

**Міністерство освіти і науки України**

**Луцький національний технічний університет**

(повне найменування закладу вищої освіти)

**Факультет комп'ютерних та інформаційних технологій**

(повне найменування факультету)

**Кафедра комп'ютерної інженерії та охоронних систем**

(повне найменування кафедри)

**КВАЛІФІКАЦІЙНА РОБОТА  
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»**

**СИСТЕМА ІНФРАЧЕРВОНОГО БАР'ЄРА ДЛЯ ОХОРОНИ  
ПЕРИМЕТРУ**

**INFRARED BARRIER SYSTEM FOR PERIMETER  
PROTECTION**

спеціальність 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія

(назва освітньої програми)

Виконав: здобувач вищої освіти  
групи КІ-41

Антонюк Андрій Олександрович

(підпис)

Керівник:

к.т.н., доцент

Костючко Сергій Миколайович

(підпис)

Кваліфікаційну роботу

допущено до захисту

« \_\_\_\_\_ » червня 2026 р.

Гарант освітньої програми:

к.т.н., доцент

Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних та інформаційних технологій

Кафедра комп'ютерної інженерії та безпеки

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри

к.т.н. Т. Терлецький

« \_\_\_\_\_ » \_\_\_\_\_ 2026 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

*Антонюку Андрію Олександровичу*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Система інфрачервоного бар'єра для охорони периметру

Керівник роботи к.т.н., доц. Костючко Сергій Миколайович

затверджені наказом закладу вищої освіти від «20» грудня 2025 року № 536/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026р.

3. Вихідні дані до роботи Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

Вступ

Аналітична частина

Проектування апаратної частини системи

Програмна реалізація та експериментальні дослідження

Висновки

5. Перелік графічного (ілюстративного) матеріалу:

## 6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
<i>Аналітична частина</i>	<i>Костючко С.М., доцент</i>		
<i>Проектування апаратної частини системи</i>	<i>Костючко С.М., доцент</i>		
<i>Програмна реалізація та експериментальні дослідження</i>	<i>Костючко С.М., доцент</i>		
<i>Нормоконтроль</i>	<i>Багнюк Н.В., доцент</i>		
<i>Гарант ОП</i>	<i>Лавренчук С.В., доцент</i>		
<i>Показник запозичень тексту</i>		_____%	
<i>Академічна доброчесність</i>	<i>Міскевич О.І., ст. викладач</i>		

7. Дата видачі завдання 23.12.2025 р.

## КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	<i>Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень</i>	до 10.02.2026 р.	<i>виконано</i>
2.	<i>Аналітична частина</i>	до 02.03.2026 р.	<i>виконано</i>
3.	<i>Проектування апаратної частини системи</i>	до 02.04.2026 р.	<i>виконано</i>
4.	<i>Програмна реалізація та експериментальні дослідження та формування додатків</i>	до 10.04.2026 р.	<i>виконано</i>
5.	<i>Представлення остаточного варіанту кваліфікаційної роботи керівникові</i>	до 01.05.2026 р.	<i>виконано</i>
6.	<i>Нормоконтроль</i>	до 23.05.2026 р.	<i>виконано</i>
7.	<i>Інструментальна перевірка на академічний плагіат</i>	до 19.05.2026 р.	<i>виконано</i>
8.	<i>Здача кваліфікаційної роботи та всіх супровідних документів на кафедру</i>	до 28.05.2026 р.	<i>виконано</i>

Здобувач вищої освіти

(підпис)

Андрій АНТОНЮК

(прізвище, ініціали)

Керівник кваліфікаційної роботи

(підпис)

Сергій КОСТЮЧКО

(прізвище, ініціали)

## АНОТАЦІЯ

Антонюк А. О. Система інфрачервоного бар'єра для охорони периметру.  
Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел.

У першому розділі проаналізовано сучасні системи охорони периметра, принцип дії інфрачервоних бар'єрів, їх класифікацію, комерційні аналоги та технічні вимоги до розроблюваної системи.

У другому розділі обґрунтовано вибір апаратних компонентів, розроблено структурну, функціональну та принципову електричну схеми інфрачервоного бар'єра, а також засоби захисту від хибних спрацювань.

У третьому розділі описано алгоритм роботи системи, програмне забезпечення для ESP32, практичну реалізацію дослідного зразка та результати експериментального тестування.

Об'єкт дослідження – процеси виявлення вторгнень на територію, що охороняється, засобами оптико-електронної детекції.

Предмет дослідження – апаратно-програмні методи побудови інфрачервоного бар'єра для охорони периметра.

Метою роботи є проектування та практична реалізація автономної системи інфрачервоного бар'єра з підвищеною завадостійкістю та можливістю дистанційного оповіщення.

Ключові слова: інфрачервоний бар'єр, охорона периметра, ESP32, PIDS, ІЧ-сигнал, модуляція 38 кГц, автономне живлення, Wi-Fi-сповіщення.

## ABSTRACT

Antoniuk A. Infrared barrier system for perimeter protection. Manuscript.

Qualification work of the bachelor of the specialty «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

The qualification work consists of an introduction, three chapters, conclusions, and a list of sources used.

The first chapter analyzes modern perimeter security systems, the principle of operation of infrared barriers, their classification, commercial analogues, and technical requirements for the developed system.

The second chapter justifies the choice of hardware components, develops a structural, functional, and basic electrical circuit of the infrared barrier, as well as means of protection against false positives.

The third chapter describes the system's operating algorithm, software for ESP32, practical implementation of the prototype, and the results of experimental testing.

The object of the study is the processes of detecting intrusions into the protected area by means of optoelectronic detection.

The subject of the study is hardware and software methods for building an infrared barrier for perimeter protection.

The purpose of the work is to design and practical implementation of an autonomous infrared barrier system with increased noise immunity and the possibility of remote notification.

Keywords: infrared barrier, perimeter security, ESP32, PIDS, IR signal, 38 kHz modulation, autonomous power supply, Wi-Fi notification.

## ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 АНАЛІТИЧНА ЧАСТИНА.....	9
1.1 Аналіз літературних джерел.....	9
1.2 Огляд сучасних технічних засобів та систем охорони периметру .....	14
1.3 Фізичні основи, принцип дії та класифікація інфрачервоних бар'єрів .....	15
1.4 Аналіз існуючих комерційних аналогів інфрачервоних систем на ринку. 17	
1.5 Обґрунтування доцільності розробки та формування технічних вимог до системи.....	19
РОЗДІЛ 2 ПРОЕКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ.....	23
2.1 Розробка структурної та функціональної схем інфрачервоного бар'єра ...	23
2.2 Вибір та обґрунтування апаратної елементної бази .....	25
2.3 Розробка принципової електричної схеми пристрою.....	28
2.4 Проектування засобів захисту системи від хибних спрацювань.....	31
РОЗДІЛ 3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ .....	35
3.1 Опис та розробка алгоритму функціонування системи.....	35
3.2 Розробка програмного забезпечення для базового мікроконтролера .....	38
3.3 Практична реалізація дослідного зразка (макета) системи охорони.....	41
3.4 Методика тестування, аналіз результатів експериментальних досліджень .....	43
ВИСНОВКИ.....	48
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....	50

## ВСТУП

Актуальність теми. У сучасних умовах глобальної цифровізації та зростання загроз фізичній безпеці об'єктів критичної інфраструктури, промислових підприємств та приватних територій, створення надійних систем охорони периметра (Perimeter Intrusion Detection Systems – PIDS) набуває стратегічного значення. Традиційні засоби захисту, такі як механічні огорожі, часто виявляються недостатніми без інтеграції з інтелектуальними електронними системами виявлення.

Інфрачервоні (ІЧ) бар'єри є одним із найбільш ефективних та економічно доцільних засобів детекції вторгнень завдяки своїй «невидимості» для порушника та стійкості до радіоперешкод. Однак існуючі комерційні рішення часто мають закриту архітектуру, високу вартість та обмежені можливості інтеграції в сучасні IoT-мережі. Крім того, проблема хибних спрацювань через погодні умови (туман, опади) та дрібних тварин залишається актуальною для бюджетних сегментів ринку. Таким чином, розробка інтелектуальної, енергоефективної та завадостійкої системи ІЧ-бар'єра на базі сучасних мікроконтролерів є актуальним науково-технічним завданням.

Мета роботи – проектування та практична реалізація системи інфрачервоного бар'єра для охорони периметра з підвищеною завадостійкістю, можливістю автономної роботи та інтеграцією в цифрові мережі моніторингу.

Об'єкт дослідження – процеси виявлення та ідентифікації вторгнень на територію, що охороняється, за допомогою засобів оптико-електронної детекції.

Предмет дослідження – методи модуляції та цифрової обробки інфрачервоних сигналів, алгоритми фільтрації завад та апаратно-програмні засоби побудови систем охорони периметра на базі мікроконтролерів.

Практичне значення роботи полягає у створенні діючого прототипу автономного інфрачервоного бар'єра, який за своїми характеристиками (дальність дії понад 50 м, Wi-Fi сповіщення) не поступається дорогим

комерційним аналогам, але має значно нижчу собівартість. Результати роботи можуть бути використані для швидкого розгортання систем безпеки на віддалених об'єктах, де відсутня стаціонарна інфраструктура живлення та зв'язку.

Для досягнення поставленої мети визначено такі завдання:

- проаналізувати сучасний стан та тенденції розвитку технічних засобів охорони периметра;
- дослідити фізичні основи роботи активних інфрачервоних систем та класифікувати їх за ключовими параметрами;
- обґрунтувати вибір апаратної бази (мікроконтролера, оптичних компонентів та системи живлення) для створення дослідного зразка;
- розробити структурну, функціональну та принципову електричні схеми пристрою;
- розробити програмне забезпечення для мікроконтролера ESP32, що реалізує логіку детекції та передачі тривожних сповіщень;
- виготовити дослідний зразок системи та провести серію експериментальних досліджень для оцінки її ефективності в реальних умовах.

## РОЗДІЛ 1

### АНАЛІТИЧНА ЧАСТИНА

#### 1.1 Аналіз літературних джерел

Аналіз опрацьованих джерел засвідчує, що проблема охорони периметра розглядається в сучасних дослідженнях як комплексне завдання, яке поєднує фізичний захист території, раннє виявлення вторгнення, обробку сенсорних даних і передавання тривожної інформації до систем моніторингу. У роботі «Perimeter Protection of the Areas of Interest» периметровий захист подано як сукупність технічних і організаційних засобів, спрямованих на виявлення порушника ще до його проникнення у внутрішню зону об'єкта [1]. Такий підхід є важливим для обґрунтування доцільності розробки інфрачервоного бар'єра, оскільки він виконує функцію первинного рубежу контролю та дозволяє фіксувати факт перетину охоронної межі.

Сучасні наукові праці дедалі частіше підкреслюють необхідність поєднання кількох технологій виявлення, оскільки жоден окремий сенсор не забезпечує однаково високу ефективність у всіх умовах експлуатації. У дослідженні, присвяченому захисту периметра з використанням електромагнітного виявлення, дронів і стаціонарних камер, акцентовано увагу на перевагах багатокomпонентних систем, які можуть поєднувати різні принципи детекції [2]. Для розроблюваної системи це означає, що інфрачервоний бар'єр може бути не лише самостійним засобом охорони, а й одним із модулів ширшої охоронної інфраструктури.

