

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

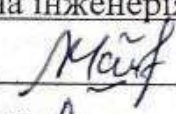
БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

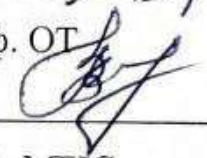
на тему:

«Мікропроцесорна система протипожежного сповіщення»

Виконав: студент 2 курсу, групи КІ-23мсз
спеціальності 123 — «Комп'ютерна
інженерія»

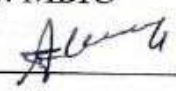
освітня програма — «Комп'ютерна інженерія»

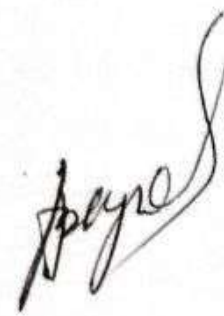
Половянова М. Г. 

Керівник к.т.н., доц. каф. ОТ 

Богомолів С. В.

Рецензент к.т.н., доц. каф. МБІС

Шиян А. А. 


Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О. Д.

"19" 06 2025 р.

Вінниця ВНТУ – 2025 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітньо—кваліфікаційний рівень бакалавр
Галузь знань — 12 Інформаційні технології
Спеціальність — 123 Комп'ютерна інженерія
Освітня програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ проф., д.т.н.

Азаров О. Д.

 21 березня 2025 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Половяновій Марині Геннадіївні

1 Тема роботи: Мікропроцесорна система протипожежного сповіщення, керівник роботи Богомолів Сергій Віталійович, к.т.н., доцент кафедри ОТ, затверджено наказом вищого навчального закладу від 20 березня 2025р. № 97.року.

2 Строк подання студентом роботи 13.05.2025 р.

3 Вихідні дані до роботи: технічний опис мікропроцесорної системи протипожежного сповіщення, технології розробки: мова програмування C для Arduino, бібліотеки для роботи з серійним зв'язком та Ethernet, мобільні сервіси, технології для інтеграції з мобільними застосунками, цільова платформа системи — Arduino, середовище розробки — Arduino IDE.

4 Зміст розрахунково-пояснювальної записки: вступ; аналіз існуючих прототипів та визначення вимог до створюваної системи; обґрунтування структури та принципів роботи системи; розробка й тестування апаратно-програмної системи; висновки.

5 Перелік графічного матеріалу: Діаграма детекції вогню.

Перелік ілюстративного матеріалу: Результати тестування системи.

6 Консультанти розділів роботи приведені в таблиці 1.

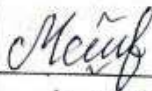
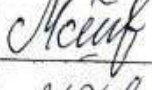
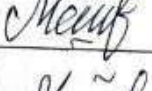
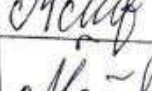
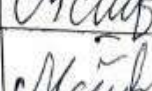
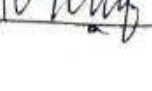
Таблиця 1 — Консультанти роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	к.т.н., доц. каф. ОТ Богомолів С. В.	21.03.2025 р. 	13.05.2025 р. 
Нормоконтроль	Швець С. І.	13.05.2025 р. 	30.05.2025 р.

7. Дата видачі завдання 21.03.2025 р.

8. Календарний план приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів дипломної роботи	Строк виконання	Підпис
1	Постановка задачі роботи	21.03.25— 30.03.25	
2	Пошук матеріалів та інформаційних джерел	21.03.25— 30.03.25	
3	Аналіз існуючих прототипів та визначення вимог до створюваної системи	31.03.25— 13.04.25	
4	Обґрунтування структури та принципів роботи системи	14.04.25— 27.04.25	
5	Розробка й тестування апаратно-програмної системи	28.04.25— 11.05.25	
6	Оформлення пояснювальної записки та ілюстративного матеріалу	13.05.25	
7	Перевірка якості виконання бакалаврської кваліфікаційної роботи та усунення недоліків	21.03.25— 30.03.25	

Студент

Керівник роботи




Марина ПОЛОВЯНОВА

к.т.н., доц. Сергій БОГОМОЛОВ

АНОТАЦІЯ

УДК 621.3:614.84

Половянова М. Г. Мікропроцесорна система протипожежного сповіщення. Бакалаврська кваліфікаційна робота зі спеціальності 123 «Комп'ютерна інженерія», освітня програма «Системне програмування». Вінниця: ВНТУ, 2025. 90 с.

На укр. мові. Бібліогр.: 25 назв, рис.31, табл. 3, ліст 5.

У бакалаврській кваліфікаційній роботі розроблено мікропроцесорну систему для виявлення пожежі та сповіщення користувача через мобільний додаток. У процесі дослідження проаналізовано існуючі методи виявлення пожеж та вивчені сучасні рішення в галузі протипожежної безпеки, зокрема у контексті Інтернету речей (IoT). Визначено переваги використання IoT для створення економічно ефективних та безпечних систем, здатних оперативно реагувати на надзвичайні ситуації.

Розроблено апаратно-програмний комплекс на базі Arduino, що включає датчики для виявлення пожежі та систему сповіщення. Для реалізації програмної частини застосовано мобільний додаток, що забезпечує швидке інформування користувачів і екстрених служб. Система пройшла випробування, які підтвердили її ефективність у задачах швидкого реагування.

Актуальність роботи полягає в необхідності зниження ризику людських втрат та матеріальних збитків через пожежі, що є особливо важливим у сучасних умовах загрози та агресії. Розроблений комплекс забезпечує надійне і швидке сповіщення про загрозу та дозволяє оперативно реагувати на виникнення пожежі.

Ключові слова: мікропроцесорна система, пожежна безпека, Інтернет речей, Arduino, сповіщення, мобільний додаток, протипожежне сповіщення.

ABSTRACT

Polovianova M. G. Microprocessor fire alarm system. Bachelor's qualification work in specialty 123 "Computer Engineering", educational program "System Programming". Vinnytsia: VNTU, 2025. 90 p.

In Ukrainian. Bibliography: 25 titles, fig. 31, tab. 3, list 5.

In the bachelor's qualification work, a microprocessor system for fire detection and user notification via a mobile application was developed. In the process of research, existing fire detection methods were analyzed and modern solutions in the field of fire safety were studied, in particular in the context of the Internet of Things (IoT). The advantages of using IoT for creating cost-effective and safe systems capable of responding promptly to emergencies were determined.

A hardware-software complex based on Arduino was developed, which includes fire detection sensors and a notification system. To implement the software part, a mobile application was used, which provides rapid notification of users and emergency services. The system has passed tests that confirmed its effectiveness in rapid response tasks.

The relevance of the work lies in the need to reduce the risk of human losses and material damage due to fires, which is especially important in modern conditions of threat and aggression. The developed complex provides reliable and rapid notification of the threat and allows for a prompt response to the occurrence of a fire.

Keywords: microprocessor system, fire safety, Internet of Things, Arduino, notification, mobile application, fire notification.

ЗМІСТ

ВСТУП	4
1 АНАЛІЗ ІСНУЮЧИХ ПРОТОТИПІВ ТА ВИЗНАЧЕННЯ ВИМОГ ДО СТВОРЮВАНОЇ СИСТЕМИ	6
1.1 Сучасні тенденції у протипожежних технологіях	7
1.1.1 Виявлення диму та полум'я за допомогою відеоаналізу	9
1.1.2 Системи голосової евакуації нового покоління	10
1.1.3 Бездротові технології в протипожежних сигналізаціях	12
1.1.4 Інноваційні рішення у звітності диспетчерських станцій	14
1.1.5 Новітні технології звукового оповіщення	15
1.2 Типова структура сучасної пожежної сигналізації	16
1.3 Обмеження і недоліки наявних технічних рішень	20
1.4 Формулювання вимог до апаратної і програмної частини проєкту	22
2 ОБҐРУНТУВАННЯ СТРУКТУРИ ТА ПРИНЦИПІВ РОБОТИ СИСТЕМИ	25
2.1 Принципи функціонування сенсорів виявлення полум'я	25
2.1.1 Класифікація сенсорів для виявлення відкритого вогню	26
2.1.2 Основні характеристики сенсорів	28
2.1.3 Оцінка використання сенсорів полум'я	30
2.2 Опис принципу роботи gsm-модуля	32
2.2.1 Можливості та обмеження GSM-рішень	36
2.3 Методика розпізнавання та діагностики загоряння	38
3 РОЗРОБКА Й ТЕСТУВАННЯ АПАРАТНО-ПРОГРАМНОЇ СИСТЕМИ ..	41
3.1 Апаратна складова комплексу	41
3.1.1 Можливості підключення Arduino Nano	43
3.1.2 Налаштування плати Arduino	45
3.1.3 Модуль ІЧ-датчика виявлення полум'я	46
3.1.4 Модуль GSM, його структура та функції	48
3.1.5 Організація живлення системи	50

3.3 Розробка прототипу системи	51
3.4 Створення програмного забезпечення	52
3.4.1 Мова програмування	54
3.4.2 Середовище для розробки.....	56
3.4.3 Застосування бібліотеки softwareserial	58
3.4.4 Використання бібліотеки string.h.....	59
3.5 Реєстрація облікового запису у thingspeak та конфігурація системи	60
3.6 Підключення мобільного додатку до пристрою для отримання повідомлень	64
3.7 Перевірка функціональності системи	66
ВИСНОВКИ	70
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	71
ДОДАТОК А Технічне завдання	73
ДОДАТОК Б Протокол перевірки навчальної (кваліфікаційної) роботи.....	77
ДОДАТОК В Графічна частина. Діаграма детекції вогню	78
ДОДАТОК Г Ілюстративна частина. Результати тестування системи	80
ДОДАТОК Д Лістинг коду програми	78

ВСТУП

Актуальність теми обумовлена тим, що забезпечення пожежної безпеки залишається одним із найважливіших завдань у сфері охорони життя та майна людини. Причини виникнення пожеж у більшості випадків пов'язані з людським фактором, несправністю електрообладнання або впливом зовнішніх чинників. Своєчасне виявлення загоряння значною мірою зменшує ризики значних втрат та дозволяє оперативно реагувати на надзвичайні ситуації.

Сучасні умови, зокрема, підвищене навантаження на енергетичні системи, зростання кількості побутової електроніки, перебої з електропостачанням, а також виклики, пов'язані з воєнними діями, обумовлюють необхідність створення ефективних систем раннього виявлення пожежі. Особливе значення мають автоматизовані, мікропроцесорні системи, що забезпечують автономну роботу та можливість віддаленого сповіщення про загрозу.

Одним із перспективних напрямів є використання платформи Arduino для побудови прототипів таких систем, завдяки її доступності, широкому функціоналу та гнучкості. Поєднання мікроконтролерів з датчиками диму та температури, а також засобами бездротової передачі даних, дозволяє реалізувати ефективне рішення для моніторингу та сповіщення про можливу пожежу. Саме тому розробка прототипу мікропроцесорної системи протипожежного сповіщення є актуальним завданням у сфері прикладної інженерії [1].

Мета роботи — розробити та дослідити прототип мікропроцесорної системи раннього виявлення пожежі з функцією сповіщення користувача про загрозу.

Задачі дослідження:

- проаналізувати існуючі підходи до побудови систем виявлення пожежі;
- визначити функціональні та технічні вимоги до розроблюваної системи;
- обрати необхідні апаратні та програмні компоненти;
- розробити структурну схему та алгоритм роботи системи;
- реалізувати прототип системи на базі Arduino;
- протестувати працездатність системи та оцінити її ефективність.

Об’єкт дослідження — мікропроцесорні системи моніторингу параметрів навколишнього середовища з метою виявлення пожежі.

Предмет дослідження — процес проєктування та реалізації прототипу системи протипожежного сповіщення на основі мікроконтролера Arduino.

Практичне значення роботи полягає в можливості використання створеного прототипу в якості основи для побудови доступних побутових або навчальних систем раннього попередження про загрозу пожежі.

Для вирішення задач, поставлених у роботі використовувалися такі **методи дослідження**, як методи аналізу технічної літератури, моделювання, структурного проєктування, розробки програмного забезпечення для мікроконтролерних систем та експериментального тестування.

Наукова новизна полягає у поєднанні простих та доступних апаратних засобів з алгоритмічним підходом до своєчасного виявлення пожежної небезпеки і передачі інформації користувачеві.

1 АНАЛІЗ ІСНУЮЧИХ ПРОТИТИПІВ ТА ВИЗНАЧЕННЯ ВИМОГ ДО СТВОРЮВАНОЇ СИСТЕМИ

Забезпечення пожежної безпеки є ключовим фактором для збереження життя та матеріальних цінностей у робочих і побутових умовах. Вона має вирішальне значення для мінімізації ризиків, пов'язаних із виникненням займання, поширенням вогню та можливими ушкодженнями інфраструктури. Упровадження ефективних заходів протипожежного захисту вимагається не лише нормативно-правовими актами, а й продиктоване необхідністю убезпечити всіх, хто може перебувати в зоні потенційної небезпеки.

Зважаючи на те, що багато робочих приміщень містять матеріали, які легко спалахують, обговорення принципів пожежної безпеки та запровадження відповідних технологій набувають особливого значення. Одним із завдань є підвищення обізнаності щодо механізмів займання — зокрема, взаємодії тепла, палива та кисню — які в сукупності утворюють так званий "вогняний трикутник". Усвідомлення цих факторів дозволяє швидше ідентифікувати загрози та відповідно реагувати на них.

Одним із ключових напрямів у попередженні пожеж є навчання персоналу та створення чітких інструкцій і планів дій. Важливо визначити зони підвищеного ризику, джерела тепла та горючі матеріали, що можуть слугувати тригерами для виникнення пожежі. До таких небезпек належать несправне електрообладнання, пошкоджені кабелі, перевантажені розетки, обігрівальні прилади, легкозаймисті речовини, а також недотримання правил поводження з відкритим вогнем.

Розробка сучасних систем виявлення пожежі та сповіщення — зокрема з використанням мікропроцесорної техніки — дозволяє не лише своєчасно фіксувати критичні зміни параметрів навколишнього середовища, але й передавати відповідну інформацію відповідальним особам або автоматично запускати алгоритми реагування. Це робить такі системи необхідним елементом сучасної інфраструктури безпеки.

1.1 Сучасні тенденції у протипожежних технологіях

У червні минулого року на конференції NFPA значну увагу було приділено концепції Smart Connected Things (SCoT), яка все активніше впроваджується в системи пожежної безпеки. Одну з тематичних сесій провели Террі Віктор (Johnson Controls, Grinnell Fire Protection Solutions) та Крістіна Френсіс (Procter & Gamble Co.). У своїх доповідях вони акцентували на тому, що такі технології дають змогу як власникам об'єктів, так і компаніям-обслуговувачам отримувати актуальну інформацію про стан систем і навіть дистанційно проводити частину процедур перевірки та тестування.

Цифрові та підключені пристрої вже давно стали невід'ємною складовою сучасного світу, і сьогодні їх активно інтегрують в інфраструктуру пожежного захисту [2]. Зокрема, застосування інтелектуальних засобів дає змогу досягти більшої точності та ефективності під час перевірок і технічного обслуговування, що в умовах надзвичайних ситуацій може виявитися життєво важливим. У публікації, що висвітлювала думки згаданих експертів, було описано уявний сценарій пожежі на складі. Якщо в такому приміщенні впроваджено розумні сенсори, які відстежують тиск води та швидкість потоку в спринклерній системі, то оператори в реальному часі знатимуть, скільки води подається щохвилини. Це дозволяє зробити висновки щодо ефективності гасіння пожежі й оперативно інформувати відповідні служби.

Можливість моніторингу параметрів протипожежної системи ззовні — лише один із прикладів того, як інтелектуальні технології здатні сприяти порятунку людських життів. Додатково такі рішення можуть автоматично повідомляти власника будівлі про критичні несправності: наприклад, про заблоковані клапани, замерзання труб або відсутність тиску в системі.

Одним з яскравих прикладів нових технологій для покращення виявлення диму у побутових умовах є розробка компанії Kidde, яка представила перший димовий сповіщувач, що повністю відповідає оновленим вимогам стандарту UL 268 (2020 рік). Ці норми вимагають, аби кожен детектор мав підвищену чутливість

до диму, спричиненого займанням пінополіуретану, а також міг чітко відрізнити дим під час готування їжі від диму, який утворюється внаслідок справжньої пожежі. Детальніше з критеріями випробувань можна ознайомитися на офіційному сайті організації UL.



Рисунок 1.1 — Сучасний детектор диму з технологією TruSense

Основне завдання нових пристроїв — вміння розрізняти тип горіння залежно від джерела: чи то хімічний матеріал, чи побутовий процес. Це дозволяє значно знизити кількість помилкових спрацювань. Технологія TruSense, що інтегрована в нову лінійку сигналізаторів Kidde, здатна ідентифікувати як стрімке займання, так і тління, а також відрізнити їх від звичайного диму, наприклад, з кухні. Такий підхід спрямований на підвищення довіри з боку користувачів — аби вони не демонтували сигналізацію через хибні тривоги, а навпаки — покладалися на неї як на надійний засіб безпеки.

Слід зазначити, що інші виробники також активно адаптують свої продукти до нових стандартів, водночас створюючи комерційні рішення, орієнтовані на використання як у житлових будинках, так і в корпоративному секторі, адже вимоги ринку до безпеки стрімко зростають.

1.1.1 Виявлення диму та полум'я за допомогою відеоаналізу

Технологія виявлення диму та полум'я за допомогою відеоаналізу активно використовується вже протягом тривалого часу (див. рис. 1.2), однак останні роки стали періодом значного розширення її можливостей і сфер застосування [3]. Суть технології полягає у використанні аналітичних алгоритмів, що базуються на відеозображеннях, які обробляються в реальному часі. Відеокамери інтегруються з сучасними системами пожежного моніторингу для точного розпізнавання диму або полум'я.

Алгоритми аналізують отримані зображення за низкою параметрів, таких як зміни яскравості, контрасту, візуального шуму, наявності динамічного руху тощо. Залежно від реалізації, система здатна не лише фіксувати факт займання, але й забезпечувати додаткові функції, зокрема виявлення руху, автоматичну локалізацію події, а також передачу тривожних повідомлень.

Ключовою особливістю технології VISD (Video Image Smoke Detection) є можливість візуально ідентифікувати ознаки загоряння ще до того, як подія досягне масштабів, здатних активувати традиційні детектори. Такий підхід є особливо ефективним для великих відкритих об'єктів або приміщень зі складною логістикою, де локалізація джерела вогню звичайними методами є ускладненою. Прикладами можуть слугувати електростанції, паперові комбінати, великі стадіони чи розподільчі склади.

Сучасні відеосистеми, як-от Flame VID, дозволяють не лише виявляти вогонь, а й оперативно визначати точне місце загоряння. Це значно прискорює реагування персоналу та дозволяє реалізувати оперативні заходи щодо гасіння пожежі ще до її поширення на критичні ділянки об'єкта.



Рисунок 1.2 — Виявлення диму за допомогою відеоаналізу

1.1.2 Системи голосової евакуації нового покоління

Голосова евакуація та можливість налаштовувати індивідуальні директиви евакуації є важливими елементами в системах безпеки, що забезпечують порятунок у надзвичайних ситуаціях. У 2019 році компанії Notifier і Edwards представили нові продукти, які підвищують ефективність голосової евакуації, зокрема інтегруючи її в комплексні системи пожежної сигналізації.

Сенсорні колонки серії L від Notifier здатні передавати важливі повідомлення, що відповідають вимогам стандартів. Вони оснащені 8-дюймовими динаміками з подвійною напругою, що забезпечують високоякісне звучання і точність передачі звуку. Колонки доступні в різних варіантах монтажу — на стіни або стелі, що робить їх ідеальними для великих складів, густонаселених приміщень або зон з високим рівнем шуму.

У свою чергу, Edwards у 2019 році представила платформу EST4, яка була розроблена як передова система для зв'язку в надзвичайних ситуаціях. Вона надає розробникам більше можливостей для налаштування і реалізації евакуаційних планів, забезпечуючи надійну мережеву платформу для пожежної сигналізації та екстреного зв'язку.

