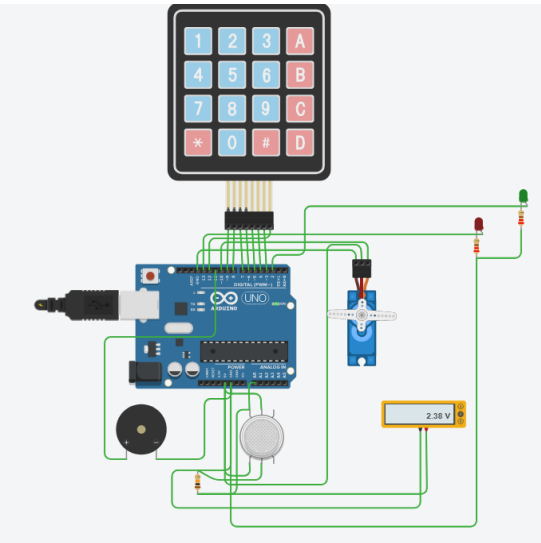


Схема з компонентів системи захисту приміщення з датчиком газу, диму та контролем доступу



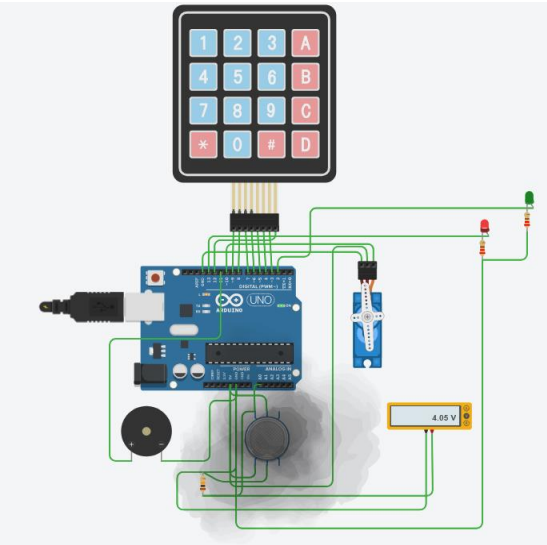
9

Тестування клавіатури та перевірка роботи сервоприводу



10

Тестування датчика газу та диму



ДЯКУЮ ЗА УВАГУ!

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проєкт здобувача (здобувачки) освіти

відділення комп'ютерних систем

Витикача Олександра Дмитровича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Обслуговування комп'ютерних систем і мереж»*

Керівник дипломного проєкту (роботи) *Кільдішев Віталій Йосипович*

(прізвище, ім`я та по батькові)

Тема дипломного проєкту (роботи) *Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу*

Обсяг розрахунково-пояснювальної записки *62* сторінок

Обсяг графічної (презентаційної) частини *12* аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проєкту завданню

Представлений на рецензію дипломний проєкт відповідає затвердженій темі та виконаний відповідно технічному завданню. Дипломний проект присвячений темі розробки багаторівневої системи захисту приміщення та складається з пояснювальної записки, мультимедійної презентації, що містить приклади використанням датчиків газу, диму та контролю доступу.

б) характеристика виконання кожного розділу дипломного проєкту

Пояснювальна записка складається з основного розділу (апаратні компоненти система контролю доступу, алгоритм авторизації системи, схема з компонентів системи захисту приміщення), економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано. Розділ охорони праці містить загальну інформацію та вимоги до техніки безпеки оператора КТ. Економічний розділ проекту містить розрахунок витрат на НДР та реалізацію проекту.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проєкту

Графічна частина складається з 12 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять ілюстративні схеми, схеми підключення датчиків газу, диму та контролю доступу, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм. Якість виконання графічної частини проекту та пояснювальної записки добра, розробку виконано у повному обсязі.

г) перелік позитивних якостей дипломного проєкту *Розроблено багаторівневу систему захисту приміщення на базі мікроконтролера Arduino, яка поєднує контроль доступу, виявлення загроз у вигляді витоку газу та аудіовізуальне сповіщення про небезпеку.*

У результаті тестування було підтверджено працездатність усіх компонентів. Система реагує на події в режимі реального часу.