Безпосередньо інфрачервоні бар'єри у прикладних джерелах описуються як ефективний спосіб створення умовної «невидимої лінії» контролю. У матеріалі про ПЧ-бар'єри для периметрового захисту розглядається принцип роботи таких систем, що базується на взаємодії передавача, приймача та інфрачервоного променя між ними [3]. Практична цінність цього підходу

полягає в тому, що система фіксує не загальний рух у зоні спостереження, а конкретний факт переривання променя, тобто перетин визначеної межі.

Питання вибору між зональним і точковим виявленням має важливе значення для побудови архітектури охоронної системи. У матеріалі Optex Europe наголошується, що різні об'єкти потребують різних підходів до периметрової безпеки: в одних випадках доцільним є контроль широкої зони, в інших – точкове або лінійне виявлення [4]. Інфрачервоний бар'єр належить саме до лінійних засобів контролю, тому його доцільно застосовувати для охорони воріт, проходів, огорож, вузьких ділянок периметра або контрольованих коридорів руху.

Ринкові огляди 2025 року демонструють, що розвиток систем периметрової охорони відбувається у напрямі автономності, цифровізації та інтеграції з віддаленими сервісами моніторингу. У статті про тенденції периметрової безпеки підкреслюється роль сучасних сенсорів, бездротових каналів зв'язку, інтелектуальної обробки подій і централізованого керування [5]. Це узгоджується з вибором ESP32 як апаратної основи розроблюваної системи, оскільки цей мікроконтролер підтримує Wi-Fi, може передавати сповіщення та забезпечує подальшу інтеграцію з IoT-інфраструктурою.

Аналітичні матеріали щодо ринку інфрачервоних бар'єрів також вказують на збереження попиту на такі рішення завдяки їх відносній простоті, доступності та придатності для широкого кола об'єктів [6]. Попри активний розвиток відеоаналітики, радарів і тепловізійних систем, класичний ПЧ-бар'єр залишається актуальним для бюджетного та середнього сегментів. Це пояснюється тим, що він не потребує складної обчислювальної обробки, має зрозумілу логіку роботи та може бути реалізований на доступній елементній базі.

Окремий напрям сучасних досліджень пов'язаний із використанням інфрачервоного та теплового діапазону для виявлення об'єктів у системах

периметрової безпеки. У роботі, присвяченій виявлення теплових об'єктів, розглядається застосування теплового аналізу для безперервного контролю територій [7]. Хоча розроблювана система не є тепловізійною, це джерело є важливим для розуміння загальної ролі ІЧ-спектра у задачах охорони. Воно підтверджує, що інфрачервоні технології можуть використовуватися як у простих бар'єрних системах, так і в складніших рішеннях із розпізнаванням об'єктів.

Порівняння активних і пасивних інфрачервоних сенсорів дає змогу точніше обґрунтувати вибір саме активного ІЧ-бар'єра. У джерелі, присвяченому відмінностям між активний інфрачервоний датчик і пасивний інфрачервоний датчик, зазначено, що активні системи формують власний сигнал і контролюють його проходження між передавачем та приймачем, тоді як пасивні датчики реагують на теплове випромінювання об'єкта [8]. Для задачі контролю конкретної лінії периметра активний принцип є доцільнішим, оскільки дозволяє чітко визначити момент переривання променя.

Наукова стаття в журналі *Sensors* про використання виявлення теплових об'єктів у периметровій безпеці розширює уявлення про можливості інфрачервоних технологій у цій сфері [9]. У ній акцентовано увагу на перевагах ІЧ-детекції для цілодобового спостереження, зокрема в умовах недостатньої видимості. Для цієї роботи це має значення як перспективний напрям подальшого розвитку: базовий ІЧ-бар'єр може бути доповнений тепловими сенсорами або елементами відеоаналітики для підвищення достовірності виявлення.

Порівняння ІЧ-бар'єра з відеоспостереженням дозволяє краще визначити місце розроблюваної системи серед інших PIDS-рішень. У роботі «Perimeter Intrusion Detection by Video Surveillance» розглядаються системи виявлення вторгнення на основі камер і алгоритмів аналізу відеопотоку [10]. Такі системи

мають ширші можливості класифікації об'єктів, але потребують якісного зображення, освітлення, обчислювальних ресурсів і складнішої інфраструктури. На цьому фоні ІЧ-бар'єр має практичну перевагу як простіше, дешевше та енергоефективніше рішення для фіксації факту перетину межі.

Проблематика навмисного впливу на інфрачервоні детектори розглядається у роботі «Adversarial Infrared Curves», де досліджуються атаки на ІЧ-детектори пішоходів у фізичному середовищі [11]. Це джерело демонструє, що ІЧ-системи можуть бути вразливими до спеціально сформованих оптичних або теплових впливів. Для розроблюваного ІЧ-бар'єра такий висновок є підставою для впровадження частотної модуляції, часової фільтрації, контролю стабільності сигналу та режиму самодіагностики.

PDF-версія цієї ж роботи дає змогу детальніше розглянути технічний бік дослідження, зокрема механізми впливу на ІЧ-детектори та особливості фізичної реалізації атак [12]. У контексті цієї кваліфікаційної роботи це підкреслює необхідність не обмежуватися простим виявленням наявності або відсутності сигналу. Система повинна аналізувати характер сигналу, його тривалість, повторюваність, стабільність і відповідність очікуваній частотній структурі.

Мультисенсорні підходи до виявлення вторгнень розглядаються в роботі «Multi-sensor Intrusion Detector System» [13]. Її значення полягає в тому, що вона демонструє доцільність поєднання різних сенсорних каналів для зменшення кількості хибних спрацювань і підвищення надійності системи. Для розроблюваного рішення це відкриває перспективу модернізації: ІЧ-бар'єр може бути доповнений PIR-датчиком, магнітним контактом, камерою, акустичним сенсором або модулем контролю вібрацій.

Промислові вимоги до систем периметрового виявлення відображені у матеріалі про PIDS сертифіковані системи виявлення вторгнень периметра 4-го класу [14]. Цей документ є корисним як орієнтир для розуміння функцій, які

характерні для професійних охоронних систем: антисаботаж, контроль несправностей, стабільність роботи, надійне оповіщення та можливість інтеграції в централізовану інфраструктуру. Хоча розроблювана система є прототипом, її архітектура повинна враховувати такі принципи, зокрема через реалізацію тамперного контролю, журналювання подій і сервісних повідомлень.

Огляд мультисенсорного виявлення вторгнень на високошвидкісних залізницях демонструє, що складні об'єкти потребують комбінування різних технологій через вплив погодних умов, складного рельєфу, обмеженої видимості та високих вимог до надійності [15]. Ці висновки важливі для розробки ІЧ-бар'єра, оскільки підтверджують: у реальному середовищі ефективність окремого сенсора залежить від контексту його застосування. Тому система повинна мати модульну структуру та допускати подальше розширення.

Приклад практичної автономної системи подано у роботі про система виявлення вторгнень по периметру на основі сонячної енергії з інтеграцією SMS та сигналізації [16]. Це джерело є особливо близьким до практичної частини дослідження, оскільки в ньому поєднуються автономне живлення, периметрове виявлення та дистанційне оповіщення. Воно підтверджує доцільність використання акумулятора, сонячної панелі, контролера заряду та бездротового каналу передавання повідомлень у системах, які мають працювати на віддалених ділянках без постійного доступу до електромережі.

Повнотекстова версія огляду з центральний PubMed щодо мультисенсорного виявлення на залізничних периметрах додатково підкреслює, що надійність PIDS значною мірою залежить від злиття даних, адаптації до погодних умов і правильного вибору сенсорної конфігурації [17]. Для розроблюваного ІЧ-бар'єра це означає, що навіть базова система повинна проєктуватися з урахуванням майбутньої інтеграції з іншими джерелами даних.

Такий підхід підвищує цінність прототипу не лише як окремого охоронного пристрою, а як потенційного елемента комплексної системи захисту.

## **1.2 Огляд сучасних технічних засобів та систем охорони периметру**

Захист периметра є першою лінією оборони будь-якого об'єкта критичної інфраструктури, промислового підприємства або приватної території. Сучасні тенденції свідчать про перехід від простих механічних бар'єрів до складних інтелектуальних систем виявлення вторгнень (PIDS – Perimeter Intrusion Detection Systems), що базуються на мультисенсорній інтеграції та цифровій обробці сигналів.

Згідно з аналітичними оглядами, сучасні системи охорони периметра можна класифікувати за фізичним принципом дії та типом детекції:

- радіохвильові та радарні системи, які використовуються для виявлення рухомих об'єктів на великих дистанціях. Вони дозволяють не лише зафіксувати факт перетину межі, а й відстежувати траєкторію цілі. Проте їхня ефективність може знижуватися в умовах щільної забудови або складної рослинності;

- вібраційні та сенсорні кабельні системи, що встановлюються безпосередньо на огорожу (сітку, паркан) і реагують на механічні коливання під час спроб перелазу або перерізання;

- системи відеоаналітики та тепловізійного спостереження. Наукові дослідження 2025 року підкреслюють зростаючу роль теплових об'єктних детекторів. Завдяки здатності працювати в повній темряві та за несприятливих погодних умов (туман, дощ), тепловізійні камери стають стандартом для систем високого рівня безпеки (Grade-4);

- інфрачервоні (ІЧ) системи, що є одним із найбільш поширених і перевірених методів захисту. Вони поділяються на пасивні ІЧ-сенсори (PIR), що реагують на зміну теплового випромінювання в зоні детекції та активні ІЧ-бар'єри (AIR), що створюють невидиму лінію з одного або декількох

променів між передавачем і приймачем. Переривання променя генерує сигнал тривоги.

Дослідження підкреслюють, що вибір між «зональною» (наприклад, радари) та «точковою» (бар'єри) детекцією залежить від стратегії безпеки. Якщо зональні системи дають більше інформації про підхід до об'єкта, то бар'єрні системи забезпечують чітку фіксацію факту вторгнення з мінімальною кількістю хибних спрацювань за умови правильного налаштування.

Окремим викликом для сучасних PIDS є робота в екстремальних умовах, таких як високошвидкісні залізниці. В таких сценаріях поодинокі датчики часто не справляються, тому актуальним стає використання Multi-Sensor Fusion – об'єднання даних з ІЧ-бар'єрів, камер та сейсмічних датчиків для досягнення максимальної надійності.

Важливим напрямком розвитку є автономність систем. Сучасні рішення все частіше інтегрують сонячні панелі для живлення та модулі бездротового зв'язку (SMS, Wi-Fi, 4G/5G) для передачі сповіщень, що робить їх незалежними від стаціонарної енергомережі та вразливості кабельних ліній зв'язку.