Один з важливих напрямів розвитку в індустрії протипожежного захисту — це забезпечення стійкості систем до різних екстремальних умов. Системи гасіння водяним туманом, такі як HI-FOG, ефективно охолоджують вогонь, зменшують теплове випромінювання та видаляють кисень з осередку пожежі. Такі технології (див. рис. 1.3) набули популярності у будівлях з підвищеними вимогами до захисту від водяних пошкоджень або в населених районах, де можуть виникати значні ризики.



Рисунок 1.3 — Система гасіння пожежі за допомогою водяного туману

Окрім традиційних спринклерних систем, існують також газові системи гасіння, що були розроблені як альтернатива водяним системам. Однак, внаслідок екологічних ризиків, таких як внесок у глобальне потепління, все більше уваги приділяється системам водяного туману. Вони є більш безпечними для навколишнього середовища і забезпечують таку ж ефективність у порівнянні з газовими системами.

Ці водяні системи, завдяки своїй екологічній безпеці та високій ефективності, стають все популярнішими в галузі протипожежного захисту.

1.1.3 Бездротові технології в протипожежних сигналізаціях

Сучасний світ є свідком широкого впровадження бездротових технологій у різні сфери життя [4]. Ринок пожежної сигналізації довгий час повільно адаптував бездротові рішення через жорсткі нормативні вимоги до обладнання, яке забезпечує безпеку життя. Проте за останні десять років завдяки розвитку бездротового обладнання в галузі пожежної сигналізації з'явилися нові продукти, що включають різноманітні передавачі, ініціальні пристрої та сповіщувачі. Одним з ключових факторів, який зробив бездротові системи життєздатними для комерційного застосування, є використання літій-іонних акумуляторів, що значно подовжують термін служби пристроїв.

На перший погляд може здатися, що повністю або переважно бездротова система пожежної сигналізації забезпечить власнику значну економію витрат на установку. І з точки зору вартості інсталяції це часто справедливо. Однак специфіка архітектурних особливостей будівель, сертифікованих за стандартами LEED, та сучасні будівельні технології можуть створювати перешкоди для широкого використання бездротових технологій у пожежній сигналізації (див. рис. 1.4). Вогнестійкі бетонні конструкції, підлоги та стелі, а також скляні та сталеві елементи можуть блокувати або знижувати потужність бездротових сигналів, що спричиняє труднощі у підтримці надійного зв'язку з системами безпеки.

Наприклад, вентилі протипожежної спринклерної системи часто розташовуються в зонах виходу на сходові клітини. Такі вентилі часто виготовляються зі сталі та бетону, що може значно послаблювати бездротові сигнали або навіть перешкоджати підтримці постійного зв'язку з обладнанням моніторингу пожежної сигналізації, що розташоване в цих зонах. Проблеми подібного роду часто виявляються тільки під час або після введення системи в експлуатацію, що робить їх вирішення набагато дорожчим.

У зв'язку з цим, технології бездротової пожежної сигналізації повинні впроваджуватися обережно і лише в специфічних ситуаціях. Часто це стосується

обмежених, архітектурно чутливих зон або випадків, коли бездротові технології є єдиним можливим варіантом для вирішення конкретних завдань.

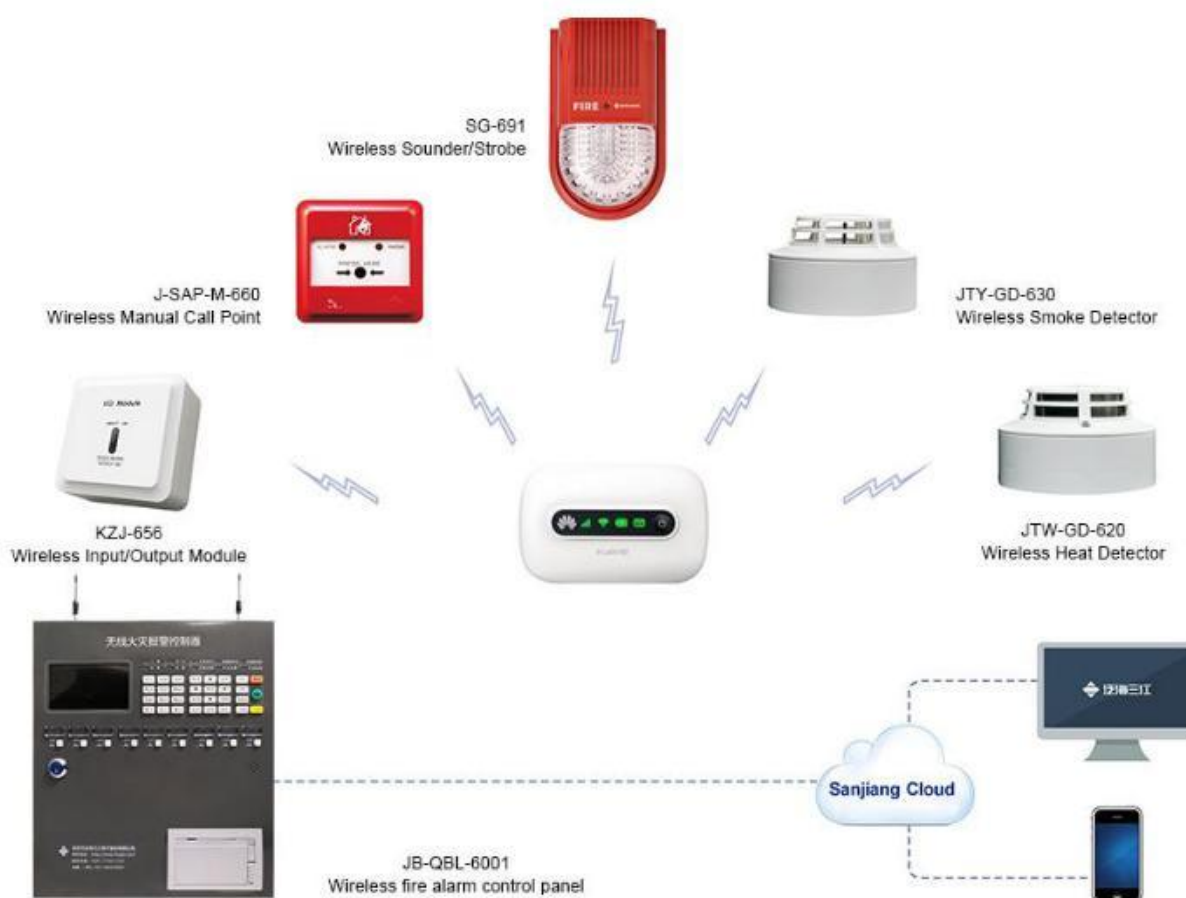


Рисунок 1.4 — Структура бездротової пожежної сигналізації

У таких випадках переваги бездротових технологій можуть бути максимально реалізовані через правильне проектування розташування передавачів і ретрансляторів, а також суворе дотримання рекомендацій виробників щодо установки. Крім того, важливе значення має надійна програма тестування, перевірки та обслуговування системи, оскільки вимагається регулярна заміна акумуляторів і забезпечення стабільної потужності сигналу протягом всього терміну служби пристроїв.

1.1.4 Інноваційні рішення у звітності диспетчерських станцій

Відомо, що звичайні телефонні лінії більше не працюють так, як раніше. Це справді так. Тисячі існуючих систем пожежної сигналізації досі використовують аналогові «стаціонарні» телефонні лінії для зв'язку з віддаленими станціями спостереження або центральними станціями через передавачі цифрової сигналізації (DACT). Хоча ця технологія була ефективною протягом багатьох років, ситуація змінюється. В останніх редакціях NFPA 72, Національного кодексу протипожежної сигналізації та сигналізації, почали віддавати перевагу бездротовим радіомережам, стільниковому зв'язку та технологіям на основі Інтернет-протоколу (IP), що забезпечують значно вищу продуктивність і знижують витрати [5].

Традиційні стаціонарні телефонні лінії (зазвичай дві) мають значні щомісячні витрати на об'єкті. Операторські компанії все частіше намагаються ліквідувати стаціонарні телефонні зв'язки, що змушує шукати альтернативи. Такі альтернативи, як правило, вимагають невеликих початкових витрат, але забезпечують значну економію протягом усього терміну експлуатації. Перехід на нові технології для звітності наглядових станцій може бути економічно вигідним і підвищити ефективність роботи системи.

Як приклад, один заклад використовував стандартне з'єднання DACT через дві телефонні лінії для звітності на станцію спостереження. Коли спрацьовував сигнал тривоги, він передавався на станцію, а потім на пожежну частину для реагування. У середньому цей процес тривав 90 секунд. Однак після відмови від стаціонарних телефонів і переходу на бездротову радіосистему час реагування скоротився до 8 секунд. Це може бути не типовим, але такий результат демонструє значне покращення в продуктивності системи. Крім того, заклад більше не має витрат на телефонні лінії.

Оновлення технології звітування потребує ретельного планування. Перед зміною варто провести дослідження разом із поточними та іншими постачальниками моніторингу, щоб дізнатися, які технології найкраще підходять

для конкретної локації і яке обладнання доступне на станціях спостереження. Якщо планується використання стільникових або радіотехнологій, важливо врахувати потужність сигналу та розташування антен. Всі зміни в технології повинні бути ретельно перевірені для забезпечення стабільного прийому і передачі сигналів.

1.1.5 Новітні технології звукового оповіщення

Системи голосової пожежної сигналізації активно використовуються вже понад 40 років. Деякі з них досі працюють ефективно, однак багато з цих систем були замінені або потребують оновлення. За останні п'ять років з'явився великий вибір голосових систем від різних виробників, спрямованих на виконання все більш складних вимог до таких систем. Незважаючи на перехід від аналогового до цифрового обладнання для обробки сигналів, основні компоненти систем, такі як підсилювачі та обладнання обробки, залишаються без значних змін протягом багатьох років [6].

Це також стосується технології гучномовців для пожежної сигналізації. З розвитком комерційних звукових і комунікаційних технологій, що проникли в галузь пожежної сигналізації, з'явилося більше варіантів щодо підвищення розбірливості звуку.

Пожежні гучномовці мають кілька загальних характеристик у більшості виробників. Використання 4-дюймового паперового конуса динаміка є економічно вигідним і дозволяє компактно розмістити гучномовець. Зазвичай його можна встановити на 4-дюймовий або 4 11/16-дюймовий короб, із можливістю використання подовжувального кільця для полегшення монтажу. Доступні два варіанти напруги (25 VRMS або 70,7 VRMS), що забезпечує універсальність під час вибору підсилювача та довжини проводів. Частота звуку майже завжди знаходиться в діапазоні від 400 до 4000 Гц, а потужність варіюється від 1/4 Вт до 2 Вт, з можливістю розширення до 4 Вт в декількох ступенях потужності. Важливо, що опції 25 VRMS можуть відрізнятися від 70,7 VRMS навіть на одному й тому ж гучномовці.

Крім того, всі гучномовці пожежної сигналізації, що мають сертифікацію UL, побудовані з врахуванням вимог щодо контролю напруги, що дозволяє забезпечити цілісність ланцюга, коли гучномовець не використовується. Це зазвичай здійснюється за допомогою блокуючого діода, що є важливою відмінністю від комерційних аудіодинаміків, які не є взаємозамінними [6].

Одним із значних нововведень у цій сфері є перехід до високоякісних динаміків, що забезпечує значне покращення звуку. Збільшення частотного діапазону гучномовців з 400–4000 Гц до 300–8000 Гц, а в деяких випадках навіть до 200–10 000 Гц, дозволяє значно поліпшити розбірливість голосових сповіщень. Варто зазначити, що частина діапазону людської мови знаходиться вище 4000 Гц, тому збільшення діапазону частот має велике значення для забезпечення високої якості звучання. Однак важливо зазначити, що термін «висока точність» часто використовується як маркетинговий інструмент, і може вказувати на підвищену точність лише на окремих частотах (наприклад, 520 Гц), а не на загальному поліпшенні діапазону частот гучномовця для людської мови.

1.2 Типова структура сучасної пожежної сигналізації

Сучасна система пожежної сигналізації для комерційного використання є невід’ємною складовою забезпечення безпеки життєдіяльності на підприємствах і промислових об’єктах [7]. Такі системи (див. рис. 1.5), що застосовуються у великих комерційних спорудах, можуть мати складну структуру — наприклад, у багатоповерхових будинках або на територіях, що включають кілька корпусів, які потребують централізованого оповіщення про небезпеку. Постачальники подібного обладнання мають постійно впроваджувати новітні досягнення у сфері пожежної безпеки, забезпечуючи сумісну та ефективну роботу всіх елементів сигналізаційної системи.



Рисунок 1.5 — Структура системи пожежної безпеки

Комерційні та промислові системи пожежної сигналізації та безпеки життя зазвичай складаються з п'яти основних елементів, що формують цілісну систему:

- пульт керування пожежною сигналізацією;
- ініціювальні пристрої;
- пристрої сповіщення;
- основне джерело живлення;
- резервне джерело живлення.

Пульт керування пожежною сигналізацією (FACP)

Центральний елемент системи — це панель керування або FACP (Fire Alarm Control Panel), яка виступає «мозковим центром» комплексу. Вона здійснює моніторинг, обробку вхідних сигналів, активацію сповіщення та передачу інформації. При спрацюванні одного з ініціювальних пристроїв, сигнал надходить на FACP, який у свою чергу активує відповідні пристрої сповіщення або запуск тривоги.

Звичайні панелі можуть містити традиційну дротову інфраструктуру з окремими платами для кожної зони. У більш розвинених системах передбачено цифрову архітектуру з можливістю програмування пристроїв і зон, що спрощує управління. Усі FACP надають інформацію про стан системи, включаючи коди несправностей, що дозволяє вручну здійснювати дії, як-от відключення тривоги чи перезавантаження системи після аварійної ситуації. У разі виникнення питань варто звертатися до постачальника системи.

Ініціювальні пристрої активують систему у випадку надзвичайної ситуації. Вони поділяються на ручні та автоматичні.

Дія ручних належать, наприклад, станція ручного спрацювання (pull station), де користувач повинен натиснути кнопку, потягнути важіль або розбити скло для активації сигналізації.

До автоматичних належать детектори диму, газу, тепла або полум'я. Ініціювальні пристрої можуть бути як адресними (визначають точне місце спрацювання), так і неадресними. Існує багато типів датчиків диму, серед яких аспіраційні або променеві. Всі вони подають сигнал на панель FACP для активації тривоги.

Вибір і розміщення таких пристроїв мають відповідати специфіці об'єкта та вимогам безпеки, тож доцільно проконсультуватися з фахівцем або постачальником систем.

Пристрої сповіщення відповідають за повідомлення людей у будівлі про небезпеку. Вони можуть включати:

- стробоскопи;
- сирени;
- гудки;
- дзвони;
- комбінації світлових і звукових сигналів.

Деякі пристрої сповіщення також транслюють голосові повідомлення з інструкціями щодо евакуації. Системи масового оповіщення можуть бути запрограмовані на передачу різних типів повідомлень залежно від типу надзвичайної ситуації.

Основне джерело живлення — це головне джерело електроживлення, від якого залежить стабільна робота всієї системи пожежної сигналізації. Зазвичай до основного джерела належить живлення від електромережі будівлі (наприклад, змінний струм 220 В). Всі елементи системи, включно з пультом керування, ініціювальними пристроями та пристроями оповіщення, підключаються до цього джерела для забезпечення постійної готовності до реагування. У разі припинення подачі електроенергії систему автоматично переводять на резервне живлення.

Резервне джерело живлення забезпечує безперебійну роботу системи у разі відключення основного джерела. Як правило, для цього використовуються акумуляторні батареї або джерела безперебійного живлення (UPS). Вони забезпечують енергоживлення протягом певного часу, що дозволяє системі залишатися функціональною в екстрених ситуаціях. Це критично важливо для збереження можливості оповіщення, контролю та евакуації навіть під час аварійного відключення електроенергії.

1.3 Обмеження і недоліки наявних технічних рішень

На сучасному етапі розвитку технологій більшість випадків загорянь все ще пов'язані з людським фактором — це може бути як необережне поводження з вогнем, так і експлуатація несправного обладнання. Саме тому спостерігається тенденція до повної автоматизації систем пожежної безпеки з метою мінімізації

впливу людини на процес виявлення та гасіння вогню. Сучасні мережеві рішення здатні оперативно виявляти займання, локалізувати джерело пожежі та передавати сповіщення, що суттєво підвищує шанси на збереження життя і майна [8].

Водночас варто усвідомлювати, що, як і будь-які інноваційні розробки, мережеві протипожежні комплекси мають не лише переваги, а й нові типи ризиків. Часто підприємства впроваджують такі технології, не до кінця усвідомлюючи потенційні загрози. Підвищення ефективності, яке дає автоматизація, супроводжується уразливістю до кіберзагроз, що є малоймовірними в традиційних системах. У зв'язку з цим надзвичайно важливо передбачити надійний захист таких рішень та підвищити відповідальність розробників і постачальників програмного забезпечення.

У класичних системах активного пожежогасіння запуск часто вимагає втручання людини — наприклад, натискання кнопки на панелі тривоги. Автоматичні компоненти, такі як димові або температурні детектори, або спринклерні установки, як правило, обмежені певною зоною покриття та потребують фізичного доступу до пульта для керування або відключення.

На відміну від них, мережеві пожежні системи мають низку функціональних переваг. У разі активації тривоги така система може не лише вказати місце події, а й зафіксувати точний час спрацювання. Вони дозволяють створювати зв'язок між окремими сегментами будівлі без прокладання фізичних кабелів, забезпечуючи централізоване дистанційне керування, включно з тестуванням і налаштуванням.

Завдяки широкому впровадженню бездротових IoT-сенсорів мережеві рішення набувають популярності як доступні й технологічно просунуті інструменти протипожежного захисту. Підтримка інтеграції з BIM-платформами дає змогу централізовано керувати всіма елементами системи через єдиний інтерфейс, а також використовувати зібрані дані для оптимізації обслуговування та прийняття рішень [9].

Очевидно, що потенціал мережевих систем у сфері активного пожежогасіння надзвичайно високий, і очікується подальше вдосконалення цих технологій. Ідея,

що системи зможуть самостійно аналізувати ризики, зв'язуватись із пожежними службами, організовувати сервісне обслуговування — поступово переходить з теорії в практику. Водночас слід визнати, що ці системи ще перебувають у процесі розвитку, і їх основною вразливістю залишається програмне забезпечення.

Для функціонування в мережевому середовищі кожен компонент системи — будь то сирена чи димовий датчик — повинен мати вбудований мікроконтролер із прошивкою, що виконує роль спеціалізованого ПЗ. Через відсутність єдиних міжнародних стандартів це програмне забезпечення найчастіше розробляється безпосередньо виробниками «заліза», серед яких значну частку займають компанії з Китаю. На жаль, оновлення таких прошивок відбувається рідко, а рівень їх безпеки часто є недостатнім.

Це може створювати серйозні загрози безпеці: користувачі, які не мають глибоких знань про конкретне обладнання або особливості його налаштування, ризикують залишити "дірки" в системі. Навіть при спробі ізолювати такі системи від Інтернету, багато IoT-компонентів є готовими рішеннями з типовими налаштуваннями, стандартними паролями й застарілою прошивкою, які відкривають можливості для зовнішнього втручання.

Наслідки цього можуть бути критичними. Зловмисник, отримавши доступ до одного пристрою, наприклад до димового сенсора, може використати його як точку входу до внутрішньої мережі підприємства. Це дозволить не тільки викрадати інформацію, а й саботувати функціонування системи безпеки, наприклад, штучно активувати або вимкнути сигналізацію під час реальної пожежі.

Втім, існують способи мінімізації таких ризиків. Один із варіантів — залишитися на традиційних автономних системах, не підключених до мережі. Проте це може обмежити функціональність та втратити переваги сучасних інтелектуальних рішень [9].

Ключову роль у забезпеченні безпеки відіграє усвідомлений вибір надійних виробників обладнання та ПЗ, що мають підтверджену репутацію в галузі кіберзахисту. Багато проблем виникають через прагнення заощадити, що

призводить до використання дешевих пристроїв з погано локалізованими інтерфейсами та неякісною прошивкою.