д) основні недоліки дипломного проєкту *Для підвищення ефективності захисту було б доцільним провести дослідження сумісного використання систем сигналізації та відеоспостереження. Відсутність захисту даних: паролі і UID-карти зберігаються в «plain text», немає шифрування й аутентифікації каналів GSM/Wi-Fi. Недостатня документація: відсутні UML-діаграми станів, опис API й репозиторій із вихідним кодом для командної роботи.*

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Добре*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові рецензента *к.т.н. Рудніченко Микола Дмитрович*

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

Підпис: _____

«26» 06 2025 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача освіти

відділення комп'ютерних систем

Витикача Олександра Дмитровича

(прізвище, ім`я та по батькові здобувача/здобувачки освіти)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Обслуговування комп'ютерних систем і мереж»*

Тема дипломного проєкту: *«Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу»*

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЄКТУ

а) обсяг і якість виконання проєкту (графічного матеріалу і розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над проектом: _____

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Проведено огляд існуючих систем захисту приміщень. Представлено аналіз основних вимог до багаторівневої системи захисту приміщень. Розроблена алгоритм роботи багаторівневої системи на основі Arduino. Проведена оцінка ефективності та перспективи розвитку розробленої системи.

в) теоретична підготовка випускника_____

відповідає вимогам, що надаються здобувачу освіти зі спеціальності

«Комп'ютерна інженерія»

г) вміння розв'язувати виробничі та конструкторські питання _____

У дипломному проєкті розроблено та реалізовано багаторівневу систему захисту приміщення на базі мікроконтролера Arduino. На основі аналізу технічних вимог та обраної архітектури було спроєктовано апаратну частину. Програмне забезпечення системи забезпечує надійну логіку роботи. У результаті тестування було підтверджено працездатність усіх компонентів як окремо, так і в складі інтегрованої системи.

Оцінка розрахункової частини 4 (добре)

Оцінка графічної (презентаційної) частини 4 (добре)

Загальна оцінка 4 (добре)

Прізвище, ім'я, по батькові керівника роботи Кільдішев Віталій Йосипович

Місце роботи і посада керівника роботи к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

«16» 06 2025 р. _____ _____

(підпис) (прізвище та ініціали керівника)

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
(ДИПЛОМНОГО ПРОЄКТУ)
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Витикач Олександр Дмитрович,

здобувач освіти гр. 4КС-58, та

Кільдішев Віталій Йосипович,
керівник дипломного проєкту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проєкту фахового молодшого бакалавра на тему:

«Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу» (автор роботи – Витикач О.Д., керівник роботи – Кільдішев В.Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Витикач О.Д. /

Керівник _____ / Кільдішев В.Й. /

«18» червня 2025 р.

ДОВІДКА

циклової комісії КТ та ПІ
про допуск до захисту дипломного проєкту
здобувача (здобувачки) освіти IV курсу
відділення комп'ютерних систем групи 4КС-58

Витикача Олександра Дмитровича

на тему *Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до дипломного проєкту виконана з некритичними порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис) *20.06.2025* (дата) *Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 15.06.2025 р. значення коефіцієнту подібності в роботі становить 16,53%, коефіцієнт цитування – 1,17%.*

(підпис) *20.06.2025* (дата) *Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) дипломного проєкту

здобувача (здобувачки) освіти *Витикача О.Д.* (П.І.Б.)

проведена «*20*» *червня* 2025 р.

Висновки *Пояснювальна записка до дипломного проєкту виконана у повному обсязі. Випускна кваліфікаційна робота (дипломний проєкт) відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Голова ЦК КТ та ПІ (підпис) *Кривченко Ю.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 6/15/2025
Дата редагування 6/15/2025

Документ прийнятий

Звіт подібності

метадані

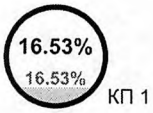
Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Розробка багаторівневої системи захисту приміщення з датчиками газу, диму та контролем доступу

Автор
Витикач Олександр Дмитрович
Науковий керівник / Експерт
Кільдішев Віталій Йосипович

підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1

КЦ

25
Довжина фрази для коефіцієнта подібності 2

10733
Кількість слів

86537
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	6
Інтервали	A⟶	0
Мікропробіли	·	0
Білі знаки	ß	0
Парафрази (SmartMarks)	a	46

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	61 0.57 %
2	https://forum.arduino.cc/t/how-to-convert-ascii-to-int/578348	49 0.46 %
3	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	41 0.38 %
4	https://card-file.ontu.edu.ua/bitstreams/21173711-5b67-4b87-b17f-6302c25e7a31/download	40 0.37 %
5	https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	37 0.34 %