Таким чином, інфрачервоні бар'єри залишаються ключовим елементом сучасних систем охорони периметра завдяки своїй «невидимості» для порушника, надійності та можливості легкої інтеграції в комплексні безпекові рішення.

### **1.3 Фізичні основи, принцип дії та класифікація інфрачервоних бар'єрів**

Функціонування інфрачервоних бар'єрів ґрунтується на властивостях електромагнітного випромінювання в ІЧ-спектрі (довжина хвилі приблизно від 700 нм до 1 мм). У системах безпеки найчастіше використовується ближній інфрачервоний діапазон, оскільки він є невидимим для людського ока, що забезпечує прихованість охорони.

Принцип роботи активного інфрачервоного бар'єра (Active Infrared – AIR) базується на створенні постійного оптичного зв'язку між двома компонентами: передавачем (випромінювачем) та приймачем (фотодетектором).

Передавач використовує інфрачервоні світлодіоди (LED) або лазерні діоди для фокусування вузьконаправленого пучка світла. Для запобігання саботажу та мінімізації впливу сонячного світла випромінювання зазвичай модулюється на певній частоті.

Приймач оснащений фотоелементом, налаштованим на частоту передавача. Поки промінь безперешкодно потрапляє на фотодетектор, система перебуває в стані «Норма».

Коли непрозорий об'єкт (людина, транспорт) перетинає лінію променя, інтенсивність сигналу на приймачі падає нижче встановленого порогу. Контролер фіксує розрив ланцюга та активує сигнал тривоги.

Важливим фізичним параметром є час переривання. Сучасні системи дозволяють налаштовувати цей показник (зазвичай від 50 до 500 мс), щоб ігнорувати дрібні об'єкти (птахів, листя, що падає), але чітко фіксувати рух людини.

За принципом дії інфрачервоні пристрої детекції класифікують за декількома основними ознаками:

- активні (AIR), що складаються з окремих блоків передавача та приймача. Створюють чітку лінію («промінь»). Найефективніші для довгих прямих ділянок периметра.

- пасивні (PIR), які не випромінюють енергію, а лише фіксують власне теплове випромінювання об'єктів (людини), що з'являються в зоні огляду. Працюють за принципом виявлення контрасту температур.

За конфігурацією променів інфрачервоні пристрої: однопроменеві, що використовуються для вузьких прорізів (двері, ворота). Легко обходяться шляхом підлізання або перестрибування; багатопроменеві (ІЧ-решітки/колони), які складаються з 2-20 променів, розташованих один над одним. Тривога

спрацьовує при перериванні певної комбінації променів (наприклад, двох сусідніх), що майже виключає помилкові спрацювання від тварин.

За типом конструкції можна виділити такі пристрої: двопозиційні – передавач і приймач рознесені на протилежні кінці ділянки; однопозиційні (рефлекторні) – передавач і приймач розміщені в одному корпусі, а на іншому кінці встановлюється пасивний відбивач (рефлектор). Це спрощує монтаж, оскільки живлення підводиться лише до однієї точки.

За дальністю дії поділяють на пристрої малої дальності (до 10-20 м) – для приміщень та вітрин; середньої та великої дальності (до 200-500 м) – для охорони зовнішніх периметрів великих об'єктів.

Сучасні тренди, описані в літературі 2025 року, вказують на популяризацію гібридних систем, де активна ІЧ-детекція поєднується з тепловізійним аналізом. Це дозволяє не просто фіксувати розрив променя, а й ідентифікувати тип порушника, підвищуючи загальний рівень інтелектуальної безпеки об'єкта.

#### **1.4 Аналіз існуючих комерційних аналогів інфрачервоних систем на ринку**

На сучасному ринку систем охорони периметра (PIDS) інфрачервоні бар'єри займають значну нішу завдяки балансу між вартістю та ефективністю. Основними гравцями, що визначають технологічні стандарти, є компанії Optex, Takex, Sick AG та Sicurit.

В таблиці 1.1 наведено порівняльний аналіз ключових комерційних серій, представлених на ринку .

Ключовими ринковими тенденціями 2025 року у сфері інфрачервоних охоронних бар'єрів є перехід до енергонезалежних, інтелектуальних і цифровізованих рішень. Сучасні виробники дедалі частіше орієнтуються на бездротові технології та автономне живлення, зокрема використання сонячних

батареї. Такі підходи характерні для рішень Optex, Hikvision та інших виробників, які пропонують серії пристроїв із передаванням сигналу через радіоканал. Це особливо важливо для охорони віддалених або протяжних об'єктів, де прокладання кабельних ліній є технічно складним або економічно недоцільним.

Таблиця 1.1 – Комерційні пропозиції представлені на ринку

Виробник	Серія / Модель	Основні характеристики	Технологічні особливості
Optex (Японія)	SL-QDM / SL-QFR	Дальність до 200 м, 4 промені, живлення від батарей або мережі.	Використання синхронізованих променів, що мінімізує вплив сонячного світла та перешкод. Підтримка бездротового зв'язку iSeries.
Takex (Японія)	PB-IN-HF	4-променеві бар'єри високої потужності, дальність до 200 м.	Система подвійної модуляції сигналу для виключення взаємного впливу сусідніх бар'єрів та стійкості до туману.
Sick AG (Німеччина)	MLG-2 / W12	Промислові світлові завіси та датчики високої точності.	Орієнтація на індустріальні об'єкти. Підтримка протоколів IO-Link та відповідність стандартам кібербезпеки IEC 62443.
Sicurit (Італія)	Dual Technology Barriers	Гібридні системи (ІЧ + мікрохвилі).	Поєднання ІЧ-променів з мікрохвильовими сенсорами для досягнення нульового рівня хибних спрацювань у важких погодних умовах.

Важливою тенденцією є також розвиток інтелектуальної фільтрації перешкод. Системи преміум-сегмента дедалі частіше використовують цифрову обробку сигналу для зменшення кількості хибних спрацювань. Завдяки цьому охоронний датчик може краще відрізнити реальне проникнення людини від руху

тварин, коливання гілок, трави або інших природних факторів. Наприклад, датчики Takeх передбачають можливість налаштування чутливості відповідно до конкретних умов місцевості, що підвищує стабільність роботи системи на відкритих територіях.

Окреме значення у 2025 році має цифровізація охоронних сенсорів та їх інтеграція в IoT-екосистеми. Сучасні пристрої дедалі частіше розглядаються не як ізольовані датчики, а як елементи комплексної системи моніторингу, що може передавати дані до централізованої платформи, підтримувати віддалене керування та взаємодіяти з хмарними сервісами. У цьому контексті зростає роль кібербезпеки, оскільки підключені до мережі сенсори повинні мати захист від несанкціонованого доступу, підміни сигналів, зламу облікових записів або втручання в роботу системи.

Ще одним напрямом розвитку є гібридизація охоронних технологій. На ринку зростає інтерес до пристроїв, які поєднують активні інфрачервоні промені з LiDAR-технологіями, відеоаналітикою або іншими засобами просторового контролю. Такі рішення дають змогу формувати умовні «віртуальні стіни», які можуть ефективно працювати на складних територіях, де традиційні фізичні бар'єри або класичні датчики не завжди забезпечують достатній рівень контролю.

### **1.5 Обґрунтування доцільності розробки та формування технічних вимог до системи**

На основі проведеного аналізу сучасних засобів охорони та існуючих комерційних аналогів, можна сформулювати обґрунтування для розробки власної системи інфрачервоного бар'єра, а також визначити перелік технічних вимог до неї.

Розробка власної системи інфрачервоного бар'єра є доцільною з огляду на потребу у створенні доступного, гнучкого та енергоефективного рішення для

охорони периметра. Комерційні системи відомих світових виробників, зокрема Optex і Takex, зазвичай мають високу вартість, що обмежує їх використання малим бізнесом, приватними домогосподарствами або невеликими об'єктами. Власна розробка на базі сучасних мікроконтролерів дає змогу суттєво знизити собівартість системи, зберігши при цьому основні функції виявлення перетину контрольованої зони.

Важливою перевагою власної системи є можливість гнучкого налаштування під конкретні умови експлуатації. На відміну від багатьох закритих комерційних рішень, розроблена система може бути адаптована до особливостей місцевості, рівня освітлення, наявності рослинності, домашніх тварин або інших чинників, що можуть спричиняти хибні спрацювання. Це дає змогу змінювати алгоритми обробки сигналу та параметри чутливості відповідно до реального середовища використання.

Додатковим аргументом на користь власної розробки є можливість інтеграції з сучасними IoT-протоколами та цифровими сервісами. Якщо більшість бюджетних аналогів обмежуються лише релейним виходом, то власна система може бути безпосередньо підключена до екосистеми «розумного дому», локального сервера або хмарної платформи моніторингу. Використання Wi-Fi, LoRaWAN або інших бездротових технологій відкриває можливість віддаленого контролю стану бар'єра, отримання сповіщень і ведення журналу подій.

Окрему практичну цінність має забезпечення енергонезалежності системи. Застосування низькоспоживаючих компонентів, енергоефективних мікроконтролерів і сонячних панелей дає змогу створити автономний охоронний вузол, який може працювати на віддалених ділянках периметра без постійного підключення до електромережі. Це особливо актуально для приватних територій, складів, аграрних об'єктів, промислових майданчиків або інших зон, де прокладання кабельної інфраструктури є складним чи економічно невиправданим.

Технічні вимоги до розроблюваної системи визначаються необхідністю забезпечення стабільної та надійної охорони периметра в різних умовах експлуатації. Основою системи має бути активний інфрачервоний бар'єр, що складається з передавача та приймача. Для зменшення кількості хибних спрацювань доцільно передбачити використання не менше двох інфрачервоних променів, оскільки це дозволяє краще відрізнити реальне перетинання контрольованої зони від випадкового потрапляння дрібних об'єктів, листя або комах.

Розроблювана система повинна забезпечувати стабільну роботу на відкритому просторі на відстані приблизно 50-100 метрів. Важливою умовою є використання алгоритму модуляції інфрачервоного сигналу, наприклад на частоті 38 кГц. Це дає змогу підвищити стійкість системи до зовнішніх перешкод, зокрема сонячного засвічення або спроб імітації сигналу сторонніми джерелами інфрачервоного випромінювання. Крім того, система повинна мати можливість налаштування часу реакції на переривання променя в межах від 50 мс до 500 мс, що дозволить адаптувати її до різних сценаріїв охорони.

З конструктивної та експлуатаційної точки зору система має бути придатною для використання на відкритому повітрі. Для цього корпус передавача та приймача повинен мати клас захисту не нижче IP65, що забезпечує захист від пилу та струменів води. Також необхідно передбачити стабільну роботу пристрою в широкому температурному діапазоні, орієнтовно від  $-25^{\circ}\text{C}$  до  $+50^{\circ}\text{C}$ . Живлення системи доцільно реалізувати з можливістю роботи від акумулятора, сонячної панелі або зовнішнього джерела напругою 12 В, що підвищить автономність і гнучкість використання охоронного бар'єра.