Окрім технічної безпеки, підприємства повинні приділяти увагу підготовці персоналу — як у сфері експлуатації, так і в питаннях оновлення систем та захисту від онлайн-атак. Як варіант або доповнення, варто інвестувати у засоби пасивного пожежного захисту: протипожежні перегородки, двері, бар'єри, які суттєво підвищують загальний рівень безпеки та сприяють збереженню критичної інфраструктури й безпечній евакуації.

Підсумовуючи, для ефективного функціонування системи протипожежного захисту на основі IoT слід прагнути мінімізації її вразливостей, одночасно забезпечуючи максимальну ефективність виявлення та оповіщення про загрозу. Це дозволить значно скоротити час реакції, забезпечити оперативне гасіння пожежі та зберегти життя людей [10].

1.4 Формулювання вимог до апаратної і програмної частини проєкту

Після аналізу наявних джерел було сформульовано перелік основних вимог до майбутньої апаратно-програмної системи виявлення пожежі:

- компактність конструкції, що забезпечить зручність її встановлення навіть у невеликих приміщеннях або важкодоступних місцях;
- інтуїтивно зрозумілий інтерфейс та загальна простота у використанні, яка дозволить швидко навчити персонал роботі з системою без потреби у спеціальній підготовці;
- високий рівень точності розпізнавання пожежі, що мінімізує кількість хибних спрацювань та дозволяє оперативно реагувати на реальні загрози;
- здатність ефективно виявляти пожежу в радіусі, достатньому для покриття типового приміщення або зони контролю;
- оптимізований розмір програмного забезпечення, який не перевищує технічні обмеження обраної апаратної платформи;

— доступність у фінансовому плані – вартість реалізації проєкту має бути нижчою порівняно з існуючими аналогічними рішеннями на ринку, що дозволить широко впроваджувати систему на підприємствах, в освітніх чи громадських закладах.

Підсумовуючи, можна підсумувати, що було проведено глибоке вивчення та аналіз сучасних методів виявлення пожеж, основних принципів роботи відповідних сенсорів та технічних засобів, що використовуються в системах пожежної безпеки. Розглянуто як класичні, так і сучасні технології, включаючи рішення на базі Інтернету речей (IoT).

Особливу увагу було приділено аналізу типових сенсорів, які використовуються у протипожежних системах, таких як датчики диму, температури, полум'я, а також комбіновані датчики. Для кожного типу було наведено їхні характеристики, принцип дії, переваги та обмеження, що дозволило зробити висновки про їхню доцільність використання у роботі.

Окремим аспектом розгляду стали проблеми, пов'язані з експлуатацією сучасних IoT-систем пожежної безпеки. Було виявлено низку недоліків, зокрема у сфері кібербезпеки, надійності та сумісності компонентів, а також запропоновано низку рішень для мінімізації ризиків та підвищення ефективності таких систем. Запропоновані підходи включають як технічні, так і організаційні заходи.

Також було проведено аналіз аналогічних систем, які вже представлені на ринку. Це дозволило оцінити їх сильні та слабкі сторони, на основі чого було визначено перелік вимог до майбутнього апаратно-програмного комплексу. Ці вимоги включають: компактність, простоту експлуатації, високу точність виявлення пожежі, ефективне покриття зони контролю, відповідність програмної частини апаратним обмеженням та конкурентну ціну.

Таким чином, завершення розділу 1 заклало теоретичне та аналітичне підґрунтя для подальшого розроблення ефективного, доступного та надійного апаратно-програмного комплексу виявлення пожежі із функцією сповіщення користувача за допомогою мобільного застосунку.

2 ОБҐРУНТУВАННЯ СТРУКТУРИ ТА ПРИНЦИПІВ РОБОТИ СИСТЕМИ

У цьому розділі розглянуто загальні принципи побудови мікропроцесорної системи протипожежного сповіщення, обґрунтовано вибір структурних елементів та сенсорів, що забезпечують виявлення загоряння, а також засобів для передачі інформації користувачеві. Основну увагу приділено характеристикам сенсорів полум'я, GSM-модулів та алгоритмам обробки сигналів, які дозволяють забезпечити оперативне виявлення небезпеки та надійне інформування про неї. Запропоновано методику розпізнавання пожежі, яка базується на аналізі даних із сенсорів та логіці прийняття рішення щодо активації системи сповіщення.

2.1 Принципи функціонування сенсорів виявлення полум'я

Сенсори виявлення полум'я є ключовим елементом у сучасних системах протипожежного сповіщення, оскільки забезпечують швидке реагування на появу відкритого вогню. Вони відрізняються від традиційних датчиків диму або температури здатністю оперативно фіксувати характерне електромагнітне випромінювання, що супроводжує процес горіння, що дозволяє значно зменшити час спрацювання та підвищити точність визначення загрози.

Такі сенсори використовуються у багатьох сферах, де необхідний постійний контроль за появою вогню, зокрема в котельних установках, печах, виробничих цехах та інших промислових об'єктах.

Принцип дії датчиків полум'я ґрунтується на реєстрації специфічного випромінювання у відповідному діапазоні спектру. Залежно від цього, розрізняють такі основні типи сенсорів:

Ультрафіолетові (УФ) сенсори фіксують короткохвильове випромінювання в діапазоні 180–250 нм, яке утворюється в початковій фазі займання. Завдяки високій чутливості такі пристрої здатні спрацювати за долі секунди. Однак недоліком є чутливість до сторонніх джерел УФ-випромінювання, що може спричинити помилкові спрацювання.

Інфрачервоні (ІЧ) сенсори орієнтовані на виявлення теплового випромінювання від продуктів горіння. Вони аналізують модуляцію сигналу в ІЧ-діапазоні, що характерна для мерехтливого полум'я. Проте, оскільки інфрачервоне випромінювання можуть створювати й інші джерела тепла, існує ризик хибного спрацювання.

Комбіновані УФ-ІЧ сенсори поєднують обидва підходи, що дозволяє ефективніше відфільтровувати зовнішні завади та підвищити точність виявлення. Завдяки обробці сигналів із двох незалежних каналів, ці сенсори демонструють вищу надійність у складних умовах експлуатації.

Усі зазначені типи сенсорів можуть бути інтегровані в мікропроцесорні системи моніторингу, що забезпечує можливість гнучкого налаштування логіки реагування: активація звукової або візуальної сигналізації, передача повідомлення користувачу, відключення обладнання, перекриття подачі пального або запуск системи пожежогасіння. Таким чином, сучасні сенсори полум'я забезпечують ефективний засіб оперативного виявлення загорянь та реалізації заходів безпеки.

2.1.1 Класифікація сенсорів для виявлення відкритого вогню

Ультрафіолетові датчики полум'я призначені для виявлення ультрафіолетового випромінювання, оскільки багато пожеж супроводжуються значним викидом УФ-випромінювання. Ці датчики особливо ефективні для застосувань, де можуть виникати специфічні загрози, наприклад, під час загоряння металів, галогенів або вуглеводнів. Вони забезпечують високу чутливість на невеликих відстанях, що варіюються в межах 0–50 футів, однак їхня ефективність значно знижується на більших відстанях. УФ-датчики також реагують на електричні розряди, такі як блискавка, що може вплинути на їх точність.

Інфрачервоні датчики полум'я призначені для виявлення інфрачервоного випромінювання, яке виникає внаслідок пожеж. Ці датчики використовують технології аналізу ІЧ-спектра, щоб ідентифікувати характерні шаблони, випромінювані гарячими газами під час пожежі. Вони працюють за

принципом термографічних камер або пристроїв із зарядовим зв'язком (CCD), які виявляють випромінювання в ближньому інфрачервоному діапазоні. Однак важливо зазначити, що вплив водяної пари значно знижує ефективність таких датчиків, оскільки вода поглинає більшу частину інфрачервоного випромінювання. Тому ці датчики можуть мати обмежену ефективність на відкритих просторах, де є високий рівень вологи в повітрі.

Ультрафіолетові та інфрачервоні сповіщувачі полум'я поєднують технології УФ- та ІЧ-датчиків, що дозволяє забезпечити вищу точність у виявленні полум'я. Кожен датчик працює окремо, однак вони інтегровані в єдину систему, що дозволяє оцінювати як УФ-, так і ІЧ-сигнали. Такий підхід значно знижує ймовірність помилкових спрацювань, оскільки кожен з датчиків перевіряє різні аспекти випромінювання, зменшуючи вплив сторонніх сигналів. Ультрафіолетові та інфрачервоні сповіщувачі можуть бути використані як в умовах відкритих просторів, так і в приміщеннях, проте їхня ефективність обмежена типом пожежі, оскільки вони виявляють лише ті пожежі, що випромінюють УФ- або ІЧ-сигнали.

Багатоспектральні інфрачервоні датчики полум'я працюють на основі багатоспектрального інфрачервоного випромінювання (MSIR), використовують кілька спектральних діапазонів для розрізнення полум'я від інших джерел інфрачервоного випромінювання. Ці датчики здатні швидко виявляти пожежі на великих відстанях — до 200 футів як в приміщеннях, так і на відкритому повітрі. Вони можуть точно реагувати навіть на слабкі пожежі з низьким рівнем теплового випромінювання та не викликають помилкових тривог від сонячного світла, штучного освітлення чи інших гарячих об'єктів.

Датчики полум'я IR3 працюють за принципом аналізу випромінювання в трьох різних інфрачервоних спектральних діапазонах, що дозволяє їм ефективно відрізняти реальне полум'я від фонових джерел випромінювання. Зазвичай ці датчики налаштовуються на виявлення випромінювання в спектрі 4,4 мкм, а інші два діапазони знаходяться вище та нижче цього спектру. Така технологія дозволяє

зменшити вплив фонових джерел, таких як інші джерела тепла чи світла, і забезпечує більш точне виявлення полум'я.

2.1.2 Основні характеристики сенсорів

Діапазон виявлення полум'я датчиком залежить від кількох факторів, таких як місце його установки, доступність до детектора та умови навколишнього середовища. Для кращого розуміння, діапазон виявлення полум'я можна побачити на зображенні нижче (див. рис. 2.1).

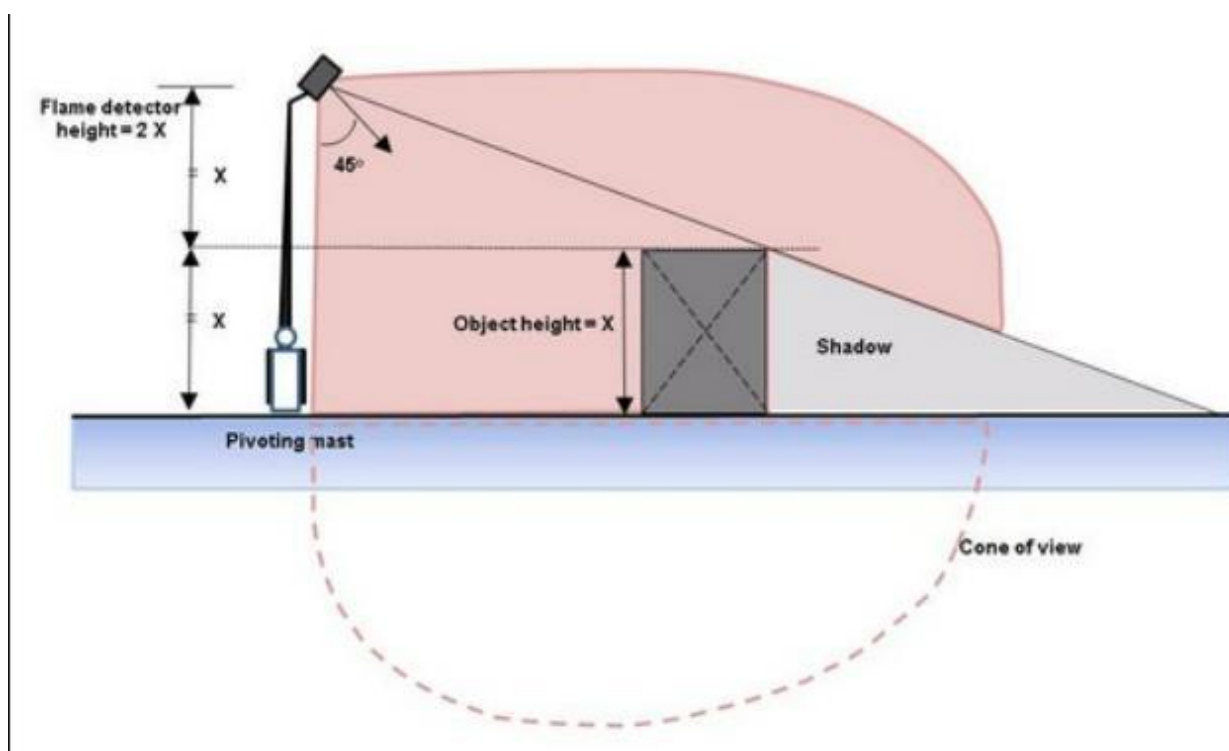


Рисунок 2.1 — Діаграма детекції вогню

Датчик полум'я встановлюється на висоті, яка є вдвічі більшою за висоту об'єкта. Кут нахилу датчика фіксується на 45 градусів для максимального покриття діапазону виявлення.

Триконтактна схема підключення датчика полум'я виглядає так, як показано на рисунку 2.2.



Рисунок 2.2 — Зовнішній вигляд давача полум'я

Призначення виводів:

- Pin1 (VCC): контакт для підключення джерела живлення 5 В;
- Pin2 (GND): контакт для підключення до землі;
- Pin3 (OUT): контакт для цифрового виходу сигналу.

Серед технічних характеристик датчика полум'я зазначено наступне:

- діапазон робочої напруги: від 3,3 В до 5 В;
- робочий струм: 15 мА;
- використовується мікросхема компаратора LM393;
- тип сенсора: фототранзистор YG1006;
- чутливість датчика регулюється за допомогою потенціометра;
- тип виходу: цифровий або аналоговий;
- червоний світлодіод індикуює підключення до живлення, зелений світлодіод сигналізує про наявність вихідного сигналу;
- спектральний діапазон: від 760 нм до 1100 нм;
- кут виявлення полум'я: від 0 до 60 градусів;
- температурний діапазон роботи: від -25 °C до 85 °C;
- розміри плати датчика: 3 см x 1,6 см.

Принципова схема модуля датчика може бути зібрана за допомогою таких компонентів: мікросхеми LM393, фототранзистора YG1006, резисторів (1K для R1 і R3, 10K для R2), потенціометра VR1 (10K), двох керамічних конденсаторів C1 і C2 (по 0,1 мкФ) та двох світлодіодів (червоний D1 і зелений D2). (див. рис. 2.3).

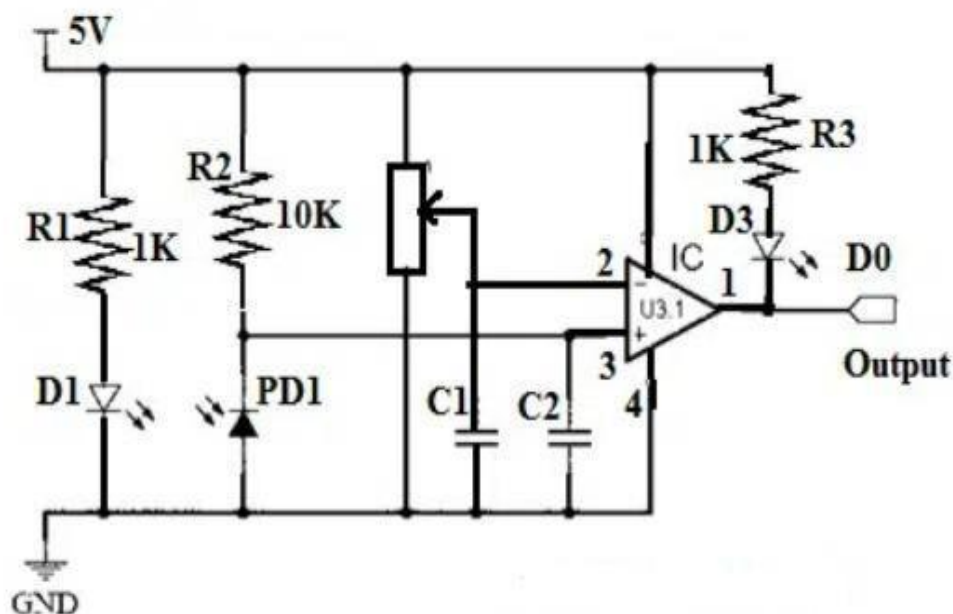


Рисунок 2.3 — Електрична принципова схема давача полум'я

2.1.3 Оцінка використання сенсорів полум'я

Серед численних типів сенсорів, що використовуються в системах пожежної безпеки, датчики полум'я вирізняються рядом вагомих переваг, які забезпечують їхню ефективність у практичному застосуванні.

Однією з головних переваг таких датчиків є висока швидкість реагування. Завдяки особливостям конструкції та принципу роботи, ці пристрої здатні миттєво виявляти наявність відкритого вогню. Це дає змогу своєчасно попередити пожежу, мінімізуючи потенційні збитки для матеріальних цінностей та здоров'я людей.

Наступною суттєвою перевагою є низька ймовірність хибних спрацювань. Датчики полум'я розроблені з урахуванням фільтрації зовнішніх впливів, що дозволяє значно знизити кількість помилкових сигналів, викликаних, наприклад, змінами освітлення або тепловими потоками, які не пов'язані з реальною загрозою пожежі.

Крім того, у порівнянні з традиційними засобами виявлення, такими як датчики диму або температури, сенсори полум'я мають підвищену точність. Вони здатні виявити полум'я навіть на великій відстані, оскільки чутливі до

інфрачервоного або ультрафіолетового випромінювання, що супроводжує горіння. Завдяки цьому забезпечується розширений діапазон дії, що робить їх особливо ефективними для захисту великих відкритих площ або промислових об'єктів.

Також слід відзначити високу надійність та адаптивність до умов навколишнього середовища. Датчики стабільно працюють у різних кліматичних умовах, зберігаючи точність навіть при значних перепадах температури та вологості. Це дозволяє застосовувати їх як у закритих приміщеннях, так і на відкритому повітрі.

Тривалість експлуатації датчиків полум'я також є перевагою. Як правило, такі пристрої мають термін служби до 5 років без необхідності в регулярному обслуговуванні або заміні основних компонентів. Це зменшує витрати на їх утримання у робочому стані. Для порівняння, середній термін експлуатації більшості елементів системи опалення становить від 15 до 30 років, тож оновлення системи виявлення полум'я в межах життєвого циклу об'єкта є цілком виправданим.

Однак, незважаючи на всі переваги, датчики полум'я мають і деякі недоліки, які слід враховувати під час проєктування системи пожежної безпеки.

По-перше, такі сенсори мають обмеження в універсальності: ультрафіолетові (УФ) та інфрачервоні (ІЧ) детектори здатні фіксувати лише ті типи полум'я, які випромінюють відповідні спектри. Це означає, що датчики неефективні при виявленні неуглецевих загорянь, тобто таких, що не супроводжуються яскравим УФ або ІЧ випромінюванням. У результаті, в деяких випадках існує ризик несвоєчасного реагування на пожежу.

По-друге, варто відзначити високу вартість оптичних датчиків полум'я у порівнянні з іншими типами сповіщувачів. Це може обмежити їх застосування у бюджетних проєктах або вимагати комбінованого підходу з використанням декількох типів сенсорів для досягнення необхідного рівня безпеки.

Загалом, датчики полум'я демонструють високий рівень ефективності при правильному застосуванні, однак потребують зваженого підходу до встановлення та налаштування для забезпечення максимальної точності й безпеки.

2.2 Опис принципу роботи GSM-модуля

Глобальна система мобільного зв'язку (GSM) є однією з найпоширеніших технологій мобільного бездротового зв'язку, яка використовується в усьому світі для забезпечення публічного мобільного доступу до телефонного зв'язку та передачі даних. Цей стандарт розроблений для впровадження єдиних протоколів функціонування цифрових мереж стільникового зв'язку другого покоління (2G).

Спочатку GSM функціонувала на основі комутації каналів, однак згодом, завдяки впровадженню технології GPRS (General Packet Radio Service – служба пакетної передачі даних), була додана можливість комутації пакетів, що суттєво розширило функціональність мережі. Основними частотними діапазонами, які використовуються в системах GSM, є 900 МГц та 1800 МГц, хоча в деяких країнах використовуються й інші діапазони.