6	https://card-file.ontu.edu.ua/bitstreams/29489599-0581-4ce6-8890-c3b13d9f2e0e/download	37 0.34 %
7	https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	35 0.33 %
8	https://card-file.ontu.edu.ua/server/api/core/bitstreams/a05c07c5-bf65-4cb0-bdfa-e28694707551/content	31 0.29 %
9	https://kb.khmnu.edu.ua/wp-content/uploads/sites/6/opp.02-tehnologiyi-ta-systemy-zahystu-informacziyi.pdf	31 0.29 %
10	https://card-file.ontu.edu.ua/server/api/core/bitstreams/6eb6bf1c-5813-45e6-93c5-25539b4709d3/content	29 0.27 %

з домашньої бази даних (0.18 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка веб-застосунку інтелектуального пошуку та сумісного перегляду аніме-контенту [redacted] 6/14/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	14 (2) 0.13 %
2	Розробка web-застосунку для генерації повідомлень із використанням технологій штучного інтелекту [redacted] 6/14/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	5 (1) 0.05 %

з програми обміну базами даних (0.07 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	КВАЛІФІКАЦІЙНА РОБОТА (ДИПЛОМНИЙ ПРОЄКТ) [redacted] 5/27/2025 Ivano-Frankivsk National Technical University of Oil and Gas (ДЕП-ЕТ)	8 (1) 0.07 %

з Інтернету (16.28 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download	550 (46) 5.12 %
2	https://card-file.ontu.edu.ua/bitstreams/aed610a6-43ef-47e0-9066-e85c89456f3e/download	245 (20) 2.28 %
3	**https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download**	**129 (9) 1.20 %**
4	**https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download**	**118 (9) 1.10 %**
5	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content**	**97 (4) 0.90 %**
6	**https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download**	**89 (3) 0.83 %**
7	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/6eb6bf1c-5813-45e6-93c5-25539b4709d3/content**	**75 (4) 0.70 %**
8	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/a05c07c5-bf65-4cb0-bdfa-e28694707551/content**	**70 (3) 0.65 %**
9	**https://kb.khmnu.edu.ua/wp-content/uploads/sites/6/opp.02-tehnologiyi-ta-systemy-zahystu-informacziyi.pdf**	**54 (3) 0.50 %**

10	**https://forum.arduino.cc/t/how-to-convert-ascii-to-int/578348**	**49 (1) 0.46 %**
11	**https://card-file.ontu.edu.ua/bitstreams/29489599-0581-4ce6-8890-c3b13d9f2e0e/download**	**42 (2) 0.39 %**
12	**https://card-file.ontu.edu.ua/bitstreams/21173711-5b67-4b87-b17f-6302c25e7a31/download**	**40 (1) 0.37 %**
13	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/21ac499a-a9e9-4137-810c-5f21a0318048/content**	**29 (1) 0.27 %**
14	**https://ppt-online.org/337137**	**25 (1) 0.23 %**
15	http://repository.ub.ac.id/166825/1/Romario%20Siregar.pdf	23 (2) 0.21 %
16	https://nm2.univd.edu.ua/index.php/download/144910	22 (1) 0.20 %
17	https://e-tk.lntu.edu.ua/mod/page/view.php?id=14512	20 (1) 0.19 %
18	https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content	13 (2) 0.12 %
19	http://reposit.nupp.edu.ua/bitstream/PoltNTU/10251/1/402-%D0%A2%D0%9A%20%D0%9A%D0%BE%D0%B1%D0%B8%D0%BB%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D0%B8%D0%B9.docx	11 (1) 0.10 %
20	https://mafiadoc.com/my-title_5b83869b097c470b7a8b4733.html	8 (1) 0.07 %
21	https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download	7 (1) 0.07 %
22	https://github.com/TricksterC/SSCS-Arduino-Comp-24/blob/main/main.c	6 (1) 0.06 %
23	https://elartu.tntu.edu.ua/bitstream/lib/46087/2/Ihor_Rii.pdf	5 (1) 0.05 %
24	https://ir.library.knu.ua/knurepo/bitstream/handle/123456789/1649/Temchur_bakalavr%20.pdf?sequence=1	5 (1) 0.05 %
25	https://card-file.ontu.edu.ua/bitstreams/bbaf3f38-16a8-4070-bead-5562769b7c71/download	5 (1) 0.05 %
26	http://www.dut.edu.ua/uploads/n_7221_44521673.pdf	5 (1) 0.05 %
27	http://www.sohu.com/a/339352145_120248280	5 (1) 0.05 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Обслуговування комп'ютерних систем і мереж»
Група: 4КС- 58

Дипломний проєкт
здобувача освіти денної форми навчання К С. 58.04.000.ДП

ВИТИКАЧА ОЛЕКСАНДРА
ДМИТРОВИЧА

м. Одеса
2025 р. МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Обслуговування комп'ютерних систем і мереж»