Окрему увагу слід приділити інтерфейсам, індикації та засобам оповіщення. Для спрощення монтажу й налаштування системи доцільно передбачити світлову LED-індикацію, яка допомагатиме виконувати юстування, тобто точне вирівнювання інфрачервоних променів між передавачем і приймачем. Вихідні сигнали системи мають передбачати як класичний

релейний вихід типу «сухий контакт», так і цифровий інтерфейс, наприклад UART або Wi-Fi, для передавання даних на центральний охоронний хаб чи іншу систему моніторингу.

Для підвищення надійності охоронного рішення необхідно також передбачити елементи антисаботажного захисту. Система повинна виявляти спроби розкриття корпусу, блокування сигналу приймача або інші дії, спрямовані на порушення її роботи. Наявність тамперного контакту, контролю стану променя та фіксації аномальних режимів роботи дозволить підвищити стійкість ІЧ-бар'єра до навмисного втручання та зробить його більш придатним для практичного використання в системах периметрової охорони.

## РОЗДІЛ 2

### ПРОЕКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ

#### 2.1 Розробка структурної та функціональної схем інфрачервоного бар'єра

Для реалізації надійної системи охорони периметра необхідно сформувати архітектуру, у якій апаратні модулі передавача та приймача працюють як єдиний канал виявлення перетину контрольованої зони. Така архітектура має забезпечувати стабільне формування інфрачервоного випромінювання, його приймання, фільтрацію від зовнішніх завад, логічну обробку сигналу та передавання тривожного повідомлення до виконавчого або інформаційного модуля.

Структурно система складається з двох територіально рознесених вузлів – передавального та приймального. Передавальний вузол формує модульований інфрачервоний сигнал і спрямовує його у бік приймача. До його складу входять джерело живлення, генератор імпульсів, драйвер ІЧ-діода та інфрачервоний випромінювач із фокусувальною оптикою. Генератор імпульсів формує несучу частоту, наприклад 38 кГц, що дозволяє приймальному вузлу відрізнити корисний сигнал від сонячного світла, освітлювальних приладів та інших фонових джерел випромінювання. Драйвер ІЧ-діода забезпечує необхідний струм випромінювача та стабільну потужність променя на заданій дистанції.

Приймальний вузол виконує перетворення оптичного сигналу в електричний, його підсилення, фільтрацію та логічний аналіз. Основними елементами цього вузла є фотодетектор, підсилювач-фільтр, компаратор або мікроконтролерний обробник, а також вихідний інтерфейс. Фотодетектор сприймає інфрачервоне випромінювання, після чого сигнал надходить на підсилювач із частотною селекцією. Фільтр виділяє корисну складову на частоті модуляції та пригнічує низькочастотні перешкоди, імпульсні шуми й випадкові зміни освітленості. Мікроконтролер аналізує факт наявності або втрати сигналу,

тривалість переривання променя та приймає рішення про формування тривожної події. (рис. 2.1)

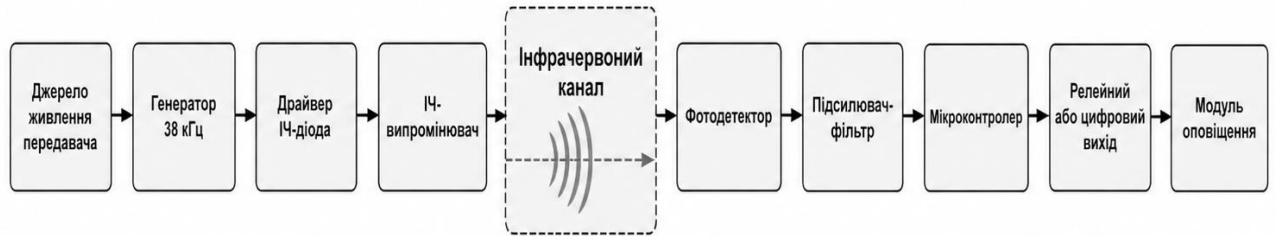


Рисунок 2.1 – Логіка проходження сигналу

Функціональна логіка роботи системи базується на порівнянні прийнятого сигналу з еталонними параметрами. Для підвищення завадостійкості доцільно використовувати амплітудну маніпуляцію ООК, за якої передавач формує не постійне випромінювання, а послідовність імпульсних пакетів. Приймач у такому випадку реагує не на будь-яке ІЧ-випромінювання, а саме на сигнал із заданою частотою та часовою структурою. Це зменшує ймовірність хибного спрацювання від зовнішнього освітлення або стороннього інфрачервоного джерела.

Важливим елементом функціональної схеми є часова селекція. Короткочасне переривання променя, спричинене комахою, листям або випадковою перешкодою, не повинно формувати тривогу. Для цього мікроконтролер вимірює тривалість втрати сигналу. Якщо час переривання менший за встановлений поріг, наприклад 50 мс, подія ігнорується. Якщо ж промінь заблокований довше заданого інтервалу, наприклад у межах 50-500 мс або більше, система розцінює це як реальне перетинання контрольованої зони та активує вихідний сигнал тривоги.

Режим юстування є окремою функціональною частиною системи. Під час монтажу необхідно точно сумістити оптичні осі передавача та приймача, тому до схеми доцільно включити індикатор рівня прийнятого сигналу. Це може бути LED-шкала, одиночний світлодіодний індикатор або звуковий сигналізатор,

який змінює режим роботи залежно від амплітуди прийнятого сигналу. Такий вузол спрощує налаштування системи на об'єкті та дозволяє досягти максимальної стабільності інфрачервоного каналу.

Розроблена архітектура (рис. 2.2) є масштабованою, оскільки дозволяє використовувати кілька пар «передавач-приймач» на одному об'єкті. Для зменшення взаємного впливу між каналами кожна пара може працювати з різною частотою модуляції, різним часовим кодом або окремою логікою синхронізації. Це особливо важливо для складних периметрів із поворотами, перепадами висот, кількома охоронними зонами та ділянками з різними умовами проходження сигналу. Таким чином, запропонована структурно-функціональна схема забезпечує не лише базове виявлення перетину променя, а й можливість побудови багатозонної системи периметрової охорони.

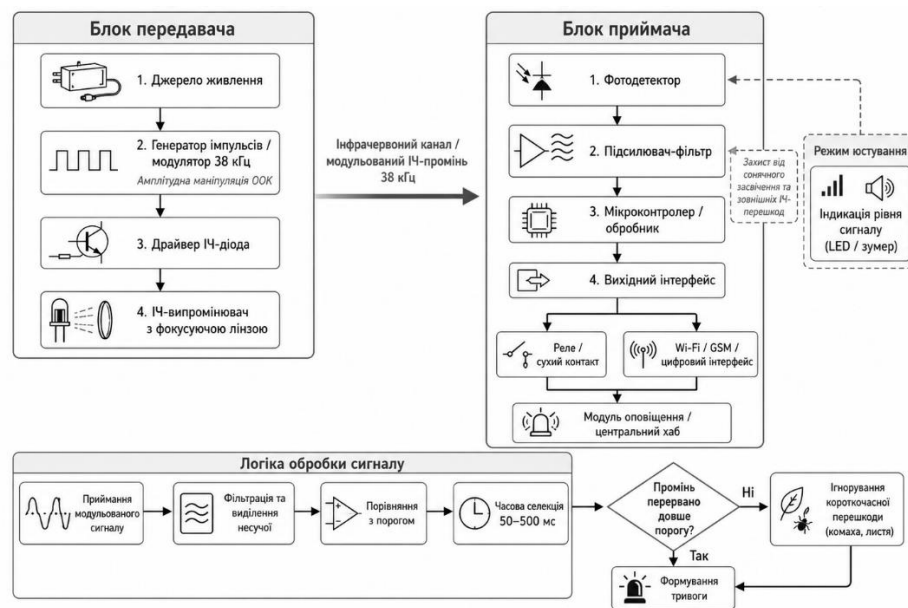


Рисунок 2.2 – Структурно-функціональна схема

## 2.2 Вибір та обґрунтування апаратної елементної бази

Для реалізації спроектованої схеми інфрачервоного бар'єра обрано елементну базу (таблиця 2.1), яка забезпечує збалансоване співвідношення надійності, енергоефективності, вартості та можливості подальшого

розширення системи. Основний акцент зроблено на стабільній роботі в умовах зовнішнього середовища, захисті від сонячних перешкод, підтримці модульованого інфрачервоного сигналу та можливості автономного живлення.

Таблиця 2.1 – Зведена таблиця основних параметрів обраних компонентів

Компонент	Модель	Робочий параметр	Призначення
Мікроконтролер	ESP32	3.3V / Dual Core	Логіка, Wi-Fi зв'язок
ІЧ-випромінювач	TSAL6100	940 nm / 10°	Генерація невидимого променя
ІЧ-приймач	TSOP34838	38 kHz Filter	Прийом та демодуляція сигналу
Джерело живлення	Li-ion 18650	3.7V / 3000mAh	Автономна робота
Корпус	ABS Plastic	IP65	Захист від вологи та пилу

Центральним елементом керування системою є мікроконтролер ESP32-WROOM-32. Його використання є доцільним, оскільки цей модуль, на відміну від класичних плат на базі ATmega328, має вбудовані інтерфейси Wi-Fi та Bluetooth. Це дає змогу реалізувати дистанційне передавання повідомлень про стан охоронного бар'єра без використання додаткових комунікаційних модулів. Крім того, достатня продуктивність ESP32 і тактова частота до 240 МГц дозволяють точно формувати імпульсні сигнали, зокрема частоту модуляції 38 кГц, необхідну для роботи інфрачервоного каналу. Важливою перевагою є також підтримка енергозберігаючих режимів, зокрема Deep Sleep, що є суттєвим для автономних систем із живленням від акумулятора.

У передавальному блоці як джерело інфрачервоного випромінювання доцільно використати ІЧ-світлодіод TSAL6100. Цей компонент працює на довжині хвилі 940 нм, яка є типовою для охоронних і дистанційних інфрачервоних систем, оскільки таке випромінювання невидиме для людського ока. Вузкий кут випромінювання дає змогу краще сфокусувати промінь у напрямку приймача, що важливо для роботи на збільшених відстанях. Завдяки достатній потужності випромінювання TSAL6100 може бути використаний у

складі активного ІЧ-бар'єра, де стабільність проходження променя напряму впливає на надійність виявлення перетину контрольованої зони.

Для приймального блоку доцільним є використання інтегрованого фотоприймача TSOP34838. Його перевага полягає в тому, що він поєднує в одному корпусі фотодетектор, підсилювач, смуговий фільтр на частоту 38 кГц і демодулятор. Це суттєво спрощує апаратну частину приймача, оскільки немає потреби окремо проєктувати складний аналоговий підсилювач і фільтрувальні каскади. На виході TSOP34838 формується готовий логічний сигнал, який може безпосередньо оброблятися мікроконтролером. Додатковою перевагою такого приймача є стійкість до оптичних перешкод, зокрема сонячного світла та люмінесцентних джерел освітлення.