Архітектура мережі GSM складається з трьох основних підсистем:

- радіопідсистема (BSS);
- підсистема комутації та мережевої взаємодії (NSS);
- операційна та підтримуюча підсистема (OSS).

До радіопідсистеми належать мобільна станція (MS) та підсистема базових станцій (BSS). Мобільна станція зазвичай представлена у вигляді мобільного телефону, що складається з елементів прийому та передавання сигналу, дисплея, мікрофона, динаміка, клавіатури та процесора керування. Головною ідентифікаційною ознакою кожного пристрою є SIM-картка (Subscriber Identity Module) — спеціалізований мікрочіп, який зберігає унікальні ідентифікаційні дані абонента (наприклад, IMSI) та криптографічний ключ (Ki).

Мобільна станція взаємодіє з мережею через радіоінтерфейс, який реалізується за допомогою таких компонентів (див.рис. 2.4).

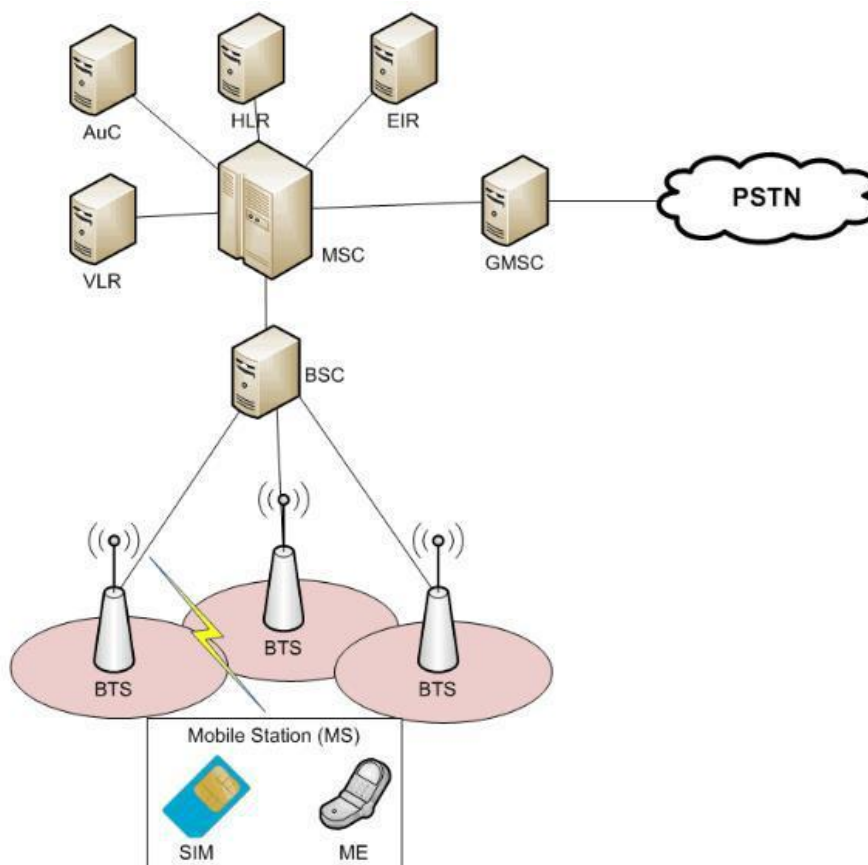


Рисунок 2.4 — Будова мереж GSM

Базова приймально-передавальна станція (BTS) — відповідає за радіозв'язок з мобільними станціями в межах однієї стільникової зони (осередку). Кожна BTS має свій унікальний ідентифікатор і може працювати в різних конфігураціях: стандартна (по одній BTS на комірку), "парасолькова" (одна потужна BTS для покриття великої зони з менш потужними додатковими станціями), а також конфігурація із суміжним розташуванням кількох BTS в одній точці, які охоплюють зону на 120 або 180 градусів кожна.

Контролер базової станції (BSC) — координує та керує роботою кількох BTS, відповідаючи за управління радіоресурсами, передачу викликів, регулювання потужності сигналу та інші функції. Зв'язок між BSC та BTS забезпечується інтерфейсом Abis.

Блок транскодування та адаптації швидкості (TRAU) — забезпечує перетворення форматів мовлення між мережевим середовищем і мобільною станцією. Його основна функція — стискування та розпаковування аудіоданих, що

дозволяє ефективніше використовувати ресурси мережі. Однак, TRAU не обробляє трафік, пов'язаний з передачею даних.

Підсистема мережевої комутації забезпечує встановлення, обробку та маршрутизацію викликів, а також керування користувацькими даними та сервісами. Основні компоненти NSS:

— центр комутації мобільного зв'язку (MSC) — це головний вузол, який виконує функції комутації викликів, взаємодії з іншими мережами (наприклад, PSTN або ISDN), а також підтримує додаткові функції, такі як автентифікація абонента, роумінг, шифрування, управління локаціями користувачів тощо;

— домашній реєстр абонентів (HLR) — велика централізована база даних, у якій зберігаються постійні параметри кожного абонента: номер телефону, послуги, надані користувачу, секретний ключ (Ki), параметри автентифікації, тощо;

— гостьовий реєстр абонентів (VLR) — тимчасова база, яка містить динамічну інформацію про абонентів, що перебувають поза межами своєї домашньої мережі: дані автоматично копіюються з HLR при переміщенні абонента в іншу географічну зону;

— реєстр ідентифікації обладнання (EIR) — база, що зберігає унікальні ідентифікаційні номери мобільних пристроїв (IMEI) і дозволяє блокувати неавторизовані чи вкрадені пристрої.

Система GSM використовує два основні типи технологій мультиплексування: FDMA (Frequency Division Multiple Access) та TDMA (Time Division Multiple Access) (див. рис. 2.5).

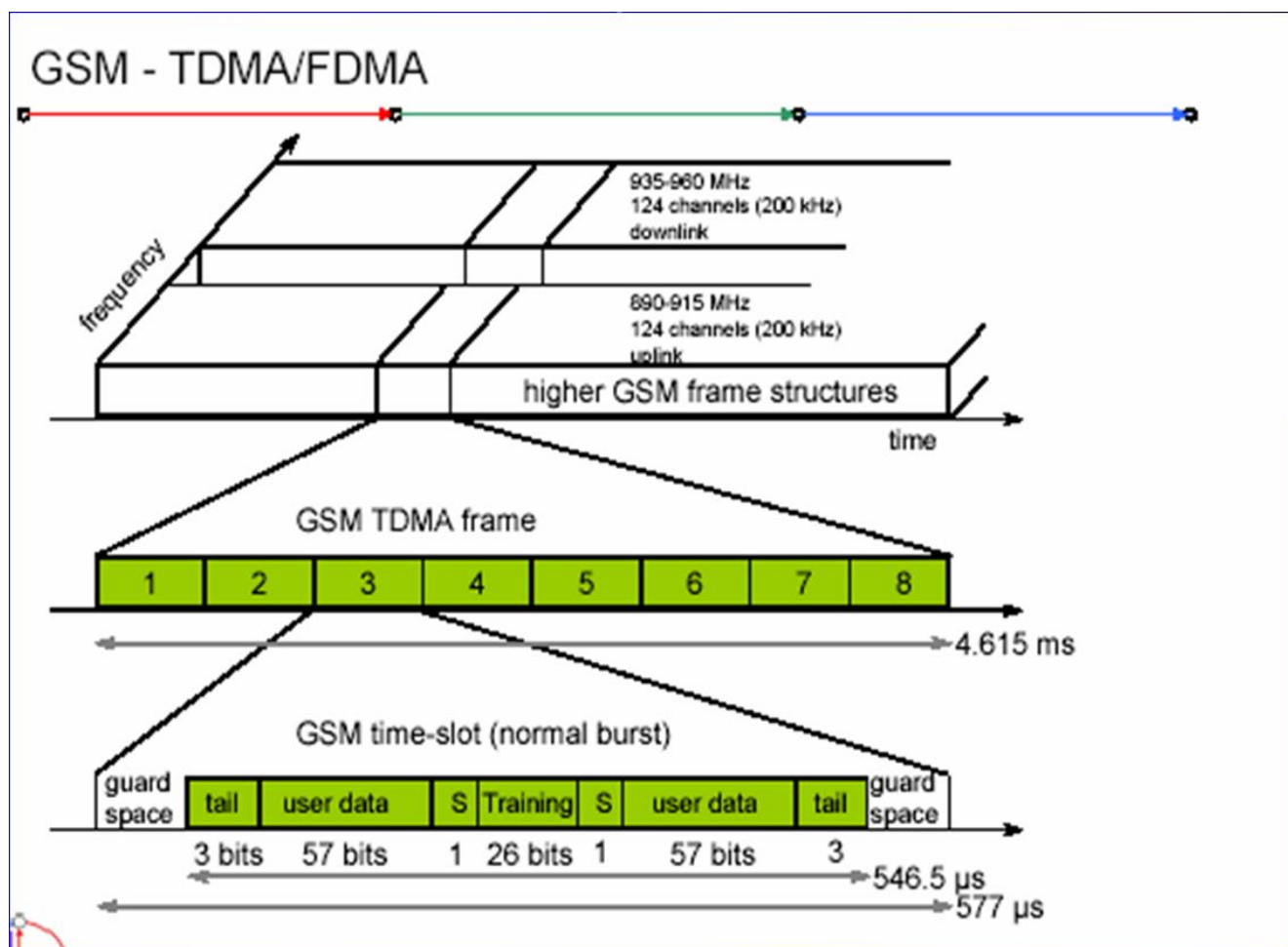


Рисунок 2.5 — Структура слота GSM

FDMA передбачає поділ широкої смуги частот на багато окремих підсмуг. У GSM смуга шириною 25 МГц розділяється на 124 радіоканали по 200 кГц кожен. Кожна BTS може працювати на одному або кількох таких каналах.

TDMA дозволяє кільком абонентам одночасно використовувати один і той самий частотний канал завдяки розподілу часу. Один TDMA-кадр триває 4,615 мілісекунди і містить 8 часових слотів по 577 мікросекунд кожен. Абоненти передають свої дані послідовно в окремих слотах, не заважаючи один одному.

Таким чином, GSM є надійною і масштабованою системою мобільного зв'язку, що забезпечує ефективне використання частотного спектра, високу якість передачі мовлення та безперервну мобільність користувачів завдяки ретельно структурованій архітектурі мережі.

2.2.1 Можливості та обмеження GSM-рішень

Технологія GSM (Global System for Mobile Communications) стала основою мобільного зв'язку у світі ще з кінця XX століття. Незважаючи на появу новіших стандартів, таких як UMTS, LTE або 5G, GSM і досі активно використовується у різних пристроях – від мобільних телефонів до вбудованих систем у сфері IoT, телеметрії, моніторингу та безпеки. У цьому підрозділі розглянемо переваги та обмеження GSM-рішень з технічної та практичної точок зору.

Однією з основних переваг GSM є висока надійність та зрілість технології, яка пройшла десятки років комерційної експлуатації. Вона підтримується переважною більшістю операторів мобільного зв'язку в усьому світі, що забезпечує глобальну сумісність і широке покриття навіть у віддалених або важкодоступних регіонах. Це особливо важливо для пристроїв, які мають функцію передавання критичних повідомлень або сигналів тривоги, наприклад, у системах пожежного або охоронного сповіщення.

Використання SIM-карт забезпечує модульність і гнучкість: абонентська ідентифікація повністю відокремлена від апаратної частини пристрою. Це дозволяє легко змінювати операторів мобільного зв'язку або переносити пристрій між країнами без необхідності перепрошивки чи повторного налаштування модуля. Такий підхід полегшує масштабування системи та обслуговування обладнання.

До важливих переваг також належить підтримка функцій передачі голосу та коротких текстових повідомлень (SMS), які залишаються надійними каналами обміну інформацією у багатьох автоматизованих системах. SMS є корисним для надсилання тривожних повідомлень, підтвердження команд або передачі конфігураційних параметрів без необхідності постійного підключення до Інтернету.

Крім того, GSM-модулі легко інтегруються з мікроконтролерами та одноплатними комп'ютерами (такими як Arduino, Raspberry Pi, STM32 тощо), що значно розширює можливості створення автономних бездротових систем. Імпульсний характер передачі в GSM (через TDMA) дозволяє економити енергію,

що є критично важливим для пристроїв, що працюють від акумуляторів або батарей.

Попри численні переваги, GSM-рішення мають і ряд істотних обмежень. Найпомітнішим є низька пропускна здатність каналу передачі даних – до 14,4 кбіт/с у стандартному режимі CSD та до 85,6 кбіт/с у режимі GPRS, що є недостатнім для передачі мультимедійного контенту, відеопотоків або великого обсягу телеметричної інформації. Через це GSM практично не використовується в застосунках, які вимагають високошвидкісного з'єднання або низької затримки.

Ще однією проблемою є обмеження по дальності – GSM забезпечує стійкий зв'язок лише на відстані до 35 км від базової станції. Це обмежує використання технології в сільській місцевості, гірських районах або пустельних зонах, де базові станції можуть бути рідкісними. Хоча застосування ретрансляторів частково вирішує цю проблему, це вимагає додаткових витрат і технічного обслуговування.

GSM-сигнал може викликати електромагнітні перешкоди для медичних або точних електронних приладів, наприклад слухових апаратів. Унаслідок цього в деяких установах – лікарнях, лабораторіях, аеропортах – діє обмеження або повна заборона на використання пристроїв із GSM-модулями.

Також слід зазначити відсутність наскрізного шифрування користувацьких даних у базовій реалізації GSM. Хоча протоколи автентифікації (наприклад, A5/1) частково захищають з'єднання, вони не забезпечують повної конфіденційності переданих даних у сучасних умовах інформаційної безпеки. Уразливість GSM-мереж до перехоплення та підміни трафіку робить їх непридатними для передавання критичних персональних або фінансових даних без додаткового шифрування на прикладному рівні.

Додатково, існує ризик технологічної несумісності між різними варіантами реалізації GSM у різних країнах або регіонах. Наприклад, діапазони частот, що використовуються у Європі, можуть відрізнятися від тих, які застосовуються в США або Азії, що потребує відповідного вибору апаратної бази при розробці глобальних рішень.

2.3 Методика розпізнавання та діагностики загоряння

Своєчасне виявлення пожежі є ключовим завданням систем протипожежної безпеки, особливо в умовах, де людський фактор не забезпечує оперативного реагування. Сучасні мікропроцесорні системи дозволяють реалізувати автоматизовану методику розпізнавання загорянь на основі аналізу фізичних параметрів навколишнього середовища, таких як температура, дим, рівень газів (зокрема чадного CO, вуглекислого CO₂), полум'я, а також інфрачервоне випромінювання. Нижче приведено основні принципи розпізнавання загоряння

Більшість пожеж супроводжуються кількома типовими ознаками, які дозволяють встановити факт загоряння:

- різке підвищення температури в короткий проміжок часу;
- поява диму, що містить тверді частинки та аерозолі;
- збільшення концентрації чадного або вуглекислого газу;
- інтенсивне інфрачервоне випромінювання від джерела вогню;
- наявність візуального або ультрафіолетового спектру полум'я.

Методика розпізнавання полягає у встановленні нижніх і верхніх порогових значень для кожного з вищезазначених параметрів, з подальшим їх порівнянням із фактичними даними, отриманими від сенсорів. У разі перевищення одного або кількох порогів, система ініціює сигнал тривоги.

Для реалізації алгоритмів діагностики загоряння використовуються такі типи сенсорів:

- температурні датчики (наприклад, термістори, цифрові датчики типу DS18B20, термопари) – дозволяють відслідковувати як загальне нагрівання приміщення, так і різкі стрибки температури, що свідчать про потенційне займання;
- датчики диму (фотоелектричні або іонізаційні) – виявляють присутність диму у повітрі, використовуючи зміну інтенсивності розсіяного світла або іонізаційного струму в контрольованому об'ємі;
- газові сенсори (MQ-2, MQ-7 тощо) – реагують на підвищення концентрації горючих газів або чадного газу;

- датчики полум'я (наприклад, ІЧ-сенсори типу YG1006, або УФ-сенсори) розпізнають наявність відкритого полум'я за спектром випромінювання;

- ультимодальні сенсори — комбіновані датчики, що фіксують кілька параметрів одночасно, підвищуючи точність діагностики.

Алгоритм роботи системи розпізнавання пожежі

У типовій реалізації алгоритм має кілька етапів:

- збір даних із сенсорів у реальному часі з певною періодичністю;
- фільтрація шумів і згладжування показників за допомогою ковзного середнього або експоненційного згладжування;

- порівняння із пороговими значеннями. Якщо значення перевищують норму — активується наступний рівень перевірки.

- оцінка комбінації факторів: наприклад, одночасне підвищення температури та фіксація диму значно підвищує ймовірність того, що має місце загоряння, а не хибна тривога.

- прийняття рішення — система приймає рішення про формування тривожного повідомлення або про ігнорування хибного спрацювання;

- передача сигналу тривоги на центральний контролер, мобільний застосунок або сповіщення користувача за допомогою GSM-модуля чи інших каналів зв'язку.

Оскільки пожежні сенсори можуть реагувати на незначні змінні або не пожежні ситуації (наприклад, дим від кухонної плити або сигарет), важливо передбачити механізми фільтрації хибних тривог. Це можуть бути:

- встановлення часових затримок перед формуванням тривоги (дебаунсінг);

- аналіз декількох показників одночасно;

- врахування контексту (наприклад, розташування пристрою);

- машинне навчання для виявлення нетипових, але небезпечних патернів (у розширених системах);

- періодичне тестування та калібрування/

Щоб система зберігала точність виявлення, необхідно проводити регулярне калібрування сенсорів, особливо газових і димових, які можуть втрачати чутливість через забруднення або старіння. Також доцільно реалізувати автотест системи — короткий діагностичний режим для перевірки працездатності всіх компонентів при запуску або в фоновому режимі.

3 РОЗРОБКА Й ТЕСТУВАННЯ АПАРАТНО-ПРОГРАМНОЇ СИСТЕМИ

3.1 Апаратна складова комплексу

Плата Arduino Nano є однією з компактних моделей мікроконтролерів, розроблених компанією Arduino.cc. Основу цієї плати складає мікроконтролер Atmega328, який також використовується в популярній платі Arduino UNO. Завдяки невеликим розмірам та універсальності, Arduino Nano підходить для багатьох сфер застосування. Серед інших плат сімейства Arduino можна згадати такі, як Arduino Mega, Pro Mini, UNO, YUN, Lilypad, Leonardo та Due. До альтернативних платформ розробки належать також AVR-плати, мікроконтролери PIC, мікрокомп'ютери Raspberry Pi, Intel Edison, плати серії MSP430 Launchpad і ESP32 (див. рис. 3.1).

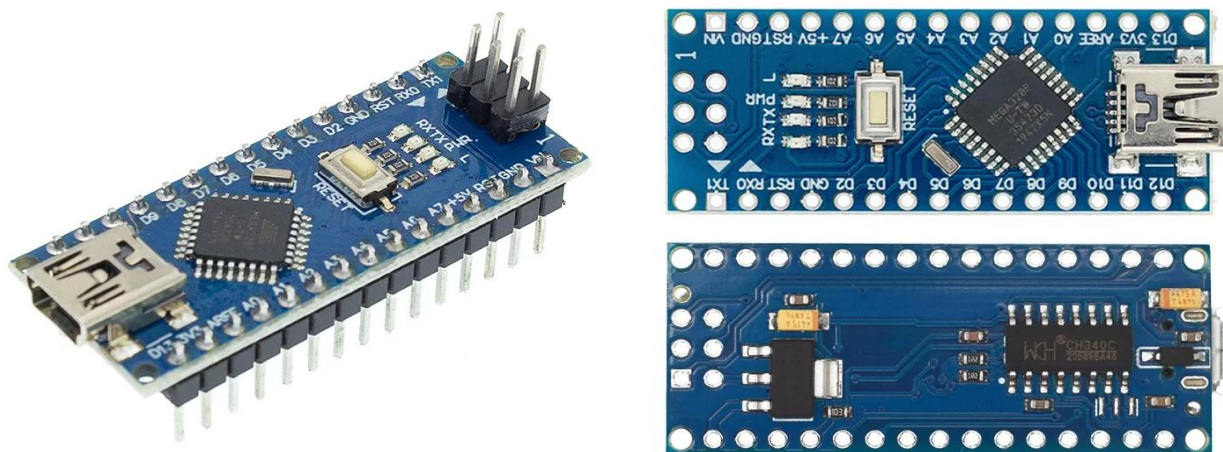


Рисунок 3.1 — Платформа Arduino Nano

На функціональному рівні Nano має схожість з Arduino Duemilanove, хоча й відрізняється форм-фактором. Зокрема, Nano не оснащено окремим гніздом для живлення постійним струмом — живлення здійснюється через mini-USB порт або ж безпосередньо через виводи VCC та GND. Діапазон допустимої напруги живлення становить від 6 до 20 В.