Оскільки виходи мікроконтролера не розраховані на безпосереднє живлення потужного ІЧ-світлодіода струмом до 100 мА, у схемі необхідно використати окремий підсилювач струму. Для цього підходить біполярний транзистор 2N2222, який виконує роль ключового драйвера ІЧ-діода. Мікроконтролер керує базою транзистора, а сам транзистор забезпечує комутацію струму через інфрачервоний випромінювач. Такий підхід дозволяє зменшити навантаження на виводи ESP32 і забезпечити стабільну роботу випромінювача в імпульсному режимі.

Для автономного живлення системи доцільно застосувати акумулятор формату 18650 у поєднанні з контролером заряду TP4056 та сонячною панеллю на 5 В. Акумулятор забезпечує роботу системи у нічний час або за відсутності достатнього освітлення, а сонячна панель використовується для підзарядки протягом дня. Контролер TP4056 виконує функції заряджання літій-іонного елемента та захисту від перерозряду, що підвищує безпечність і довговічність джерела живлення. Така схема живлення дає змогу створити автономний охоронний вузол, придатний для використання на віддалених ділянках периметра без постійного підключення до електромережі.

Вибір даних компонентів дозволяє реалізувати систему, що стійка до погодних умов і здатна працювати у складі сучасного «розумного» периметра з мінімальним обслуговуванням.

### **2.3 Розробка принципової електричної схеми пристрою**

Принципова електрична схема системи визначає повний склад елементів, їх електричні параметри та взаємозв'язки між функціональними вузлами. Оскільки інфрачервоний бар'єр реалізується у вигляді двох просторово рознесених модулів, доцільно розглядати окремо схему передавального вузла, приймального вузла та підсистему живлення. Такий підхід дає змогу чітко відокремити функції генерації оптичного сигналу, приймання і аналізу променя, а також автономного енергозабезпечення.

Принципова схема передавального модуля орієнтована на формування стабільного модульованого інфрачервоного випромінювання. Джерелом керувального сигналу є мікроконтролер ESP32, один із цифрових виходів якого використовується для генерації прямокутного сигналу з частотою близько 38 кГц. Цей сигнал не може безпосередньо навантажувати потужний ІЧ-випромінювач, оскільки струм GPIO-виводів ESP32 обмежений і недостатній для забезпечення великої дальності дії. Саме тому між виходом мікроконтролера та ІЧ-світлодіодом передбачено ключовий підсилювальний каскад на транзисторі 2N2222. Транзистор працює в режимі електронного ключа та забезпечує комутацію імпульсного струму через випромінювач TSAL6100. Для коректної роботи каскаду використовується базовий резистор, який обмежує струм керування транзистором, а також резистор у колі ІЧ-діода, що задає робочий струм випромінювача та запобігає його термічному перевантаженню. У результаті передавач формує вузькоспрямовані пачки інфрачервоних імпульсів, придатні для стабільної передачі на значну відстань.

Приймальний модуль реалізує функцію виявлення інфрачервоного сигналу, його демодуляції, фільтрації та передачі до блоку цифрової обробки. Основним елементом цього вузла є інтегрований фотоприймач TSOP34838, який працює на частоті 38 кГц і містить усередині фотодетектор, попередній підсилювач, смуговий фільтр і демодулятор. Така інтеграція значно спрощує схему приймача, оскільки не потребує побудови окремих аналогових каскадів. Модуль живиться від напруги 3,3 В, сумісної з ESP32, а його вихід підключається безпосередньо до цифрового входу мікроконтролера. У нормальному режимі, коли модульований промінь стабільно досягає приймача, на виході формується один логічний стан, а при втраті сигналу внаслідок переривання променя - інший. Це дає змогу мікроконтролеру безпосередньо контролювати стан ІЧ-каналу та виконувати часовий аналіз тривалості блокування променя.

Для підвищення стабільності роботи приймального модуля у схемі доцільно передбачити локальну фільтрацію живлення. Конденсатор, підключений поблизу виводів живлення TSOP34838, разом із серійним або підтягувальним резистором формує елемент фільтрації, який знижує вплив імпульсних завад і пульсацій живлення. Це особливо важливо через наявність у системі ESP32 із вбудованим Wi-Fi-модулем, який може створювати додаткові електромагнітні перешкоди в колах живлення. Таким чином, застосування локальної розв'язки покращує завадостійкість і знижує ризик хибних спрацювань.

Мікроконтролер приймального вузла виконує не лише реєстрацію логічного стану виходу фотоприймача, а й логічну обробку події. Після фіксації зміни стану він вимірює тривалість відсутності модульованого сигналу та приймає рішення про формування тривоги. Якщо час переривання перевищує встановлений пороговий інтервал, на одному з виходів активується виконавчий пристрій. Як такий пристрій може бути використано релейний модуль для комутації зовнішньої сирени або п'єзокерамічний зумер для локального

звукового оповіщення. За потреби цей самий вузол може додатково передавати інформацію через Wi-Fi до зовнішньої системи моніторингу.

Підсистема живлення обох модулів має однакову загальну структуру та орієнтована на автономну роботу. Як джерело накопичення енергії застосовується літій-іонний акумулятор типорозміру 18650, а заряджання виконується через модуль TP4056. До його вхідних клем підключається сонячна панель, яка забезпечує поповнення заряду акумулятора у денний час. Модуль TP4056 контролює режим заряджання та, за наявності захисної версії, запобігає перерозряду акумулятора, що є критично важливим для збільшення строку служби батареї. Оскільки ESP32 та TSOP34838 потребують стабільної напруги 3,3 В, після акумулятора доцільно встановити лінійний стабілізатор напруги, наприклад AMS1117-3.3. Він забезпечує узгодження напруги живлення всіх електронних вузлів та стабільність функціонування системи в різних режимах навантаження.

З погляду практичної реалізації друкованої плати важливим є правильне трасування живильних і сигнальних ліній. Для зменшення впливу імпульсних струмів, що виникають у передавальному каскаді, доцільно розділяти силові та цифрові ділянки плати або, принаймні, мінімізувати спільні струмові контури. Особливу увагу слід приділити топології заземлення, оскільки помилки в цій частині можуть призвести до наведень, нестабільної роботи фотоприймача та зниження дальності системи. Окремо необхідно передбачити елементи локальної розв'язки живлення біля мікроконтролера, фотоприймача і стабілізатора.

Для спрощення монтажу та юстування до схеми доцільно включити допоміжний індикатор, зокрема світлодіод, який відображає наявність або рівень прийнятого сигналу. Такий індикатор дозволяє оператору під час встановлення передавача і приймача візуально контролювати момент точного суміщення оптичних осей. Це важливо, оскільки навіть незначне відхилення

напрямку випромінювання може призвести до зменшення амплітуди корисного сигналу та нестабільності роботи бар'єра.

Для захисту схеми від помилкового підключення живлення на вході доцільно застосувати діод Шотткі. Його включення в ланцюг живлення дозволяє запобігти пошкодженню електронних компонентів у разі переполюсовки акумулятора або джерела живлення. Використання саме діода Шотткі є виправданим завдяки малому прямому падінню напруги, що важливо для енергоощадних автономних систем.

Принципова електрична схема зображена на рисунку 2.3.

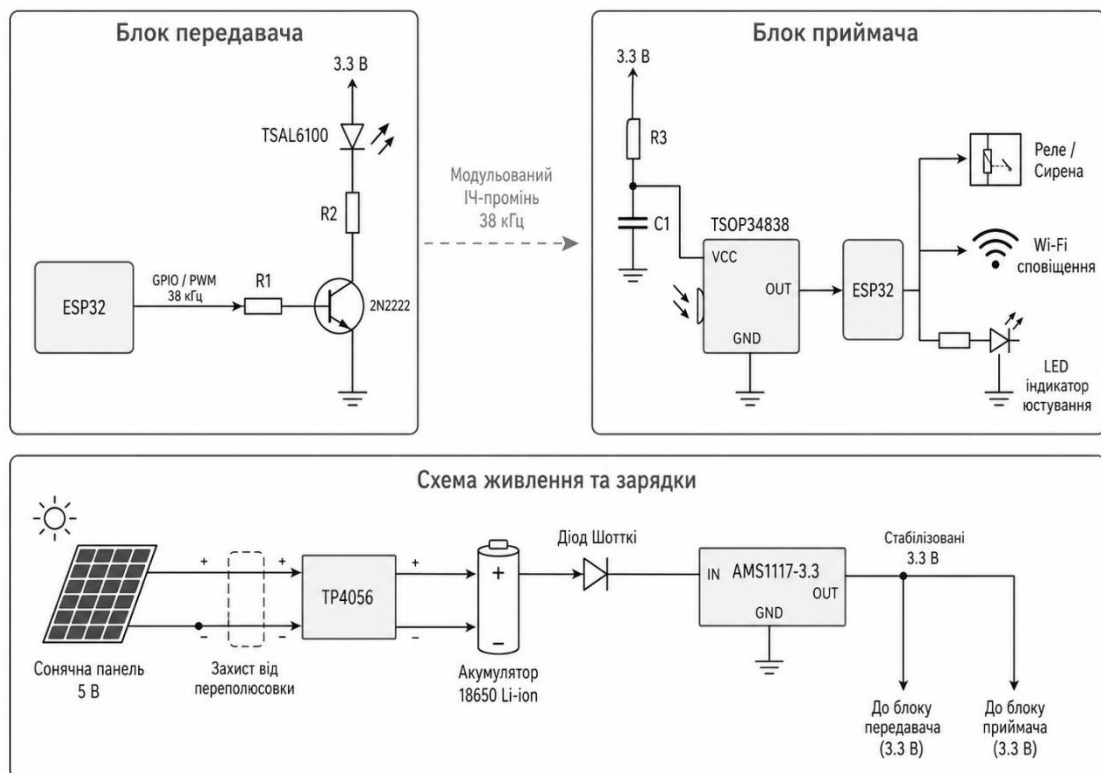


Рисунок 2.3 – Принципова електрична схема бар'єра

## 2.4 Проектування засобів захисту системи від хибних спрацьовувань

Для зменшення кількості хибних тривог у розроблюваній системі інфрачервоного бар'єра передбачено поєднання апаратних і програмних методів фільтрації сигналу. Основна проблема таких систем полягає в тому, що приймач

може реагувати не лише на корисний ІЧ-промінь від передавача, а й на зовнішні джерела випромінювання, погодні фактори, рух дрібних об'єктів або нестабільність самого оптичного каналу. Тому система повинна не просто фіксувати факт зміни сигналу, а аналізувати його частотні, часові та логічні характеристики.

Одним із ключових рішень є захист від оптичних перешкод. Пряме сонячне світло, відбиті промені або світло автомобільних фар можуть створювати паразитне інфрачервоне випромінювання, яке за певних умов здатне впливати на фотоприймач. Для усунення цього недоліку використовується приймальний модуль TSOP34838, який має вбудований смуговий фільтр, налаштований на частоту 38 кГц. Завдяки цьому приймач реагує не на будь-яке ІЧ-випромінювання, а саме на модульований сигнал із заданою частотою. Постійне або повільно змінне випромінювання, зокрема сонячне засвічення, не сприймається як корисний сигнал. Додатково фотоприймач доцільно розміщувати всередині непрозорого тубуса з вузьким входним отвором. Така конструкція обмежує кут огляду приймача та зменшує вплив бокових променів. Перед входною лінзою також може застосовуватися ІЧ-фільтр, який пропускає переважно випромінювання з довжиною хвилі понад 850 нм і блокує значну частину видимого спектра.