Основні характеристики Arduino Nano:

— тип мікроконтролера: ATmega328P (8-розрядний AVR);

- робоча напруга: 5 В;
- вхідна напруга (V_{in}): від 7 до 12 В;
- кількість цифрових входів/виходів: 22;
- кількість аналогових входів: 6 (від A0 до A5) ;
- загальна кількість цифрових пінів: 14;
- типове споживання струму: 19 мА;
- максимальний струм на один пін введення/виведення: 40 мА;
- обсяг флеш-пам'яті: 32 КБ;
- обсяг оперативної пам'яті SRAM: 2 КБ;
- EEPROM: 1 КБ;
- тактова частота: 16 МГц;
- підтримувані інтерфейси: SPI, I2C (TWI), USART;
- вага: приблизно 7 г;
- габарити: 18 × 45 мм.

Схематичне зображення пінів плати Arduino Nano наведено на рис. 3.2, де кожен вивід виконує конкретну функцію.

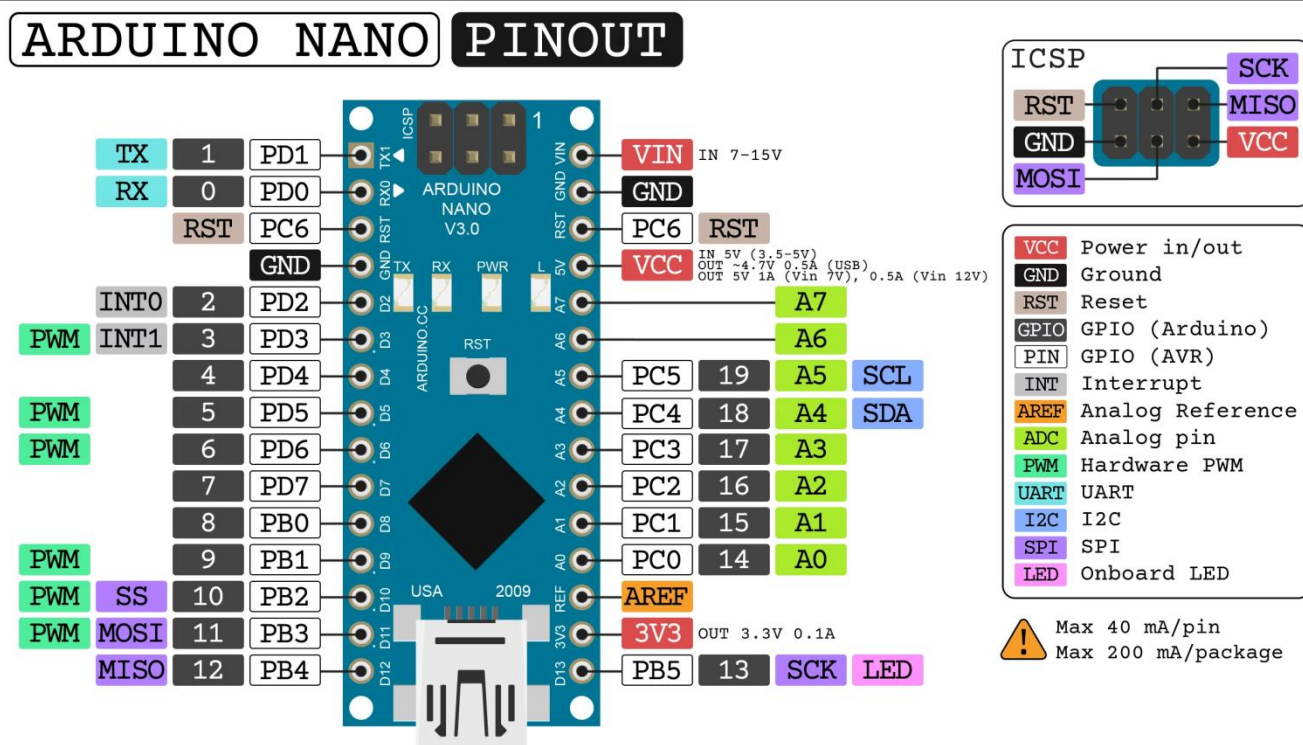


Рисунок 3.2 — Конфігурація пінів плати Arduino Nano

Призначення основних пінів:

- Vin — використовується для підключення зовнішнього джерела живлення з напругою від 7 до 12 В;
- 5V — стабілізована напруга живлення, що подається на саму плату та периферійні пристрої;
- 3.3V — знижену напругу формує внутрішній стабілізатор;
- GND — контакти заземлення;
- RST (Reset) — скидає роботу мікроконтролера;
- A0–A7 — аналогові входи для вимірювання напруги в діапазоні від 0 до 5 В;
- D0–D13 — цифрові контакти, які можуть працювати як входи або виходи;
- Tx, Rx — використовуються для серійної передачі/прийому даних;
- 2, 3 — підтримують зовнішні переривання;
- 3, 5, 6, 9, 11 — контакти для ШІМ (широтно-імпульсної модуляції);
- 10, 11, 12, 13 — SPI-інтерфейс;
- 13 — вивід з вбудованим світлодіодом;
- A4, A5 — інтерфейс I2C;
- AREF — використовується для підключення зовнішньої опорної напруги до АЦП.

3.1.1 Можливості підключення Arduino Nano

Arduino Nano — це компактна та водночас потужна платформа, яка підтримує широкий спектр методів обміну даними з зовнішніми пристроями та системами. В основі плати лежить мікроконтролер ATmega328P, який забезпечує можливості апаратного та програмного серійного зв'язку, а також підтримку інших інтерфейсів, зокрема SPI та I2C.

Одним із базових способів комунікації є послідовний інтерфейс UART, що функціонує через цифрові виводи TX (передача) та RX (прийом). Завдяки цьому підключення Arduino Nano до комп'ютера або іншої плати здійснюється

безпосередньо через USB-кабель за допомогою вбудованого перетворювача UART-USB. В момент передавання чи приймання даних на платі активуються світлодіоди TX і RX, які інформують користувача про роботу інтерфейсу обміну.

У середовищі розробки Arduino IDE користувач може скористатися вбудованим послідовним монітором (Serial Monitor), який дозволяє зчитувати повідомлення з плати та надсилати команди у вигляді текстових рядків. Це особливо корисно для налагодження програмного забезпечення або перевірки роботи датчиків та виконавчих механізмів у реальному часі.

Крім основного апаратного UART, Arduino Nano підтримує створення додаткових програмних серійних портів завдяки бібліотеці SoftwareSerial. Вона дозволяє реалізувати ще один або кілька інтерфейсів UART на будь-яких цифрових пін-контактах. Це дуже зручно у випадках, коли основний UART вже зайнятий підключенням до комп'ютера, а необхідно організувати обмін із модулем GSM, Bluetooth, GPS тощо.

Ще одним важливим каналом зв'язку є інтерфейс SPI (Serial Peripheral Interface), який призначений для швидкого обміну даними між мікроконтролером і периферією. Контакти SPI (MISO, MOSI, SCK, SS) дозволяють підключати модулі пам'яті, дисплеї, зчитувачі карт та інші пристрої з високою швидкістю передавання інформації.

Інтерфейс I2C (або TWI — Two-Wire Interface) — ще одна зручна технологія, що використовується для підключення великої кількості пристроїв, таких як температурні датчики, RTC-годинники, дисплеї та багато іншого. Контакти A4 (SDA) і A5 (SCL) забезпечують обмін даними лише двома лініями, що особливо цінно в умовах обмеженої кількості доступних пінів.

Таким чином, Arduino Nano є надзвичайно гнучким і функціональним рішенням у контексті побудови мікропроцесорних систем, яке дозволяє інтегрувати її в складні багатокомпонентні проєкти. Можливість комбінування кількох типів зв'язку (UART, SPI, I2C) відкриває широкі перспективи для

розробників як у сфері автоматизації, так і в інтернеті речей (IoT), мобільних системах та робототехніці.

3.1.2 Налаштування плати Arduino

Для програмування плати Arduino Nano використовується офіційне середовище розробки Arduino IDE, яке надає користувачам інтуїтивно зрозумілий інтерфейс для написання, компіляції та завантаження скетчів (програм) безпосередньо на мікроконтролер. Після встановлення програмного забезпечення необхідно обрати відповідну модель плати та мікроконтролер. Для цього у меню "Інструменти" (Tools) слід перейти до пункту "Плата" (Board) та обрати "Arduino Nano", після чого вказати тип мікроконтролера — ATmega328P (у класичній або новішій версії).

Arduino Nano постачається з попередньо запрограмованим завантажувачем (bootloader), що дозволяє завантажувати скетчі через USB без необхідності в зовнішньому програматорі. Завантажувач — це невелика програма, яка знаходиться у флеш-пам'яті мікроконтролера та відповідає за прийом коду з комп'ютера через USB-порт. Завдяки цьому можна швидко вносити зміни в програму та перевантажувати її на пристрій без складних процедур.

Комунікація між Arduino IDE та платою Arduino Nano відбувається через послідовний інтерфейс (UART), який реалізується за допомогою протоколу STK500. Передача даних забезпечується через мікросхему-перетворювач USB↔UART, що вбудована в плату, або через зовнішній адаптер FTDI, якщо плата цього не підтримує.

У деяких випадках можлива ситуація, коли необхідно обійти стандартний механізм завантаження через завантажувач. У таких випадках для безпосереднього програмування мікроконтролера використовується метод In-Circuit Serial Programming (ICSP). Це дозволяє завантажити прошивку прямо в пам'ять ATmega328P, мінаючи завантажувач. Для цього застосовується спеціальний

адаптер, наприклад Arduino ISP, який підключається до шести ICSP-пінів (MISO, MOSI, SCK, RESET, VCC, GND) і програмує контролер на низькому рівні.

Таким чином, Arduino Nano є не лише зручною, а й універсальною платформою, що підтримує кілька способів програмування — як через вбудований завантажувач, так і через ICSP-інтерфейс, що робить її придатною для широкого кола застосувань — від навчальних проєктів до промислових прототипів.

3.1.3 Модуль ІЧ-датчика виявлення полум'я

Для реалізації функції виявлення загоряння у системі було обрано інфрачервоний датчик полум'я, що забезпечує надійне виявлення джерел відкритого вогню за рахунок фіксації інфрачервоного випромінювання, яке виникає під час горіння.

Детектор полум'я є спеціалізованим сенсорним модулем, призначеним для фіксації наявності відкритого вогню в зоні його дії. У разі виявлення полум'я датчик може активувати запрограмовану реакцію системи, зокрема — подачу звукового сигналу, ініціацію повідомлення користувачу, а також запуск системи пожежогасіння або відключення лінії подачі пального (наприклад, природного газу чи пропану). У рамках реалізації даної системи цей модуль підключається до плати Arduino для подальшої обробки сигналу (див. рис. 3.3).

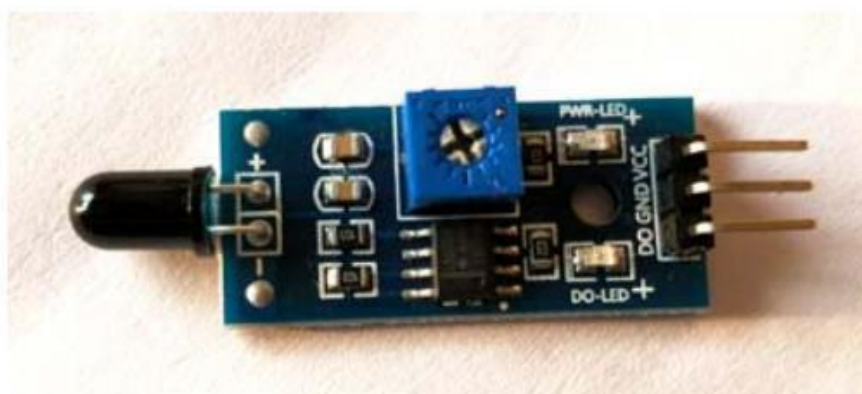


Рисунок 3.3 — Інфрачервоний давач полум'я

Основні технічні характеристики обраного модуля наведені у таблиці 3.1.

Таблиця 3.1 — Технічні параметри інфрачервоного сенсора полум'я

Параметр	Значення
Робоча напруга	3.3 В – 5 В
Споживаний струм	15 мА
Мікросхема компаратора	LM393
Тип сенсора	Фототранзистор YG1006
Спектральна чутливість	760 нм – 1100 нм
Кут виявлення	0–60°
Робоча температура	від -25°C до +85°C
Габаритні розміри	30 мм × 16 мм

Принцип дії сенсора полягає у фіксації інфрачервоного випромінювання, що утворюється під час горіння. Коли в полі зору модуля з'являється полум'я, фотодіод (ІЧ-приймач) реєструє інфрачервоне світло, що викликає зміну напруги на виході. Ця зміна обробляється операційним підсилювачем-компаратором LM393, який формує відповідний логічний сигнал: LOW (0 В) — при виявленні полум'я, та HIGH (5 В) — при його відсутності.

Основа модуля — фототранзистор YG1006, який відрізняється високою чутливістю до інфрачервоного випромінювання і швидкою реакцією. Його кут огляду становить близько 60°, що дозволяє ефективно виявляти джерела полум'я у заданому напрямку. У складі модуля також присутні: резистори, конденсатори, компараторна мікросхема та потенціометр, за допомогою якого можна змінювати чутливість сенсора залежно від умов експлуатації.

Інтерфейс модуля дозволяє підключати його до цифрових входів Arduino та реагувати на зміну логічного рівня, що спрощує його інтеграцію у проєкт. Живлення здійснюється від стандартного джерела постійного струму в межах від 3,3 В до 5 В, що сумісне з більшістю мікроконтролерних платформ.

Таким чином, вибір інфрачервоного датчика полум'я є технічно обґрунтованим завдяки його простоті, доступності, швидкодії та достатньо високій точності для побутових і напівпрофесійних систем виявлення пожеж.

3.1.4 Модуль GSM, його структура та функції

У складі апаратно-програмного комплексу, призначеного для надсилання повідомлень про виникнення пожежі, було використано стільниковий модуль SIM800L, що забезпечує бездротову передачу даних на великі відстані з використанням мереж мобільного зв'язку. Даний модуль вирізняється компактністю, енергоефективністю, сумісністю з більшістю мікроконтролерів, а також підтримкою широкого діапазону частот, що робить його придатним для застосування у глобальному масштабі.

SIM800L дозволяє реалізувати такі функції, як:

- надсилання та приймання SMS-повідомлень;
- здійснення та прийом голосових дзвінків;
- передача GPRS-даних (General Packet Radio Service), що дає змогу організувати базову передачу інформації через Інтернет.

Однією з ключових переваг модуля є його низька вартість та універсальність, що дозволяє ефективно інтегрувати його у пристрої, де важлива автономність та мінімізація витрат.

Після подачі живлення модуль автоматично виконує ініціалізацію: запускається внутрішня прошивка, здійснюється пошук мобільної мережі, а потім — процедура авторизації в операторській мережі. Процес з'єднання та поточний стан модуля сигналізується за допомогою вбудованого світлодіода індикації. Режими його роботи такі:

- відсутність покриття — світлодіод блимає дуже швидко;
- реєстрація в мережі — блимає із середньою частотою;
- успішне з'єднання — повільне миготіння або постійне світло.

Конструктивно модуль виконано у компактному корпусі, який легко інтегрується в електронні пристрої з обмеженим простором. Його габарити становлять лише 25×23 мм (див. рис. 3.4).

Нижче наведено узагальнені технічні характеристики модуля у таблиці 3.2.



Рисунок 3.4 — Зовнішній вигляд модуля GSM SIM800L

Таблиця 3.2 — Технічні параметри модуля SIM800L

Параметр	Значення
Напруга живлення	3,8 В – 4,2 В
Рекомендована напруга живлення	4 В
Споживання у сплячому режимі	< 2,0 мА
Споживання в режимі очікування	< 7,0 мА
Споживання при передачі (середнє)	≈ 350 мА
Споживання при передачі (пік)	до 2000 мА
Розміри модуля	25 × 23 мм
Інтерфейс зв'язку	UART (TTL 2,8 В), AT-команди
Підтримка частот	Quad Band: 850 / 900 / 1800 / 1900 МГц
Робочий температурний діапазон	від -40°C до +85°C

Для взаємодії з мікроконтролером Arduino модуль використовує UART-інтерфейс з підтримкою передачі та прийому даних на рівні логіки 2,8 В. Керування відбувається за допомогою AT-команд — набору текстових інструкцій, які дозволяють виконувати такі операції, як встановлення зв'язку, передача повідомлень, отримання сигналу мережі тощо.

Особливу увагу при інтеграції модуля слід приділити живленню, оскільки при передачі GSM-сигналу модуль може короткочасно споживати струм до 2 А, що

потребує використання стабільного джерела живлення з відповідним запасом потужності.

Таким чином, модуль SIM800L є оптимальним вибором для бездротового обміну інформацією у проектах з Arduino, що потребують мобільного зв'язку, особливо у контексті сповіщення про пожежу або надзвичайні ситуації.

3.1.5 Організація живлення системи

Для живлення системи було вибрано літій-іонний акумулятор LP18650A. Елементи живлення, що використовуються в електрохімічній схемі Li-SOCL2, забезпечують тривалий термін служби при температурах від -55° до 85° [18].

На рис. 3.5 представлено зовнішній вигляд обраного джерела живлення.



Рисунок 3.5 — Літій-іонний акумулятор для живлення плати

У табл. 3.4 подано характеристики джерела живлення.

Таблиця 3.4 — Характеристики Li-SOCL2 джерела живлення

Параметр	Значення
Ємність	2400 мА/год

Найвища робоча температура	85° C
Найнижча робоча температура	-55° C

3.3 Розробка прототипу системи

Перед безпосереднім виготовленням прототипу системи моніторингу місцезнаходження було виконано етап проєктування апаратної частини з використанням спеціалізованого програмного забезпечення Fritzing. Це дозволило провести попереднє моделювання функціональності системи, виявити потенційні помилки у з'єднаннях компонентів та оптимізувати їх розміщення ще до збирання на макетній платі. Такий підхід значно підвищує ефективність розробки та знижує ризик помилок при подальшому складанні пристрою.

Fritzing — це інтуїтивно зрозумілий інструмент, орієнтований як на початківців, так і на досвідчених розробників у сфері електроніки. Він дозволяє створювати візуальні макети електронних схем, використовуючи інтерфейс перетягування компонентів на віртуальну плату. Програма підтримує кілька режимів роботи: макетну схему, принципову електричну схему та вигляд друкованої плати. Це забезпечує цілісний підхід до розробки – від ідеї до готового пристрою.

У бібліотеці Fritzing міститься широкий спектр електронних компонентів: мікроконтролери (наприклад, ESP32 або Arduino), модулі зв'язку (Wi-Fi, LoRa, Bluetooth), сенсори, елементи живлення, кнопки, резистори, світлодіоди, реле та багато іншого. Користувач має можливість налаштовувати параметри компонентів, створювати власні бібліотеки та експортувати схеми у популярних форматах для подальшої розробки або виготовлення.

Процес проєктування у Fritzing почався з формування логічної структури системи, зокрема з'єднання Arduino Nano, ІЧ-модуля, GSM-модуля, контролера живлення та акумулятора. Усі ці елементи були розміщені на віртуальній макетній платі з дотриманням реального масштабування та топології з'єднань. Це дозволило

ще до фізичної реалізації оцінити просторове розміщення компонентів та забезпечити ергономічність плати.

Після фіналізації схеми було сформовано макетну модель пристрою, яка послужила основою для переходу до наступного етапу — збирання прототипу. На рисунку 3.6 представлено остаточний вигляд макетної схеми, розробленої в середовищі Fritzing, що демонструє повне компонування електронної частини системи.

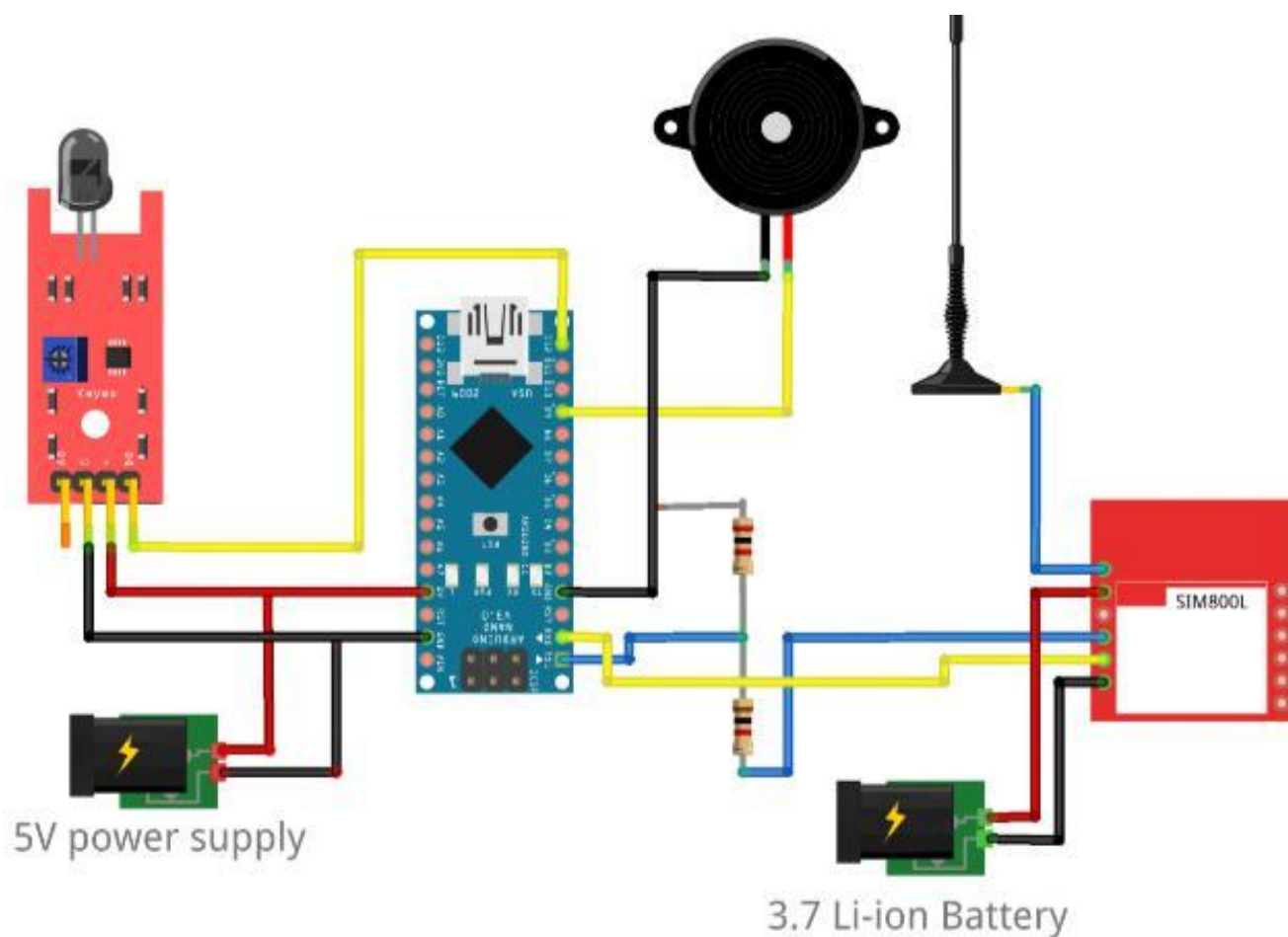


Рисунок 3.6 — Функціональна схема прототипу

3.4 Створення програмного забезпечення

Перед тим як перейти до реалізації програмного забезпечення для апаратно-програмного комплексу, було створено блок-схему алгоритму його роботи. Для цього використано зручне онлайн-середовище draw.io, яке дозволяє візуалізувати логіку програмних процесів у вигляді зрозумілих діаграм. Такий підхід є важливим етапом проєктування, адже дозволяє заздалегідь опрацювати послідовність дій системи, виявити логічні помилки та оптимізувати процеси взаємодії між модулями.

На рисунку 3.8 представлено алгоритм функціонування програмної частини комплексу, розроблений у draw.io.

Як видно зі схеми, робота комплексу починається з перевірки наявності належного живлення. Цей крок є критичним, оскільки недостатнє або нестабільне живлення може спричинити некоректну роботу мікроконтролера або підключених модулів. Якщо живлення відповідає вимогам, виконується етап ініціалізації основних модулів системи — інфрачервоного сенсора полум'я та GSM-модуля, який відповідає за зв'язок із зовнішніми користувачами.

Наступним кроком у алгоритмі є калібрування підключених датчиків. Це дозволяє забезпечити більш точне зчитування параметрів навколишнього середовища, що є критично важливим для своєчасного виявлення пожежі. Після цього система переходить до основного циклу — безперервного моніторингу стану за допомогою датчика полум'я. Якщо протягом зчитування ознак займання не зафіксовано, алгоритм повертається до етапу повторної перевірки, утворюючи цикл постійного спостереження.

У випадку виявлення ознак пожежі активується наступна послідовність дій: передача відповідного повідомлення через GSM-модуль, надсилання інформації до мобільного застосунку користувача, а також формування сигналу для відповідних аварійно-рятувальних служб. Отримання підтвердження про доставку сповіщення завершує основний логічний блок — система вважає свою роботу успішною, оскільки виконано головну мету: виявлення та передача критичної інформації.

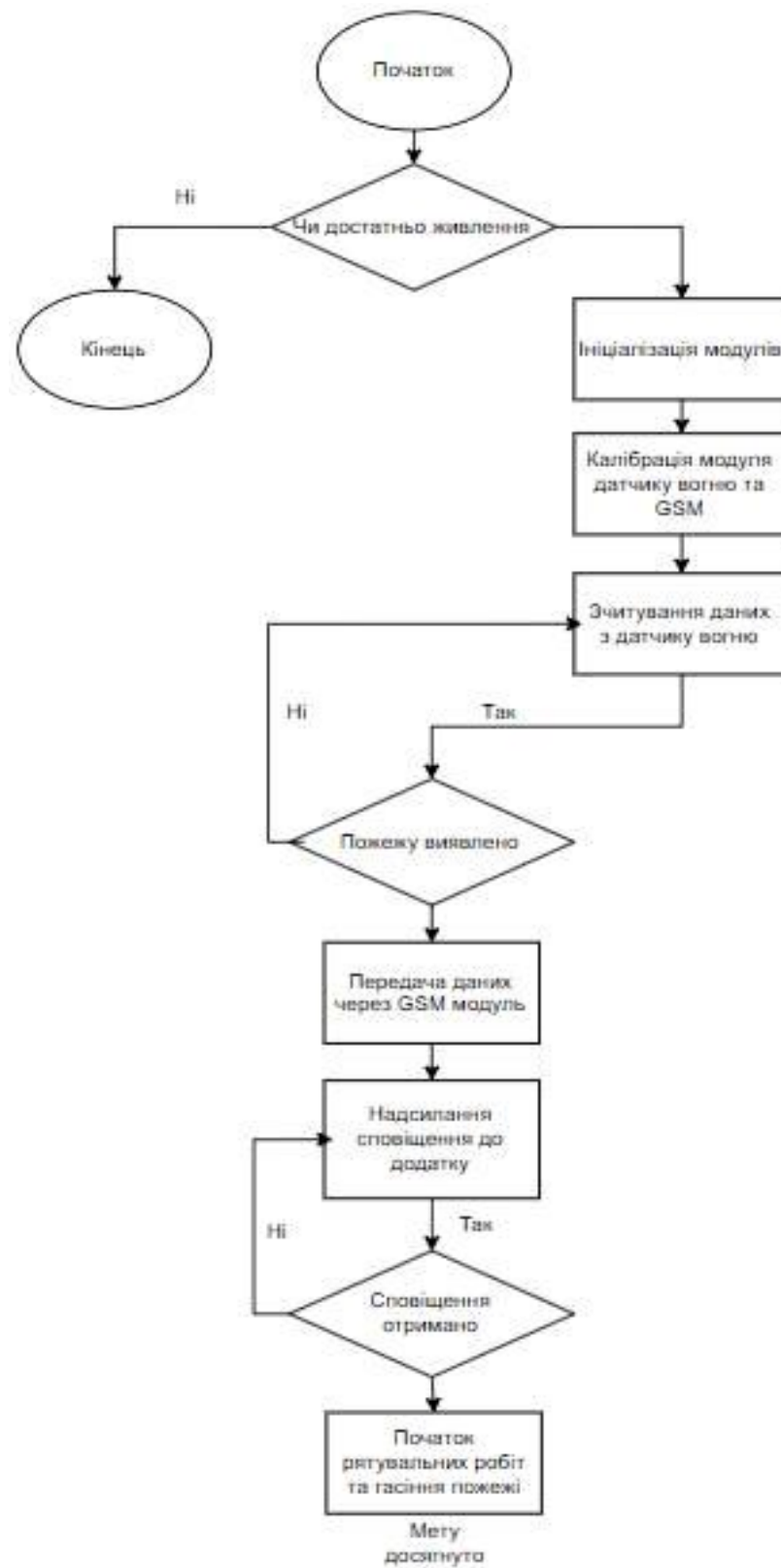


Рисунок 3.8 — Алгоритм роботи програми

Реалізація такої структурованої логіки дозволяє досягти високої надійності та оперативності роботи системи в умовах реального часу, що є необхідним для системи виявлення пожеж.

3.4.1 Мова програмування

Для створення програмної логіки апаратно-програмного комплексу було обрано мову програмування C, яка є основною для платформ мікроконтролерів, зокрема Arduino Nano.

Застосування мови C у поєднанні з Arduino має низку вагомих переваг, що визначають її популярність серед розробників вбудованих систем:

Мова програмування C є незалежною від конкретної апаратної архітектури. Завдяки цьому код, написаний на C, легко переноситься між різними пристроями та платами, що суттєво спрощує масштабування та адаптацію проекту до інших платформ.

Мова підтримує чітку структурну організацію коду з використанням блочних конструкцій та фігурних дужок. Це не лише полегшує читання коду, а й сприяє модульності: кожна функція виконує чітко визначене завдання, що підвищує керованість та надійність програмного забезпечення.

C є однією з найбільш розповсюджених мов програмування у сфері мікроконтролерної техніки. Для неї доступна велика кількість бібліотек, прикладів та інструментів, що дає змогу легко взаємодіяти з різноманітними периферійними модулями: датчиками температури, вологості, полум'я, GPS, GSM тощо.

C дозволяє здійснювати динамічний розподіл пам'яті, що особливо корисно для систем із обмеженими ресурсами. Програміст має можливість виділяти або звільняти пам'ять залежно від актуальних потреб програми, що сприяє ефективному її використанню.

Оскільки C є компільованою мовою, вона забезпечує високу швидкість виконання коду. Це критично важливо для реального часу та систем, які повинні реагувати миттєво на зміни середовища, як у випадку виявлення займання.

Таким чином, вибір мови C для реалізації програмної частини комплексу є логічно обґрунтованим: вона забезпечує високу ефективність, простоту інтеграції з апаратними модулями та дозволяє створювати надійні та швидкодіючі рішення для систем виявлення та оповіщення про пожежу.

3.4.2 Середовище для розробки

Для реалізації програмної частини апаратно-програмного комплексу було використано Arduino IDE — інтегроване середовище розробки, яке спеціально створене для роботи з мікроконтролерами Arduino.

Arduino IDE (Integrated Development Environment) — це кросплатформене програмне забезпечення з відкритим вихідним кодом, яке дозволяє створювати, редагувати, компілювати та завантажувати програмний код безпосередньо на плату мікроконтролера. Платформа підтримує операційні системи Windows, macOS та Linux, що забезпечує широке охоплення серед розробників і ентузіастів електроніки.

Програмний код, який створюється в Arduino IDE, має спеціальне позначення — скетч (англ. *sketch*). За замовчуванням усі скетчі зберігаються у файлах з розширенням `.ino`, і кожен такий скетч є незалежним програмним модулем. Важливою перевагою IDE є її здатність працювати з багатофайловими проектами: кожен файл відображається на окремій вкладці інтерфейсу. Окрім основних файлів скетчу, середовище підтримує також файли з розширеннями `.c`, `.cpp`, `.h`, що дозволяє використовувати більш гнучку та масштабовану структуру коду.

Перед компіляцією всі основні файли скетчу (`.ino`, `.pde`) автоматично об'єднуються в єдиний компільований файл у відповідному порядку вкладок. Інші типи файлів залишаються без змін і компілюються окремо.

На рис. 3.9 зображено зовнішній вигляд середовища розробки Arduino IDE, що використовувалося для написання коду системи виявлення пожежі.

Важливу роль у створенні повноцінного коду відіграють бібліотеки, які розширюють базову функціональність Arduino IDE. Бібліотеки дозволяють легко

працювати з периферійними пристроями, такими як датчики, дисплеї, модулі зв'язку тощо.

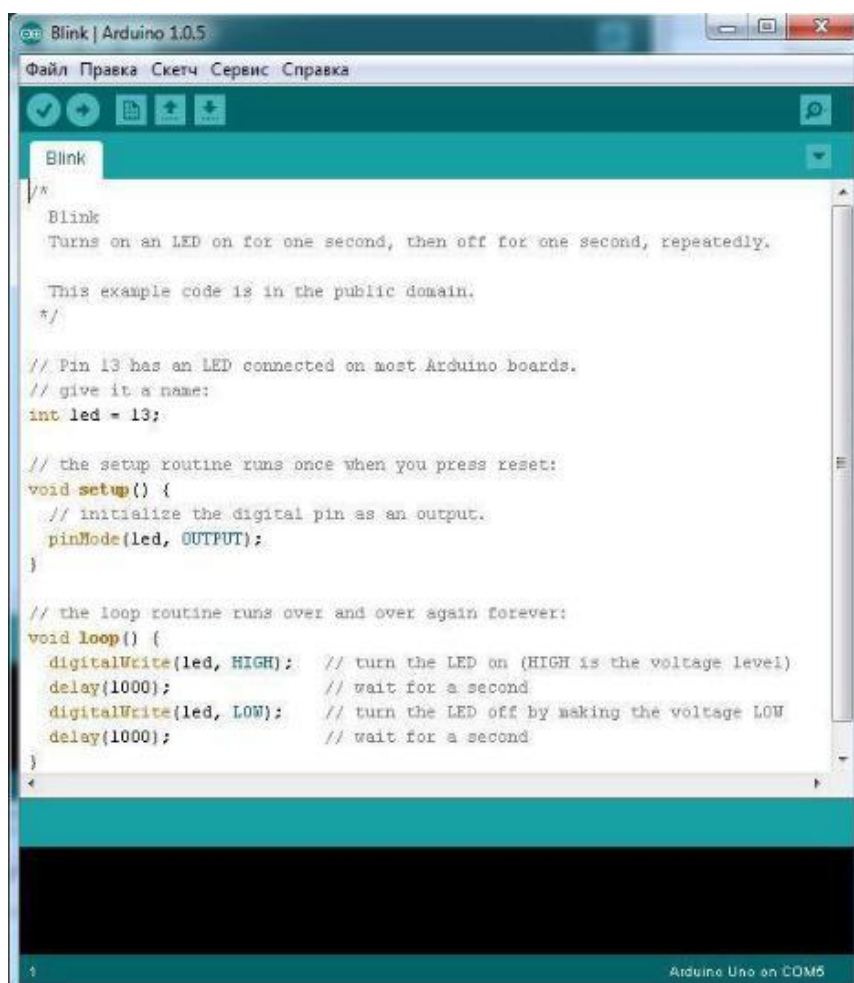


Рисунок 3.9 — Інтерфейс середовища розробки Arduino IDE

Для підключення бібліотеки достатньо скористатися меню «Скетч» → «Імпортувати бібліотеку», після чого у верхній частині скетчу з'являється директива `#include`, яка забезпечує підключення необхідного модуля. Усі бібліотеки компілюються разом зі скетчем і завантажуються у пам'ять мікроконтролера. У разі, якщо бібліотека більше не використовується, її можна видалити, просто прибравши відповідні директиви підключення.

Таким чином, Arduino IDE є простим у використанні, але потужним середовищем розробки, яке ідеально підходить для проєктування вбудованих систем на базі Arduino.

3.4.3 Застосування бібліотеки `softwareserial`

Плати Arduino, зокрема моделі на базі мікроконтролера Atmega328P, мають вбудовану апаратну підтримку для реалізації послідовного обміну даними (Serial Communication) через стандартний інтерфейс UART (Universal Asynchronous Receiver/Transmitter). Передача і прийом даних за цим інтерфейсом здійснюється через цифрові контакти 0 (RX) та 1 (TX). Ці ж контакти використовуються для програмування плати через USB-інтерфейс, оскільки конвертер USB-to-Serial вбудований в Arduino Nano або інші моделі.

Вбудований UART дозволяє апаратно забезпечити надійну передачу та обробку даних у фоновому режимі. Це означає, що основний мікроконтролер здатен приймати і обробляти послідовні дані навіть тоді, коли він виконує інші задачі. Це суттєво підвищує ефективність та стабільність роботи систем, у яких задіяно кілька периферійних пристроїв, що працюють через UART (наприклад, модулі GSM, Bluetooth, GPS тощо).

Однак, оскільки Arduino має лише один апаратний послідовний порт, виникає необхідність у створенні додаткових віртуальних послідовних з'єднань. Для цього використовується спеціальна бібліотека `SoftwareSerial`, яка дозволяє програмно реалізовувати UART-подібний інтерфейс на будь-яких вільних цифрових пінках плати.

Бібліотека `SoftwareSerial` дозволяє розробнику призначити довільні виводи для передачі (TX) та прийому (RX) даних, створивши цим самим нові логічні послідовні порти. Підтримується робота з швидкостями обміну до 115200 бод, хоча оптимальними вважаються значення до 9600 або 38400 бод для забезпечення надійності.

Крім того, бібліотека підтримує інверсію сигналу, що є корисним для взаємодії з модулями, які використовують нестандартну логіку (наприклад, де логічна «1» передається як низький рівень сигналу). У таких випадках параметр `inverse_logic` дозволяє автоматично адаптувати сигнал відповідно до вимог підключеного пристрою.

Завдяки поєднанню апаратного UART та програмної реалізації через `SoftwareSerial` можна одночасно працювати з кількома пристроями, що комунікують через послідовний інтерфейс, навіть на обмежених платах типу `Arduino Nano`.

3.4.4 Використання бібліотеки `string.h`

У мові програмування C рядки реалізуються як масиви символів, завершені нульовим символом (`'\0'`), який вказує на кінець рядка. Для роботи з такими рядками в стандартній бібліотеці мови C передбачено заголовочний файл `<string.h>`, який містить велику кількість функцій для ефективного обробки текстової інформації.

Бібліотека `<string.h>` надає набір функцій для виконання різноманітних операцій над рядками, зокрема:

- порівняння рядків (функції `strcmp()`, `strncmp()`) дозволяє визначити, чи два рядки ідентичні;
- копіювання рядків (`strcpy()`, `strncpy()`) дає змогу перенести значення одного рядка в інший;
- об'єднання рядків (`strcat()`, `strncat()`) використовується для конкатенації (з'єднання) двох рядків в один;
- обчислення довжини рядка (`strlen()`) допомагає визначити кількість символів у рядку;
- пошук символів або підрядків (`strchr()`, `strstr()`) дозволяє знаходити певний символ або підрядок у більшому рядку.

Окрім операцій із символами, бібліотека `string.h` також містить функції для операцій з пам'яттю, зокрема:

- `memcpy()` — копіює блок пам'яті;
- `memset()` — заповнює блок пам'яті певним значенням;
- `memcmp()` — порівнює блоки пам'яті.