Стійкість до погодних умов забезпечується як енергетичним запасом передавача, так і правильним вибором приймального модуля. Туман, дощ, сніг або пил можуть розсіювати й послаблювати інфрачервоний промінь, унаслідок чого рівень сигналу на приймачі зменшується. Щоб система не втрачала працездатність у таких умовах, передавальний каскад розраховується з певним запасом потужності. ІЧ-світлодіод працює в імпульсному режимі через транзисторний драйвер, що дозволяє короткочасно формувати достатньо інтенсивний промінь без перевантаження виводів мікроконтролера. Навіть за часткового ослаблення сигналу приймач повинен отримувати достатній рівень модульованого випромінювання для коректної детекції. Водночас внутрішня

система автоматичного регулювання підсилення, яка реалізована в TSOP34838, дає змогу адаптуватися до зміни рівня фонового шуму. Конструктивно корпус передавача і приймача доцільно оснащувати козирком або захисним екраном, який не допускає прямого потрапляння крапель води, снігу чи бруду на оптичну частину.

Для відсікання хибних спрацювань, спричинених дрібними тваринами, птахами, комахами або листям, у системі застосовується часова селекція. Мікроконтролер ESP32 не формує тривогу одразу після короткого зникнення сигналу, а вимірює тривалість переривання променя. Якщо промінь був перекритий лише на короткий час, наприклад менше 100-200 мс, така подія розглядається як випадкова перешкода і не призводить до спрацювання сигналізації. Якщо ж переривання триває довше встановленого порогу, система інтерпретує його як імовірне проникнення людини або великого об'єкта в контрольовану зону. Такий підхід дозволяє значно зменшити кількість помилкових тривог без зниження чутливості до реального перетину периметра.

Більш надійним методом є використання геометричної селекції на основі подвійного променя. У цьому випадку система має два паралельні інфрачервоні канали, розміщені на різній висоті, наприклад із вертикальним рознесенням 20-30 см. Логіка прийняття рішення будується за принципом «І»: тривога формується лише тоді, коли обидва промені перериваються протягом заданого часового інтервалу. Це дозволяє ігнорувати ситуації, коли невеликий об'єкт перекриває лише один промінь. Наприклад, птах може перетнути верхній промінь, а дрібна тварина – нижній або простір під ним, але система не сформує тривогу, якщо не буде одночасного порушення обох каналів.

Програмна фільтрація на рівні ESP32 доповнює апаратні методи захисту. Мікроконтролер аналізує не лише факт наявності або відсутності сигналу, а й характер його зміни в часі. Якщо сигнал нестабільний, часто зникає та з'являється без чіткої картини перетину, така поведінка може бути класифікована як перешкода від гілок, рослинності або нестабільного

оптичного каналу. У цьому випадку система може не формувати тривогу, а видати службове попередження про перешкоду або потребу в юстуванні. Такий підхід підвищує інформативність системи, оскільки користувач отримує не лише сигнал «тривога», а й повідомлення про технічний стан бар'єра.

Окремо передбачається самодіагностика системи. Мікроконтролер може контролювати напругу живлення, тривалість відсутності стабільного сигналу, кількість короткочасних переривань і стан каналу зв'язку. Якщо рівень сигналу поступово знижується, це може свідчити про забруднення лінзи, розряд акумулятора, зміщення оптичної осі або погіршення погодних умов. У такому разі доцільно формувати сервісне повідомлення через Wi-Fi, а не одразу активувати тривожний вихід. Це дозволяє своєчасно виконати обслуговування системи та уникнути некоректної роботи в майбутньому.

## РОЗДІЛ 3

### ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

#### 3.1 Опис та розробка алгоритму функціонування системи

Алгоритм роботи мікропроцесорної системи інфрачервоного бар'єра побудований на циклічному контролі стану оптичного каналу між передавачем і приймачем. Його основне практичне призначення полягає не лише у фіксації факту переривання ІЧ-променя, а й у визначенні характеру цієї події. Програмна логіка повинна відрізнити короткочасну випадкову перешкоду, наприклад комаху, листя або краплю дощу, від реального перетину контрольованої зони людиною чи іншим значним об'єктом.

У передавальному блоці алгоритм є відносно простим, оскільки головне завдання цього вузла – сформувати стабільний модульований інфрачервоний сигнал. Після запуску системи мікроконтролер ESP32 ініціалізує відповідний GPIO-вивід і налаштовує таймер для генерації PWM-сигналу з частотою 38 кГц. Саме така частота вибрана тому, що вона відповідає робочому діапазону приймального модуля TSOP34838 і дозволяє відокремити корисний сигнал від фонового освітлення. Практично це означає, що приймач реагує не на будь-яке ІЧ-випромінювання, а лише на сигнал із заданою частотною структурою.

Для підвищення завадостійкості передавач може працювати не в режимі постійного випромінювання, а в режимі формування пакетів імпульсів. Наприклад, мікроконтролер формує інтервали активного випромінювання тривалістю 500 мкс, після яких іде пауза такої самої або заданої тривалості. Такий підхід полегшує приймачеві розпізнавання «свого» сигналу та знижує ризик помилкового спрацювання через сторонні джерела інфрачервоного випромінювання. У практичній реалізації це також дозволяє зменшити середнє енергоспоживання ІЧ-світлодіода та підвищити автономність передавального модуля.

Алгоритм приймального блока є складнішим, оскільки саме він виконує аналіз подій і приймає рішення про формування тривоги. Після запуску ESP32 ініціалізує цифровий вхід, до якого підключено вихід TSOP34838, а також налаштовує внутрішні таймери для вимірювання тривалості зникнення сигналу. У нормальному режимі система перебуває у стані «Охорона» та постійно контролює наявність модульованого ІЧ-променя. Якщо промінь присутній, тривожна подія не формується, а система продовжує моніторинг.

Коли приймач фіксує зникнення сигналу, мікроконтролер не активує тривогу миттєво, а запускає таймер початку переривання. Далі обчислюється тривалість розриву оптичного каналу. Цей параметр можна позначити як  $T_{gap}$ . Якщо сигнал відновлюється швидше, ніж за встановлений поріг, наприклад 100-200 мс, подія вважається короткочасною завадою і не впливає на стан охоронної системи. Такий підхід має важливе практичне значення, оскільки дозволяє уникати спрацювань через дрібні об'єкти, що випадково перетинають промінь.

Якщо ж сигнал відсутній довше заданого порогу, мікроконтролер переводить систему у стан «Тривога». У цьому режимі активується локальний виконавчий пристрій – реле, зумер або сирена. Паралельно ESP32 може сформувати повідомлення для передавання на сервер моніторингу або центральний охоронний хаб через Wi-Fi. Для цього в практичній реалізації можуть застосовуватися HTTP-запити, MQTT-повідомлення або інший простий протокол обміну даними. У повідомленні доцільно передавати ідентифікатор вузла, час події, тип події та поточний стан системи.

Для запобігання багаторазовим спрацюванням під час повільного перетину променя в алгоритмі передбачено гістерезис. Після того як промінь знову з'являється на приймачі, система не одразу повертається у нормальний режим, а очікує стабільного сигналу протягом 1-2 секунд. Якщо протягом цього часу сигнал не зникає повторно, стан «Тривога» скидається, а система повертається до режиму «Охорона». Такий механізм особливо важливий для реальних умов

експлуатації, коли порушник або рухомий об'єкт може частково перекривати промінь кілька разів поспіль.

Окремим режимом роботи є самодіагностика. Якщо модульований сигнал відсутній протягом тривалого часу, наприклад понад 10 секунд, система не повинна трактувати це лише як звичайну тривогу. Така ситуація може свідчити про несправність, втрату юстування, забруднення лінзи, розряд акумулятора або навмисне блокування приймача. У цьому випадку мікроконтролер формує службовий стан «Несправність» або «Саботаж» і передає відповідне повідомлення користувачу. Практично це дозволяє відрізнити коротку подію проникнення від технічної проблеми, яка потребує обслуговування системи.

Для монтажу та налаштування передбачено режим юстування. Він активується сервісною кнопкою або програмною командою. У цьому режимі ESP32 підвищує частоту оновлення LED-індикатора або зумера, який відображає якість приймання сигналу. Якщо передавач і приймач точно спрямовані один на одного, індикатор показує стабільний рівень приймання. Якщо промінь зміщений, індикатор працює нестабільно або сигналізує про недостатній рівень. Це спрощує практичне встановлення системи на об'єкті, особливо на відкритих ділянках периметра.

З погляду енергоспоживання алгоритм орієнтований на автономну роботу. ESP32 може перебувати в режимі зниженого енергоспоживання, а активні обчислення виконувати лише під час зміни стану на вході фотоприймача або в моменти планової перевірки системи. У приймальному модулі це дозволяє зменшити споживання від акумулятора, а в передавальному – оптимізувати роботу ІЧ-світлодіода за рахунок імпульсного режиму. У результаті система може тривалий час працювати від акумулятора з підзарядкою від сонячної панелі.

У практичній реалізації алгоритм можна подати як послідовність станів: «Ініціалізація», «Охорона», «Фіксація переривання», «Аналіз тривалості», «Тривога», «Самодіагностика», «Юстування» та «Повернення в охорону». Така структура є зручною для програмування, оскільки кожен стан має чітко визначені

умови входу, виконувані дії та умови переходу до наступного режиму. Це підвищує надійність програмного забезпечення та спрощує подальше тестування системи.

### 3.2 Розробка програмного забезпечення для базового мікроконтролера

Програмне забезпечення (лістинг 3.1) для ESP32 розроблено в середовищі Arduino IDE мовою C++, що дає змогу швидко перевіряти роботу алгоритму безпосередньо на апаратному прототипі. Основна увага в програмній частині приділена формуванню стабільного модульованого сигналу 38 кГц, оскільки саме на цю частоту налаштований приймальний модуль інфрачервоного бар'єра. Для передавального вузла використовується апаратний PWM-контролер ESP32, зокрема модуль LEDC, який формує несучу частоту у фоновому режимі без постійного навантаження на процесор. Це практично важливо, оскільки мікроконтролер може одночасно виконувати додаткові задачі, наприклад контролювати режим живлення, сервісну кнопку або змінювати параметри випромінювання. Такий підхід забезпечує стабільну роботу ІЧ-передачача, зменшує ризик дрейфу частоти та підвищує надійність приймання сигналу фотоприймачем.

Лістинг 3.1 – Код передавача

---

```
// Налаштування генерації 38 кГц для ІЧ-діода
const int ledPin = 18;      // Вихід на транзисторний драйвер
const int freq = 38000;    // Частота модуляції 38 кГц
const int ledChannel = 0;  // Канал ШІМ
const int resolution = 8;  // Роздільна здатність (8 біт)

void setup() {
    ledcSetup(ledChannel, freq, resolution);
    ledcAttachPin(ledPin, ledChannel);
    // Встановлюємо 50% робочий цикл (128 із 255)
    ledcWrite(ledChannel, 128);
}
```

```

}

void loop() {
    // Передавач працює безперервно або в імпульсному режимі для
економії
    delay(1000);
}

```

---

кінець лістингу 3.1

Структура коду приймача (лістинг 3.2) орієнтована на швидку фіксацію зміни стану фотоприймача TSOP34838 та подальшу часову перевірку цієї події. Для цього в ESP32 використовується механізм апаратних переривань, які спрацьовують у момент зміни логічного рівня на вході, підключеному до виходу фотоприймача. Такий підхід практично ефективніший за постійне опитування входу, оскільки мікроконтролер не витрачає ресурси на безперервну перевірку стану сигналу. У нормальному режимі ESP32 може перебувати в енергоощадному стані, а активна обробка запускається лише після переривання променя або зміни стану ІЧ-каналу. Це дозволяє зменшити споживання енергії приймального блока та підвищити автономність системи під час роботи від акумулятора.

#### Лістинг 3.2 – Код приймача

---

```

#define IR_PIN 14           // Вхід від TSOP34838
#define ALARM_PIN 26       // Вихід на реле/сирену
#define DEBOUNCE_TIME 150 // Поріг фільтрації перешкод (мс)
volatile bool motionDetected = false;
unsigned long lastInterruptTime = 0;
void IRAM_ATTR handleInterrupt() {
    motionDetected = true; // Фіксація розриву променя
}
void setup() {

```

```

pinMode(IR_PIN, INPUT_PULLUP);
pinMode(ALARM_PIN, OUTPUT);
// Налаштування переривання по зміні сигналу (Falling edge)
attachInterrupt(digitalPinToInterrupt(IR_PIN), handleInterrupt,
FALLING);
}
void loop() {
  if (motionDetected) {
    unsigned long currentTime = millis();
    // Перевірка: чи триває переривання довше за поріг фільтрації
    if (digitalRead(IR_PIN) == LOW && (currentTime -
lastInterruptTime > DEBOUNCE_TIME)) {
      sendAlarm(); // Функція відправки сповіщення через Wi-Fi
      digitalWrite(ALARM_PIN, HIGH);
      delay(2000); // Час активації тривоги
      digitalWrite(ALARM_PIN, LOW);
    }
    motionDetected = false;
    lastInterruptTime = currentTime;
  }
}
}

```

---

кінець лістингу 3.2

Функція мережевого оповіщення реалізується за рахунок вбудованого Wi-Fi-модуля ESP32, що дає змогу інтегрувати ІЧ-бар'єр у локальну систему моніторингу або «розумний дім». Після фіксації тривожної події мікроконтролер може сформувати HTTP POST-запит або MQTT-повідомлення, у якому передаються ідентифікатор пристрою, час спрацювання, стан променя та тип події. На практиці це дозволяє не обмежуватися лише локальним зумером чи реле, а передавати сигнал на сервер, мобільний застосунок або центральний охоронний хаб. Для економії заряду акумулятора після передавання повідомлення ESP32 може короткочасно переходити в режим Deep Sleep або

Light Sleep, особливо якщо порушення триває і немає потреби постійно дублювати однакові сповіщення. Така логіка підвищує автономність системи та робить її придатною для встановлення на віддалених ділянках периметра.

У процесі оптимізації програмного забезпечення важливо забезпечити стабільну роботу ESP32 в умовах можливих збоїв Wi-Fi-з'єднання, імпульсних завад і нестабільного живлення. Для цього використовується Watchdog Timer, який автоматично перезапускає мікроконтролер у разі зависання основного циклу або мережевого стека. Додатково в коді реалізується програмна фільтрація коротких імпульсних сплесків на виході фотоприймача, що дозволяє відсікати випадковий шум і «брязкіт» сигналу. Практичним доповненням є підтримка OTA-оновлення, завдяки якій прошивку можна оновлювати через Wi-Fi без фізичного підключення до плати. У результаті програмний комплекс перетворює набір електронних компонентів на автономний інтелектуальний датчик, здатний виявляти події, фільтрувати завади, передавати сповіщення та підтримувати віддалене обслуговування.

### **3.3 Практична реалізація дослідного зразка (макета) системи охорони**

На завершальному етапі проєктування було виконано складання та первинне тестування фізичного прототипу інфрачервоного бар'єра. Практична реалізація дала змогу перевірити працездатність передавального та приймального модулів, оцінити стабільність проходження ІЧ-променя на відкритій ділянці та уточнити параметри чутливості. Під час тестування особливу увагу було приділено впливу зовнішнього освітлення, точності юстування оптичних осей і стабільності роботи приймача за різних відстаней між блоками.

Первинну перевірку схеми було виконано на безпайковій макетній платі. Такий підхід дозволив швидко перевірити логіку роботи мікроконтролера ESP32, ІЧ-випромінювача, приймального модуля та виконавчих елементів без

виготовлення остаточної плати. На цьому етапі було протестовано генерацію модульованого сигналу 38 кГц, реакцію фотоприймача на переривання променя та роботу програмної фільтрації короткочасних перешкод.

Оскільки система призначена для використання на відкритому повітрі, конструктивне виконання прототипу орієнтоване на захист від пилу, вологи та механічних впливів. Для розміщення електроніки використано герметичні корпуси з ABS-пластику з рівнем захисту IP65. Такий корпус дає змогу експлуатувати модулі в умовах підвищеної вологості, дощу та пилового забруднення. Навпроти ІЧ-випромінювача та фотоприймача встановлено оптичні вікна, прозорі для інфрачервоного діапазону, що забезпечує проходження робочого сигналу без суттєвого послаблення.

Для підвищення спрямованості оптичного каналу всередині корпусів використано пластикові циліндричні бленди, які виконують роль тубусів. Вони обмежують кут огляду приймача, зменшують вплив бокового засвічення та полегшують формування вузького ІЧ-променя між передавачем і приймачем. Конструкція корпусів передбачає також поворотні кронштейни, які дають змогу регулювати положення блоків у горизонтальній і вертикальній площинах. Діапазон регулювання в межах приблизно  $\pm 15^\circ$  є достатнім для практичного юстування системи під час монтажу на стіні, стійці або огороженні.

Одним із найважливіших етапів практичного налаштування є точне суміщення оптичних осей передавача та приймача. Для попереднього вирівнювання було використано метод «видимого світла», коли паралельно до осі інфрачервоного випромінювання тимчасово встановлювався лазерний вказівник. Це дало змогу швидко зорієнтувати блоки один відносно одного до початку електронного налаштування. Після грубого вирівнювання виконувалася точніша юстировка за допомогою сервісного режиму приймача.

У програмному забезпеченні було передбачено режим «Service Mode», у якому яскравість сервісного LED-індикатора на приймальному блоці змінюється залежно від рівня або стабільності прийнятого сигналу. Це дало змогу

монтажнику візуально оцінювати якість наведення без підключення додаткових вимірювальних приладів. Під час налаштування блоки поступово поверталися до положення, у якому індикатор демонстрував найбільш стабільний стан приймання. За результатами тестування вдалося досягти стійкої роботи оптичного каналу на дистанції близько 40 метрів, що підтверджує придатність обраної елементної бази та конструктивного рішення для практичного використання.

У ході випробувань макета було отримано результати зображені в таблиці 3.1.

Таблиця 3.1 – Результати тестування приладу

Параметр	Значення (замір)	Коментар
Максимальна дальність	65 метрів	У сонячну погоду; стабільна детекція.
Струм споживання (Tx)	45 мА	В імпульсному режимі модуляції.
Час реакції	120 мс	Оптимально для детекції людини (відсікає птахів).
Автономність	до 14 діб	Без підзарядки від сонця (акумулятор 3000 mAh).

### **3.4 Методика тестування, аналіз результатів експериментальних досліджень**

Для підтвердження працездатності розробленого інфрачервоного бар'єра було проведено серію експериментальних випробувань, спрямованих на перевірку стабільності роботи системи в умовах, наближених до реальної експлуатації. Основну увагу під час тестування було зосереджено на визначенні максимальної дальності дії, стійкості до оптичних завад, здатності системи відрізнити випадкові перешкоди від реального перетину променя, а також на оцінюванні енергоспоживання в різних режимах роботи.

Експериментальні дослідження проводилися на відкритій місцевості з використанням дослідного зразка системи, що складається з передавального та

приймального модулів. Перед початком випробувань було виконано юстування оптичних осей, перевірено стабільність генерації модульованого ІЧ-сигналу з частотою 38 кГц та протестовано реакцію приймального модуля на переривання променя. Відстань між передавачем і приймачем поступово збільшувалася, після чого фіксувалося, за яких умов система зберігає стабільний логічний стан «Норма» без випадкових втрат сигналу.

Під час перевірки максимальної дальності було встановлено, що за сприятливих умов, зокрема у сутінках або за ясної погоди без прямого сонячного засвічення, система забезпечує стабільну роботу на відстані приблизно 30-50 м. У таких умовах рівень оптичного шуму є мінімальним, а модульований сигнал від ІЧ-випромінювача впевнено реєструється приймальним модулем. При яскравому полуденному сонці дальність стабільної роботи зменшувалася до 20-30 м, що пояснюється підвищенням рівня фонового інфрачервоного випромінювання та додатковим навантаженням на систему фільтрації приймача.

Окремо було проведено тестування стійкості системи до умов зниженої прозорості середовища. Для імітації туману використовувався напівпрозорий фільтр, який частково послаблював інтенсивність ІЧ-променя. За таких умов стабільна детекція зберігалася на відстані до 35 м. Отриманий результат підтверджує, що атмосферні завади істотно впливають на дальність роботи інфрачервоного бар'єра, тому під час практичного монтажу необхідно передбачати запас потужності передавача та не використовувати систему на граничній відстані.

Також було виконано тест селекції об'єктів. Для цього моделювалися різні сценарії перетину променя: короткочасне перекриття малим об'єктом, швидкий проліт предмета через контрольовану зону та повільний перетин людиною. Як малий об'єкт використовувався тенісний м'яч, що імітував птаха або іншу випадкову перешкоду. Завдяки програмній затримці спрацювання на рівні 150 мс система не формувала тривогу при короткочасних перериваннях сигналу. Це

підтвердило ефективність часової селекції для відсікання швидких і малорозмірних об'єктів.

Під час імітації реального проникнення, коли людина перетинала промінь із нормальною швидкістю кроку, система стабільно переходила у стан «Тривога». Імовірність детекції у таких умовах становила близько 0,98, що свідчить про достатню надійність алгоритму розпізнавання тривалого переривання променя. Невелика частка пропусків може бути пов'язана з неповним перекриттям оптичної осі, неточністю юстування або особливостями кута перетину променя.