Ці функції широко використовуються не лише в роботі з текстовими даними, а й у керуванні динамічною пам'яттю, зокрема в системах з обмеженими

ресурсами, як-от мікроконтролери Arduino. Знання і правильне застосування функцій з бібліотеки `string.h` є обов'язковим для ефективного написання програмного забезпечення на мові C.

Особливо актуально це для мікропроцесорних систем, у яких потрібно швидко та економно обробляти текстові повідомлення, наприклад, дані для SMS, які передаються через GSM-модуль або команди, що надходять від користувача через UART.

3.5 Реєстрація облікового запису у ThingSpeak та конфігурація системи

Для створення прототипу апаратно-програмного комплексу та тестування роботи системи виявлення пожежі та надсилення сповіщень було обрано онлайн-платформу ThingSpeak [21].

ThingSpeak™ — це аналітична хмарна платформа для Інтернету речей (IoT), яка забезпечує можливість агрегації, візуалізації та аналізу поточних даних у реальному часі. Платформа дозволяє отримувати миттєвий доступ до даних, що надсилаються пристроями, а також виконувати обробку даних за допомогою вбудованого середовища MATLAB®. Завдяки цьому, ThingSpeak активно використовується для створення прототипів IoT-рішень та перевірки концепцій, що вимагають аналітики (див. рис. 3.10).

Основні можливості платформи ThingSpeak включають:

- просту інтеграцію з пристроями, які надсилають дані за допомогою популярних IoT-протоколів;
- відображення даних датчиків у режимі реального часу;
- імпорт даних із зовнішніх джерел на запит;
- обробку й аналіз даних за допомогою середовища MATLAB;
- автоматичне виконання аналітичних сценаріїв за розкладом або на основі подій;
- можливість реалізації повноцінних IoT-систем без необхідності налаштовувати власний сервер чи веб-інтерфейс;

— реалізацію реакції на події з використанням сторонніх сервісів, таких як Twilio® чи Twitter®.

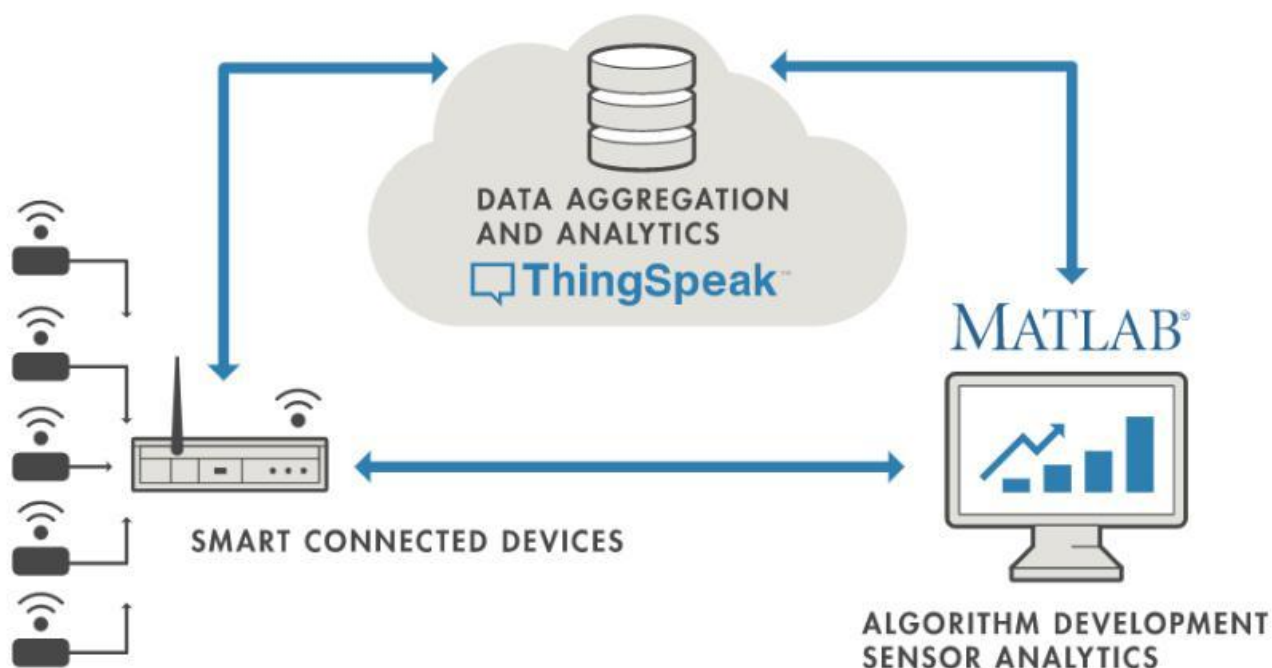


Рисунок 3.10 — Архітектура ThingSpeak

Реєстрація та налаштування каналу в ThingSpeak:

Спочатку було створено обліковий запис MathWorks на сайті <https://thingspeak.com> (див. рис. 3.11).

My Profile

Email: [redacted]@gmail.com
[Edit MathWorks Account Settings](#)

Time Zone: (GMT-05:00) Eastern Time (US & Canada) ▼

Username: mwa0000029213224
[Edit](#)

Help

Account Settings:

- MathWorks Account email and password are needed to sign in to ThingSpeak.
- If you edit your MathWorks Account settings, you will need to sign out of ThingSpeak and log back in.
- Your username is displayed as the author of your public channels.
- Your username must be 6-27 characters, containing only letters and numbers.
- Time Zone is used when displaying data in your charts, and when scheduling your ThingSpeak apps.
- User API key is required to create and manage channels using the [REST API](#).

Рисунок 3.11 — Створення облікового запису MathWorks

Після авторизації у сервісі ThingSpeak було натиснуто кнопку «New Channel», після чого вказано назву проєкту та описано поля для збору даних. Дані збережено натисканням «Save Channel» (див. рис. 3.12).

Рисунок 3.12 — Створення проєкту для збору даних

У результаті була створена окрема сторінка каналу, яка представляє систему виявлення пожежі — основну складову для подальшого прототипування (див. рис. 3.13).

Рисунок 3.13 — Сторінка проєкту

Для перевірки працездатності комплексу було створено віджет, який імітує візуальний відгук на подію — коли датчик полум'я фіксує наявність вогню та надсилає сигнал у систему, лампа загоряється зеленим кольором (див. рис. 3.14).

Configure widget parameters ? x

Name

Condition If

▼

▼

turn Lamp ON

Update Interval second(s)

Color

Рисунок 3.14 — Вікно для контролю пожеж

3.6 Підключення мобільного додатку до пристрою для отримання повідомлень

Для реалізації функції повідомлення користувача про початок пожежі було обрано сервіс Pushsafer. Pushsafer — це платформа для миттєвого надсилання push-сповіщень на мобільні пристрої (iOS, Android), а також настільні системи (Windows 10, Chrome, Firefox) з різних джерел, зокрема, з проєктів на базі Arduino. Надсилання повідомлень можливе як через шлюз електронної пошти, так і через

власне API, що забезпечує широку інтеграцію з програмним забезпеченням будь-якого типу [22].

Для тестування процесу надсилання сповіщень було обрано мобільний додаток Pushsafer, встановлений на смартфон (див. рис. 3.15).

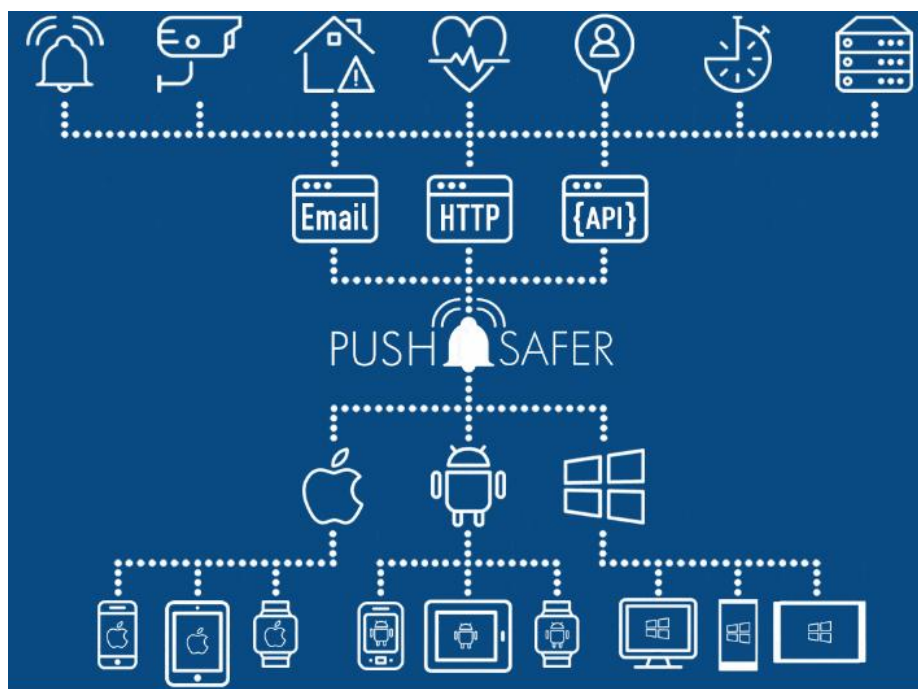


Рисунок 3.15 — Мобільний додаток Pushsafer

На наступному етапі в додатку було створено обліковий запис користувача, що дозволило налаштувати канал отримання сповіщень із розробленого апаратно-програмного комплексу (див. рис. 3.16).

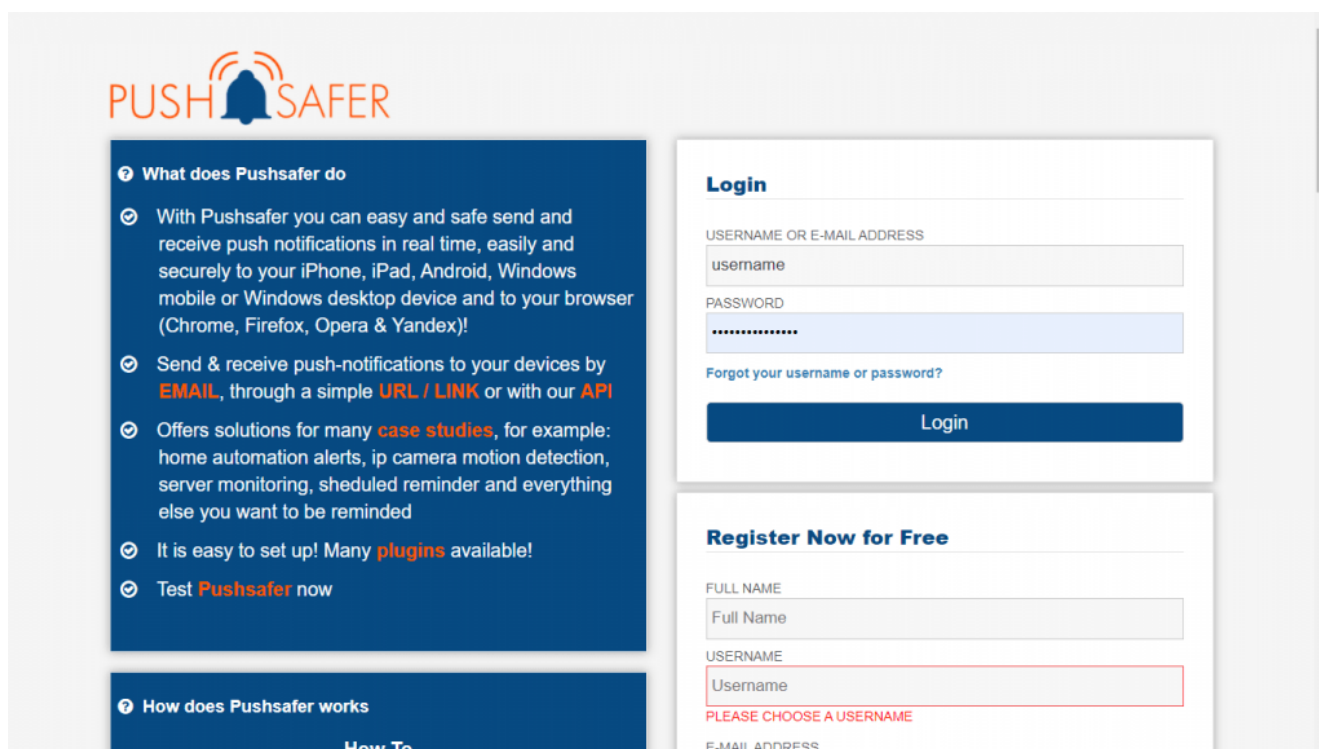


Рисунок 3.16 — Створення облікового запису користувача

У результаті реєстрації було успішно створено обліковий запис у Pushsafer, а також додано пристрій до списку девайсів мобільного застосунку. Таким чином, користувача було поінформовано, що розроблений пристрій здатен отримувати та обробляти сповіщення про початок пожежі у реальному часі (див. рис. 3.17).



Рисунок 3.17 — Сповіщення про початок пожежі у реальному часі

З'єднання апаратно-програмного комплексу з Pushsafer відбувається за наступним алгоритмом:

- отримання Private or Alias Key після реєстрації у Pushsafer;
- використання HTTP-запиту через API для відправлення push-повідомлення;
- параметри запиту включають заголовок, текст повідомлення, ідентифікатор пристрою та інші налаштування;
- надсилання даних із мікроконтролера при спрацюванні датчика полум'я [23].

3.7 Перевірка функціональності системи

Було повністю зібрано та з'єднано всі компоненти апаратно-програмного комплексу (див. рис. 3.18). Після компіляції програмного коду та його завантаження до апаратної платформи було проведено перевірку працездатності системи. Зокрема, здійснено імітацію пожежі, під час якої датчик полум'я успішно зафіксував наявність джерела загоряння.

Після запуску програми та спрацювання системи детекції у середовищі ThingSpeak, у віджеті, що відповідає за виявлення пожежі, засвітилася зелена індикаторна лампа, що відповідало очікуваному результату. Це свідчить про правильність роботи комплексу (див. рис. 3.19).

Одразу після фіксації загоряння користувач отримав push-сповіщення у мобільному застосунку Pushsafer на смартфоні.

Після відкриття застосунку було підтверджено отримання двох сповіщень про виявлення пожежі: о 17:33 під час першого тесту та о 18:58 – під час повторного. Обидва повідомлення були доставлені успішно (див. рис. 3.20).

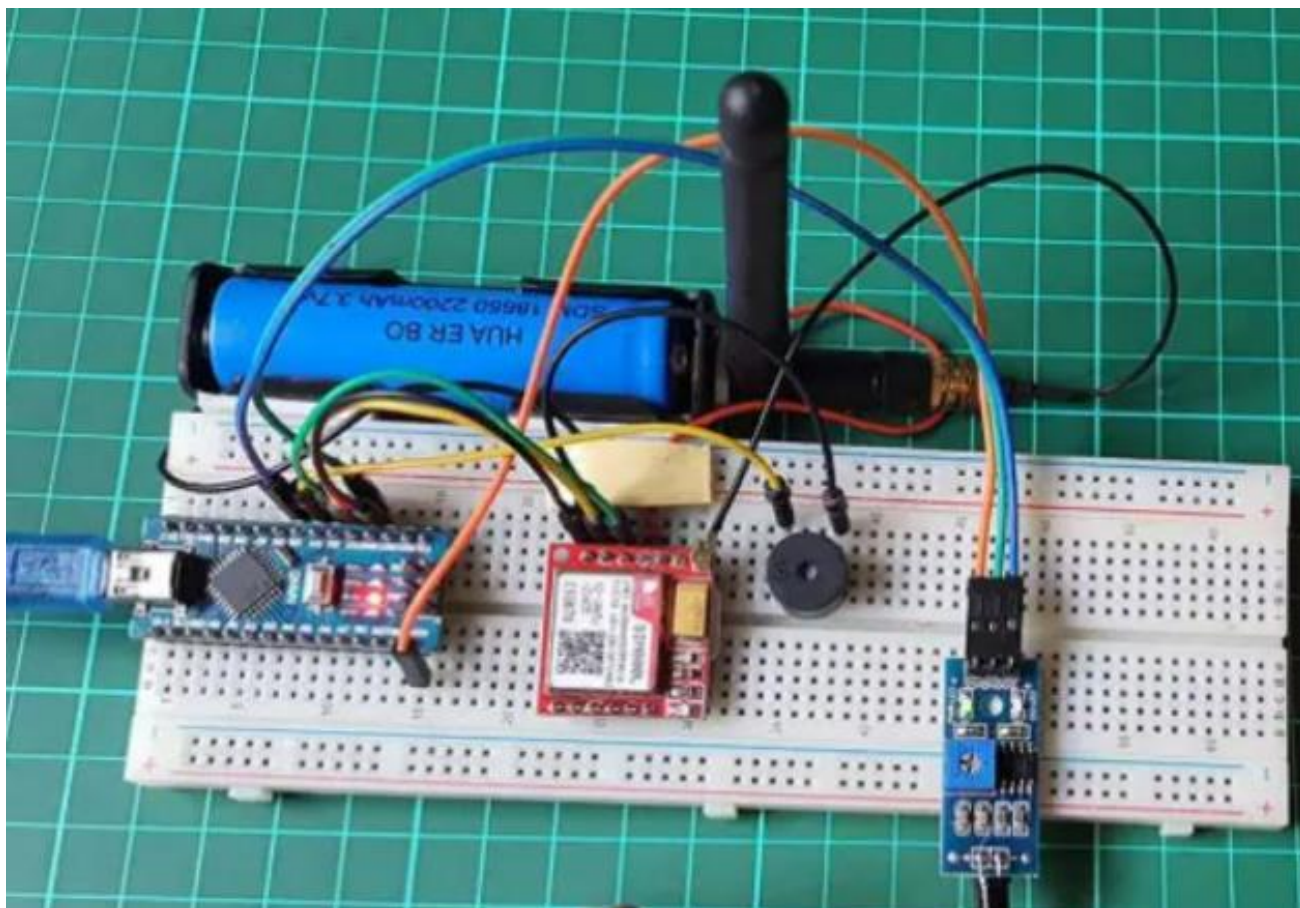


Рисунок 3.18 — Прототип мікропроцесорної системи

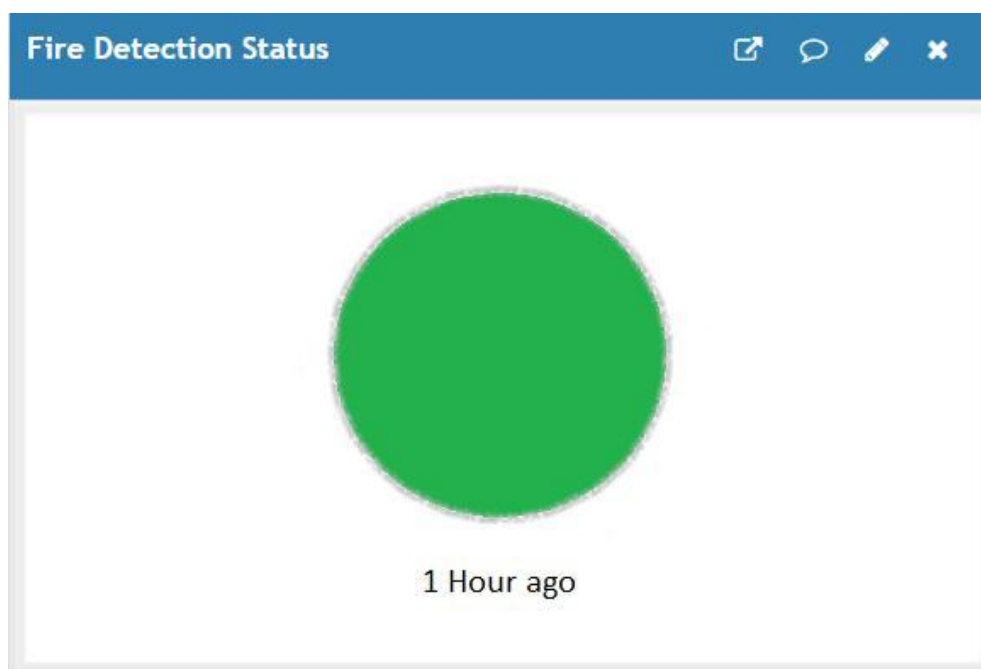


Рисунок 3.19 — Тестування системи у ThingSpeak



Рисунок 3.20 — Повідомлення про виявлення пожежі

Надалі було проведено серію експериментів з різними розташуваннями джерела вогню в межах чутливості інфрачервоного датчика полум'я. Загалом виконано 10 тестувань, результати яких подано у вигляді графіка на рис. 3.21. Вимірювався час від моменту виявлення пожежі до моменту отримання сповіщення в мобільному додатку, що відображає загальну реакцію системи на надзвичайну подію [24].