Для оцінки автономності було проведено вимірювання струму споживання в основних режимах роботи. Окремо аналізувалися режим очікування, режим активної передачі ІЧ-сигналу та режим Wi-Fi-сповіщення. Найменше енергоспоживання спостерігалось у стані очікування, тоді як найбільше навантаження на акумулятор створювалося під час передавання мережевого повідомлення через Wi-Fi. Це підтверджує доцільність використання коротких сеансів зв'язку та переходу ESP32 в енергоощадний режим після завершення передавання даних. (таблиця 3.2)

Таблиця 3.2 – Узагальнені результати тестувань

Тип об'єкта	Швидкість перетину	Результат (Тривога)	Коментар
Птах / Листя	> 5 м/с	Ні	Відсікається таймером
Людина (біг)	3-5 м/с	Так	Миттєва реакція
Людина (крок)	1-2 м/с	Так	Чітка фіксація
Дрібна тварина	< 0.5 м/с	Ні	Проходить під променем

Оцінка енергоефективності розробленої системи показала, що основне навантаження на джерело живлення створює передавальний модуль Tx, оскільки ІЧ-випромінювач працює в імпульсному модульованому режимі практично постійно. Середній струм споживання передавача становив близько 35 мА, що є прийнятним значенням для автономного вузла з живленням від Li-ion акумулятора 18650. Таке споживання пояснюється роботою ІЧ-світлодіода

TSAL6100 через транзисторний драйвер, який забезпечує достатню потужність випромінювання для стабільної роботи оптичного каналу.

Приймальний модуль Rx у режимі очікування споживає значно менше енергії – приблизно 12 мА. У цьому стані основне навантаження формують мікроконтролер ESP32, фотоприймач TSOP34838 та допоміжні елементи індикації. Водночас під час передавання тривожного повідомлення через Wi-Fi струм короткочасно зростає до 180 мА. Це пов'язано з активацією радіомодуля ESP32, який у момент підключення до мережі та передавання даних має пікове енергоспоживання. Саме тому в програмній логіці доцільно використовувати короткі сеанси зв'язку та переводити мікроконтролер у режим енергозбереження після завершення передавання повідомлення.

Результати експериментальних досліджень підтвердили, що розроблена система загалом відповідає вимогам до автономного інфрачервоного бар'єра охорони периметра. Програмна фільтрація короткочасних переривань променя ефективно зменшує кількість хибних спрацювань від дрібних об'єктів, листя, комах або випадкових перешкод. Практична дальність роботи понад 50 м є достатньою для більшості приватних, складських, промислових і господарських об'єктів, де потрібно контролювати окремі ділянки периметра без прокладання складної кабельної інфраструктури.

Важливим результатом є підтвердження стабільності роботи системи за інтенсивного сонячного освітлення. Завдяки використанню модуляції 38 кГц і приймального модуля з частотною селекцією система зберігає здатність відрізнити корисний ІЧ-сигнал від фонового оптичного шуму. Водночас експерименти показали, що погодні умови та рівень засвічення суттєво впливають на граничну дальність роботи, тому під час монтажу доцільно мати запас за відстанню та не розміщувати передавач і приймач на межі максимально можливої дистанції.

Аналіз результатів також показав напрями подальшого вдосконалення системи. Найперспективнішим є застосування фокуруючих лінз Френеля або

спеціалізованої оптики для ІЧ-випромінювача та приймача. Це дозволить збільшити концентрацію променя, підвищити рівень сигналу на приймальній стороні та розширити робочу дистанцію до 100-120 м без істотного збільшення енергоспоживання. Додатково доцільно реалізувати адаптивне налаштування порогу спрацювання, моніторинг рівня заряду акумулятора та автоматичне сервісне повідомлення у разі забруднення лінзи або втрати юстування.

## ВИСНОВКИ

У ході виконання кваліфікаційної роботи було розроблено та практично реалізовано автономну систему інфрачервоного бар'єра для охорони периметра. На основі проведених досліджень та експериментів можна стверджувати, що мета роботи досягнута, а поставлені завдання виконані в повному обсязі, а саме:

Проаналізовано сучасний стан та тенденції розвитку технічних засобів охорони периметра. Встановлено, що ринок зміщується в бік інтелектуальних мультисенсорних систем (PIDS), де ключову роль відіграє поєднання класичної детекції з цифровою обробкою сигналів та IoT-технологіями.

Досліджено фізичні основи роботи активних інфрачервоних систем. Визначено, що використання модуляції несучої частоти 38 кГц є найбільш ефективним методом захисту від природних та штучних оптичних перешкод. Класифіковано існуючі бар'єри за дальністю та конфігурацією променів.

Обґрунтовано вибір апаратної бази. Для реалізації системи обрано мікроконтролер ESP32, який забезпечує необхідну обчислювальну потужність та наявність бездротових інтерфейсів. Використання високопотужних ІЧ-діодів TSAL6100 та інтегрованих фотоприймачів TSOP34838 дозволило досягти високої чутливості системи.

Розроблено структурну, функціональну та принципову електричні схеми. Спроектвана архітектура забезпечує стабільну роботу двох територіально рознесених модулів (передавача та приймача) з можливістю автономного живлення від літій-іонних акумуляторів та сонячних панелей.

Спроектовано засоби захисту від хибних спрацювань. Впроваджено апаратні рішення (оптичні тубуси, ІЧ-фільтри) та програмні алгоритми часової селекції (фільтрація сигналів коротших за 150 мс), що дозволило системі ігнорувати птахів, листя та опади, чітко фіксуючи перетин межі людиною.

Розроблено програмне забезпечення для мікроконтролера ESP32. Програма реалізує стабільну генерацію частоти модуляції, енергоефективну

обробку переривань від датчиків та протокол передачі тривожних сповіщень у локальну мережу Wi-Fi.

Виготовлено дослідний зразок та проведено експериментальні дослідження. Тестування в реальних умовах підтвердило стабільну дальність роботи системи до 55-65 метрів при сонячному освітленні та високу імовірність детекції (0,98) при мінімальній кількості хибних тривог.

Результати роботи мають практичне значення для побудови бюджетних, але високонадійних систем безпеки віддалених об'єктів. Спроектований пристрій може бути інтегрований у комплексну систему «Розумний будинок» або використаний як самостійний вузол охорони периметра. Перспективи подальшого розвитку теми полягають у використанні лінз Френеля для збільшення дальності дії та впровадженні протоколу LoRaWAN для роботи на надвеликих відстанях без використання Wi-Fi інфраструктури.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Perimeter Protection of the Areas of Interest. 2021. URL: [https://www.researchgate.net/publication/357294759\\_Perimeter\\_Protection\\_of\\_the\\_Areas\\_of\\_Interest](https://www.researchgate.net/publication/357294759_Perimeter_Protection_of_the_Areas_of_Interest) (дата звернення: 28.12.2025).
2. Secured Perimeter with Electromagnetic Detection and Tracking with Drone Embedded and Static Cameras. *Sensors*. 2021. Vol. 21, No. 21. Article 7379. URL: <https://www.mdpi.com/1424-8220/21/21/7379> (дата звернення: 28.12.2025).
3. Infrared Beam Barriers: Invisible Security for Perimeter Protection. LinkedIn. 2025. URL: <https://www.linkedin.com/pulse/infrared-beam-barriers-invisible-security-perimeter-protection-salim-nfdic> (дата звернення: 12.01.2026).
4. Zone or point detection for better perimeter security? Optex Europe. 2022. URL: <https://www.optex-europe.com/about/in-the-media/zone-or-point-detection-for-better-perimeter-security> (дата звернення: 28.12.2025).
5. Trends In Perimeter Security: Safeguarding The First Line Of Defense. 2025. URL: <https://isrmag.com/trends-in-perimeter-security-safeguarding-the-first-line-of-defense> (дата звернення: 15.02.2026).
6. Infrared Barriers Market Growth Drivers and Key Trends [Electronic resource]. LinkedIn. 2025. URL: <https://www.linkedin.com/pulse/infrared-barriers-marketkey-insights-trends-drivers-regional-ze0hc> (дата звернення: 15.02.2026).
7. Perimeter Security Utilizing Thermal Object Detection. ResearchGate. 2025. URL: [https://www.researchgate.net/publication/397226487\\_Perimeter\\_Security\\_Utilizing\\_Thermal\\_Object\\_Detection](https://www.researchgate.net/publication/397226487_Perimeter_Security_Utilizing_Thermal_Object_Detection) (дата звернення: 20.03.2026).
8. Active Infrared Sensor vs Passive Infrared Sensor in Perimeter Intrusion Detection Systems. Gato Security. 2025. URL: <https://www.gato-security.com/active-infrared-sensor-vs-passive-infrared-sensor-in-perimeter-intrusion-detection-systems> (дата звернення: 20.03.2026).

9. Perimeter Security Utilizing Thermal Object Detection. *Sensors*. 2025. Vol. 25, No. 21. Article 6680. URL: <https://www.mdpi.com/1424-8220/25/21/6680> (дата звернення: 25.04.2026).

10. Perimeter Intrusion Detection by Video Surveillance. *Sensors*. 2022. Vol. 22, No. 9. Article 3601. URL: <https://www.mdpi.com/1424-8220/22/9/3601> (дата звернення: 25.12.2025).

11. Adversarial Infrared Curves: An Attack on Infrared Pedestrian Detectors in the Physical World. *arXiv*. 2024. URL: <https://arxiv.org/abs/2312.14217> (дата звернення: 24.03.2026).

12. Adversarial Infrared Curves: An Attack on Infrared Pedestrian Detectors in the Physical World. *arXiv*. 2024. URL: <https://arxiv.org/pdf/2312.14217> (дата звернення: 24.03.2026).

13. Multi-sensor Intrusion Detector System. *arXiv*. 2024. URL: <https://arxiv.org/pdf/2406.05137> (дата звернення: 02.02.2026).

14. PIDS Certified Grade-4 Perimeter Intrusion Detection Systems. *Sicurit*. 2024. URL: [https://sicurit-pps.it/wp-content/uploads/2024/09/PIDS\\_brochure\\_PPS\\_Riyahd\\_2024\\_v09.pdf](https://sicurit-pps.it/wp-content/uploads/2024/09/PIDS_brochure_PPS_Riyahd_2024_v09.pdf) (дата звернення: 02.02.2026).

15. A Survey on Multi-Sensor Fusion Perimeter Intrusion Detection in High-Speed Railways. *Sensors*. 2024. Vol. 24, No. 17. Article 5463. URL: <https://www.mdpi.com/1424-8220/24/17/5463> (дата звернення: 04.01.2026).

16. Solar Based Perimeter Intrusion Detection System with Integration of SMS and Alarm System. *ResearchGate*. 2023. URL: [https://www.researchgate.net/publication/373990398\\_Solar\\_Based\\_Perimeter\\_Intrusion\\_Detection\\_System\\_with\\_Integration\\_of\\_SMS\\_and\\_Alarm\\_System](https://www.researchgate.net/publication/373990398_Solar_Based_Perimeter_Intrusion_Detection_System_with_Integration_of_SMS_and_Alarm_System) (дата звернення: 04.01.2026).

17. A Survey on Multi-Sensor Fusion Perimeter Intrusion Detection in High-Speed Railways. *PubMed Central*. 2024. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11397917/> (дата звернення: 25.04.2026).