Проміжок виявлення, сек.



Рисунок 3.21 — Результати тестування системи

ВИСНОВКИ

У процесі виконання бакалаврської кваліфікаційної роботи було проведено всебічний аналіз існуючих технологій та методів виявлення пожежі, а також розглянуто технічні рішення, що вже використовуються у цій сфері. Окрему увагу було приділено вивченню принципів роботи та типів датчиків полум'я, особливостям їх використання, а також засобам бездротової передачі даних, зокрема модулю GSM.

Для реалізації прототипу було обрано апаратну платформу Arduino Nano, яка завдяки своїм характеристикам виявилася оптимальним рішенням для побудови компактного та енергоефективного комплексу. У ході роботи було розроблено програмну частину, що реалізує алгоритм ініціалізації модулів, зчитування даних з датчика вогню та надсилання сповіщення користувачу при фіксації загоряння.

Було виконано проєктування апаратної схеми та створено макет, після чого проведено тестування з використанням середовища ThingSpeak та мобільного застосунку Pushsafer. Результати експериментів підтвердили працездатність системи та її здатність ефективно виявляти пожежу й оперативно інформувати користувача. Варіювання часу реагування залежало від розташування джерела вогню щодо датчика, що було враховано під час аналізу ефективності роботи комплексу.

Мікропроцесорна система має ряд переваг, серед яких – простота реалізації, низька вартість, можливість масштабування та адаптації під різні типи приміщень.

Розроблена система може бути використана як автономне рішення для пожежної безпеки у невеликих приміщеннях, офісах, приватних будинках або допоміжних спорудах. Завдяки можливості розширення, її можна інтегрувати до більших систем моніторингу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пожежна безпека об'єктів будівництва. URL: <https://wiki.legalaid.gov.ua/> (дата звернення: 10.05.2025).
2. Fire Safety Systems. URL: <https://www.csuohio.edu/access-security/fire-safety-systems> (дата звернення: 10.05.2025).
3. Плата NANO Arduino. URL: https://uk.wikipedia.org/wiki/Arduino_Nano (дата звернення: 10.05.2025).
4. Fire Alarm System. URL: https://en.wikipedia.org/wiki/Fire_alarm_system (дата звернення: 10.05.2025).
5. Пожежна безпека об'єктів будівництва. URL: <https://wiki.legalaid.gov.ua/> (дата звернення: 10.05.2025).
6. Fire Detection control panel. URL: <https://www.ddfire.gov.uk/fire-detection-and-warning-system> (дата звернення: 10.05.2025).
7. Arduino IoT Cloud. URL: <https://docs.arduino.cc/arduino-cloud/> (дата звернення: 10.05.2025).
8. Rebizant W., Szafran J., Wiszniewski A. Digital Signal Processing in Fire System Protection and Control. Springer, Berlin, 2011. № 3:622.
9. Монк С. Arduino programming. Professional work with sketches. СПб, 2017.
10. Thampi S. M., Krishnan S., Corchado J. M., Das S., Wozniak M., Al-Jumeily D. Advances in Signal Processing and Intelligent Recognition Systems. SIRS. 2017.
11. Getting Started with Arduino products. URL: <https://www.arduino.cc/en/Guide> (дата звернення: 10.05.2025).
12. Arduino Integrated Development Environment. URL: <https://docs.arduino.cc/software/ide-v1/tutorials/arduino-ide-v1-basics> (дата звернення: 10.05.2025).
13. SIM800L GSM module characteristics. URL: <https://nettigo.eu/products/sim800l-gsm-grps-module> (дата звернення: 10.05.2025).
14. Fire detection. URL: <https://www.sciencedirect.com/topics/engineering/fire-detection> (дата звернення: 10.05.2025).

15. Fire safety through mathematical modelling. URL: https://www.researchgate.net/publication/228763095_Fire_safety_through_mathematical_modelling (дата звернення: 10.05.2025).
16. Flame Sensor: Principle of work. URL: <https://www.watelectronics.com/flame-sensor/> (дата звернення: 10.05.2025).
17. Infrared Flame Sensor Module, how it works. URL: <https://www.electroduino.com/ir-infrared-flame-sensor-module/> (дата звернення: 10.05.2025).
18. Push notifications using Pushsafer. URL: <https://projecthub.arduino.cc/pushsafer/acd03914-b45f-40a3-93b6-73c0d7ba5ae0> (дата звернення: 10.05.2025).
19. Connection of Arduino project with Pushsafer app. URL: <https://www.pushsafer.com/en/arduino> (дата звернення: 10.05.2025).
20. What is GSM? URL: <https://www.techtarget.com/searchmobilecomputing/definition/GSM> (дата звернення: 10.05.2025).
21. Learn More About ThingSpeak. URL: https://thingspeak.com/pages/learn_more (дата звернення: 10.05.2025).
22. Li-Ion battery 3.6V - 3.7V with 3200mAh capacity. URL: https://www.akkuteile.de/en/lithium-ionen-battery/size-26500/26650a-li-ion-battery-3-6v-3-7v-with-4500mah-capacity-and-15a-discharge-current_100733_3027 (дата звернення: 10.05.2025).
23. Different Types of Fire Detector sensors. URL: <https://firerisk.co.uk/different-types-of-fire-detector-heads/> (дата звернення: 10.05.2025).
24. Arduino Programming in C. URL: <https://www.codementor.io/@dewetvanthomas/tutorial-arduino-programming-in-c-12b7cztyui> (дата звернення: 10.05.2025).
25. UML Diagrams: Types. URL: <https://tallyfy.com/uml-diagram/> (дата звернення: 10.05.2025).

ДОДАТОК А**Технічне завдання**

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ ВНТУ

д.т.н., проф.

_____ О. Д. Азаров

«21» березня 2025 року

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврського дипломного проекту

«Мікропроцесорна система протипожежного сповіщення»

08-54.БКР.009.00.000 ПЗ ТЗ

Науковий керівник к.т.н., доц. каф. ОТ

_____ Богомолів С.В.

Студент групи КІ-23мс

_____ Половянова М. Г.

Вінниця 2025

1 Підстава виконання магістерської кваліфікаційної роботи

Наказ про затвердження теми бакалаврської кваліфікаційної роботи від 20.03.2025 р. №97.

2 Мета та призначення БКР

2.1 Мета роботи — Розробка мікропроцесорної системи протипожежного сповіщення, яка автоматично виявляє пожежу за допомогою датчиків диму та температури, сповіщає користувача про загрозу через бездротові канали зв'язку, що дозволяє оперативно реагувати на пожежні ситуації та мінімізувати ризики.

2.2 Призначення розробки — виконання бакалаврської кваліфікаційної роботи.

3 Вихідні дані для виконання БКР

Вихідні дані: технічний опис мікропроцесорної системи протипожежного сповіщення, технології розробки: мова програмування C для Arduino, бібліотеки для роботи з серійним зв'язком та Ethernet, мобільні сервіси, технології для інтеграції з мобільними застосунками, цільова платформа системи — Arduino, середовище розробки — Arduino IDE.

4. Вимоги до виконання БКР

БКР повинна задовольняти такі вимоги:

- проаналізувати існуючі підходи до побудови систем виявлення пожежі;
- визначити функціональні та технічні вимоги до розроблюваної системи;
- обрати необхідні апаратні та програмні компоненти;
- розробити структурну схему та алгоритм роботи системи;
- реалізувати прототип системи на базі Arduino;

— протестувати працездатність системи та оцінити її ефективність.

4. Етапи БДП та очікувані результати наведені в табл.. А1.

Таблиця А.1 – Етапи виконання роботи

№ з/п	Назва етапів дипломної роботи	Строк виконання	Підпис
1	Постановка задачі роботи	21.03.25— 30.03.25	
2	Пошук матеріалів та інформаційних джерел	21.03.25— 30.03.25	
3	Аналіз існуючих прототипів та визначення вимог до створюваної системи	31.03.25— 13.04.25	
4	Обґрунтування структури та принципів роботи системи	14.04.25— 27.04.25	
5	Розробка й тестування апаратно-програмної системи	28.04.25— 11.05.25	
6	Оформлення пояснювальної записки та ілюстративного матеріалу	13.05.25	
7	Перевірка якості виконання бакалаврської кваліфікаційної роботи та усунення недоліків	21.03.25— 30.03.25	

6 Матеріали, що подаються до захисту БКР

Пояснювальна записка БКР, графічні і ілюстративні матеріали, протокол попереднього захисту БКР на кафедрі, відзив наукового керівника, рецензія опонента, протоколи складання державних екзаменів, анотації до БКР українською та іноземною мовами, довідка про відповідність оформлення БКР діючим вимогам.

7 Порядок контролю виконання та захисту БКР

Виконання етапів графічної та розрахункової документації БКР контролюється науковим керівником згідно зі встановленими термінами. Захист БКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

8 Вимоги до оформлювання та порядок виконання БКР.

8.1 При оформлювання БДР використовуються:

- ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;
- ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;
- міждержавний ГОСТ 2.104-2006 «Єдина система конструкторської документації. Основні написи»;
- Методичні вказівки до виконання бакалаврських кваліфікаційних робіт зі спеціальності 123 «Комп'ютерна інженерія» (освітня програма «Комп'ютерна інженерія»). Кафедра обчислювальної техніки ВНТУ 2022;
- документами на які посилаються у вище вказаних.

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

ДОДАТОК Б

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Мікропроцесорна система протипожежного сповіщенняТип роботи: бакалаврська кваліфікаційна робота
(бакалаврська кваліфікаційна робота / магістерська кваліфікаційна робота)Підрозділ кафедра обчислювальної техніки
(кафедра, факультет, навчальна група)Коефіцієнт подібності текстових запозичень, виявлених у роботі
системою StrikePlagiarism 0,5 %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

- ✓ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту
- ☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.
- ☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

Азаров О.Д., зав. каф. ОТ
(прізвище, ініціали, посада)
(підпис)Крупельницький Л.В., доц. каф. ОТ
(прізвище, ініціали, посада)
(підпис)Особа, відповідальна за перевірку
(підпис)Захарченко С.М.
(прізвище, ініціали)

З висновком експертної комісії ознайомлений(-на)

Здобувач
(підпис)Половянова М. Г.
(прізвище, ініціали)Керівник роботи
(підпис)Богомолів С.В., доц. каф. ОТ
(прізвище, ініціали, посада)

ДОДАТОК В

Графічна частина

ДІАГРАМА ДЕТЕКЦІЇ ВОГНЮ

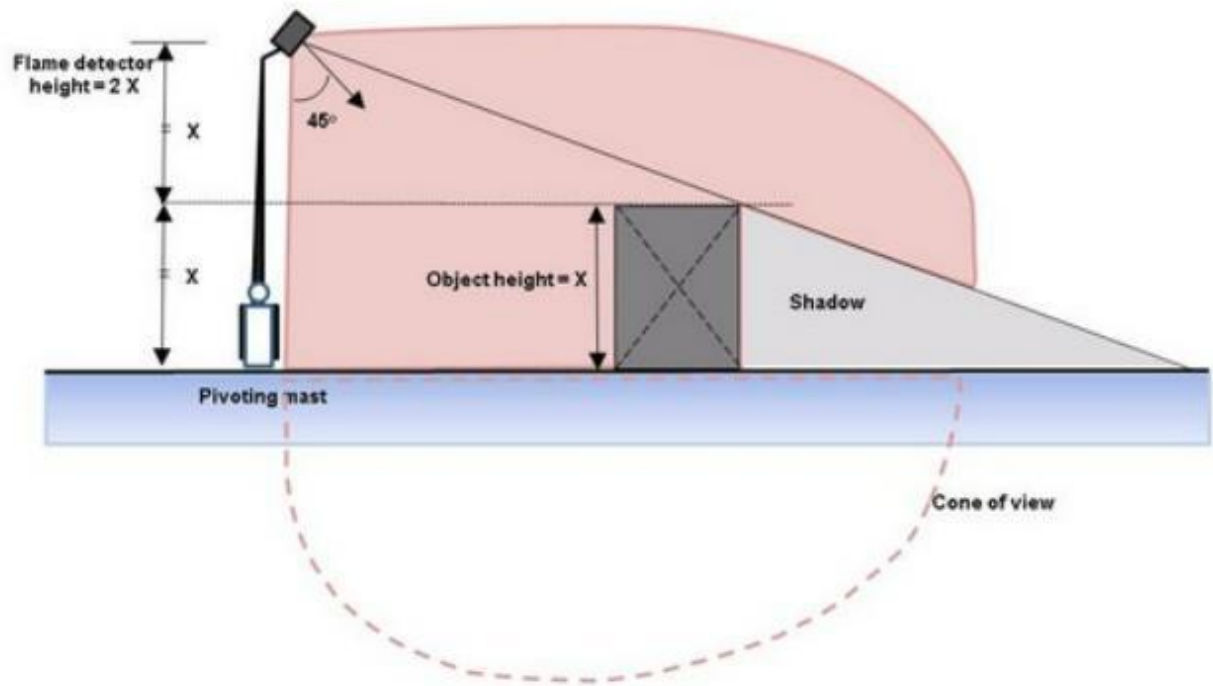


Рисунок В.1 — Діаграма детекції вогню

ДОДАТОК Г

Ілюстративна частина

РЕЗУЛЬТАТИ ТЕСТУВАННЯ СИСТЕМИ

Проміжок виявлення, сек.

Рисунок Г — Результати тестування системи

ДОДАТОК Д

Лістинг коду програми

```

#include <SoftwareSerial.h>
SoftwareSerial gprsSerial(10, 11);
#include <String.h>
#include <SPI.h>
#include <Ethernet.h>
byte mac[] = {0xDE, 0xAC, 0xBF, 0xEF, 0xFE, 0xAA};
String privatekey = "Fire Detection system";
int length;
EthernetClient client;
int flag = 0;
void setup() {
    pinMode(9, OUTPUT);
    pinMode(12, INPUT);
    gprsSerial.begin(9600); // the GPRS baud rate
    Serial.begin(9600);     // the GPRS baud rate
    Module_Init();
}
void loop() {
    if (gprsSerial.available())
        Serial.write(gprsSerial.read());

    int fire = digitalRead(12);
    if (fire == 0) {
        digitalWrite(9, HIGH);
        void setup() {
            Serial.begin(9600);
            Serial.print(F("Starting ethernet..."));
        }
    }
}

```

```

    if (!Ethernet.begin(win))
        Serial.println("failed");
    else
        Serial.println(Ethernet.localIP());
    delay(5000);
    Serial.println("Ready");
}

void loop() {
    pushsafer("Fire was detected!", "Fire detection system", "1", "1",
"1",          "#FF0000",          "https://www.pushsafer.com/dashboard",
"wPP6gykYx9ZxzQYc utKS", "0", "2", "60", "6000", "Successful detection",
"63376");
    delay(60000);
}

byte pushsafer(char *pushsafermessage, char *pushsafertitle, char
*pssound, char *psvibration, char *psicon, char *pscolor, char *psurl, char
*psurltitle, char *pstime2live, char *pspriority, char *psretry, char *psexpire,
char *psanswer, char *psdevice) {
    String title = pushsafertitle;
    String message = pushsafermessage;
    String device = psdevice;
    String sound = pssound;
    String vibration = psvibration;
    String icon = psicon;
    String color = pscolor;
    String url = psurl;
    String urltitle = psurltitle;
    String time2live = pstime2live;
    String priority = pspriority;
    String retry = psretry;

```

```

String expire = psexpire;
String answer = psanswer;

length = 45 + message.length() + title.length() + sound.length() +
vibration.length() + icon.length() + color.length() + url.length() +
urltitle.length() + time2live.length() + device.length() + privatekey.length();

if (client.connect("pushsafer.com", 80)) {
    client.println("POST /api HTTP/1.1");
    client.println("Host: https://www.pushsafer.com");
    client.println("Connection: close\r\nContent-Type: application/x-
www-form-urlencoded");

    client.print("Content-Length: ");
    client.print(length);
    client.println("\r\n");
    client.print("k=");
    client.print(privatekey);
    client.print("&m=");
    client.print(message);
    client.print("&t=");
    client.print(title);
    client.print("&s=");
    client.print(sound);
    client.print("&v=");
    client.print(vibration);
    client.print("&i=");
    client.print(icon);
    client.print("&c=");
    client.print(color);
    client.print("&u=");
    client.print(url);
    client.print("&ut=");

```

```

    client.print(urltitle);
    client.print("&l=");
    client.print(time2live);
    client.print("&pr=");
    client.print(priority);
    client.print("&re=");
    client.print(retry);
    client.print("&ex=");
    client.print(expire);
    client.print("&a=");
    client.print(answer);
    client.print("&d=");
    client.print(device);
    while (client.connected()) {
        while (client.available()) {
            char ch = client.read();
            Serial.write(ch);
        }
    }
    client.stop();
}

gprsSerial.println("AT+CIPSTART=\"TCP\", \"api.thingspeak.com\", \"80\");
// start up the connection
    delay(6000);
    ShowSerialData();
    gprsSerial.println("AT+CIPSEND"); // begin send data to remote
server
    delay(4000);
    ShowSerialData();

```

```

        String          str          =          "GET
https://api.thingspeak.com/update?api_key=ER43PXXXXXHQF0I&field1="
+ String(1);
        Serial.println(str);
        gprsSerial.println(str); // begin send data to remote server
        delay(4000);
        ShowSerialData();
        digitalWrite(9, LOW);
        gprsSerial.println((char)26); // sending
        delay(5000); // waiting for reply, important! the time is based on the
condition of internet

        gprsSerial.println();
        ShowSerialData();
        gprsSerial.println("AT+CIPSHUT"); // close the connection
        delay(100);
        ShowSerialData();
    } else {
        digitalWrite(9, LOW);
        if (flag == 0) {
            flag = 1;

gprsSerial.println("AT+CIPSTART=\"TCP\", \"api.thingspeak.com\", \"80\");
// start up the connection
            delay(6000);
            ShowSerialData();
            gprsSerial.println("AT+CIPSEND"); // begin send data to remote
server
            delay(4000);
            ShowSerialData();

```

```

        String          str          =          "GET
https://api.thingspeak.com/update?api_key=ER43PWT91CGHQF0I&field1="
+ String(0);

        Serial.println(str);
        gprsSerial.println(str); // begin send data to remote server
        delay(4000);
        ShowSerialData();
        digitalWrite(9, LOW);
        gprsSerial.println((char)26); // sending
        delay(5000); // waiting for reply, important! the time is based on the
condition of internet

        gprsSerial.println();
        ShowSerialData();
        gprsSerial.println("AT+CIPSHUT"); // close the connection
        delay(100);
        ShowSerialData();
    }
}

void ShowSerialData() {
    while (gprsSerial.available() != 0)
        Serial.write(gprsSerial.read());
    delay(5000);
}

void Module_Init() {
    gprsSerial.println("AT");
    delay(1000);
    gprsSerial.println("AT+CPIN?");
    delay(1000);
    gprsSerial.println("AT+CREG?");

```

```
delay(1000);
gprsSerial.println("AT+CGATT?");
delay(1000);
gprsSerial.println("AT+CIPSHUT");
delay(1000);
gprsSerial.println("AT+CIPSTATUS");
delay(2000);
gprsSerial.println("AT+CIPMUX=0");
delay(2000);
ShowSerialData();
gprsSerial.println("AT+CSTT=\"www\"");
delay(1000);
ShowSerialData();
gprsSerial.println("AT+CIICR");
delay(3000);
ShowSerialData();
gprsSerial.println("AT+CIFSR");
delay(2000);
ShowSerialData();
gprsSerial.println("AT+CIPSPRT=0");
delay(3000);
ShowSerialData();
```