

ІНЦЗФН

Кафедра *інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА Пояснювальна записка

рівень вищої освіти *перший (бакалаврський)*

Розробка модульної системи захисту від FPV-дронів

(тема)

Виконав:

здобувач *3* року навчання,
групи *ТРИМІзу-23-1*

Євген Перістий

(власне ім'я, прізвище)

Спеціальність *172 Електронні комунікації
та радіотехніка*

(код і повна назва спеціальності)

Тип програми *освітньо-професійна*

Освітня програма *Інформаційно-мережна
інженерія*

(повна назва освітньої програми)

Керівник *доц. к.т.н. Дарія Чеботарьова*

(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ІМІ

(підпис)

Микола МОСКАЛЕЦЬ

(власне ім'я, прізвище)

2026 р.

Не містить відомостей, заборонених до відкритого публікування

Студент

(підпис)

Євген Перістий

(власне ім'я, прізвище)

Керівник

(підпис)

Дарія Чеботарьова

(власне ім'я, прізвище)

Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра Інформаційно-мережної інженерії
(повна назва)

Рівень вищої освіти перший (бакалаврський)

Спеціальність 172 Електронні комунікації та радіотехніка
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ _____
(підпис)

“ 26 ” червня 2026р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Перістому Євгену Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка модульної системи захисту від FPV-дронів

затверджена наказом університету від “18” травня 2026 р. №74 Стз

2. Термін подання здобувачем роботи до екзаменаційної комісії 24 червня 2026 р.

3. Вихідні дані до роботи Проаналізувати сучасні засоби захисту від безпілотних літальних апаратів, визначити переваги та недоліки існуючих засобів. Виконати проєктування структури та принципу дії модульної системи захисту від FPV-дронів. Для розробки використати платформу Arduino, дешифратор 74НС138 та шинні формувачі 74НС245/74LS245. Розробити алгоритм та програмне забезпечення роботи модуля системи.

4. Перелік питань, що потрібно опрацювати в роботі _____

1. Аналіз засобів захисту від ворожих БПЛА

2. Проєктування структури та принципу дії модульної системи захисту від FPV-дронів

3. Опис апаратних та програмних засобів

4. Розробка алгоритму та програмного забезпечення модуля системи захисту

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

Слайди у форматі Power Point (назва, мета та задачі роботи, актуальність проблеми захисту від БПЛА в Україні, БПЛА військового типу, методи виявлення та нейтралізації ворожих дронів, порівняльний аналіз сучасних засобів захисту від FPV-дронів, структура та принцип дії запропонованої модульної системи, принцип роботи та функціональна схема модуля системи, апаратні та програмні засоби, алгоритм та програмна реалізація роботи модуля системи захисту, перевірка роботи програми на симуляторі SimulIDE, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	18.05.26	Виконано
2	Підбір літератури за темою роботи.	19.05 - 23.05.26	Виконано
3	Виконання розділу 1	24.05 - 31.05.26	Виконано
4	Виконання розділу 2	01.06 - 07.06.26	Виконано
5	Виконання розділу 3	08.06 - 13.06.26	Виконано
6	Виконання розділу 4	14.06 - 19.06.26	Виконано
7	Оформлення пояснювальної записки,		
	презентаційного матеріалу та підготовка		
	до захисту у ЕК	20.06 - 24.06.26	Виконано

Дата видачі завдання 18 травня 2026 р.

Здобувач _____
(підпис)

Керівник роботи _____
(підпис)

доц. Дарія Чеботарьова
(посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 83 с., 29 рис., 8 табл., 30 джерел, 3 додатки

Об'єкт дослідження – система захисту від FPV-дронів.

Мета роботи – проектування та розробка модульної системи захисту від ворожих FPV-дронів.

Результати – в роботі виконано аналіз сучасних засобів захисту від ворожих дронів, визначено переваги та недоліки існуючих засобів. Запропоновано модульну систему захисту від FPV-дронів, виконано проектування її структури та принципу дії, розроблено функціональну схему модуля системи захисту. Описано апаратні та програмні засоби потрібні для розробки модуля системи захисту, виконано розробку алгоритма та програми роботи модуля, роботу програми перевірено на симуляторі.

БПЛА, ДРОН, FPV-ДРОН, БЕЗПЕКА, ЗАХИСТ, СИСТЕМА, МОДУЛЬ, ARDUINO, ПРОТИДІЯ, ПРОГРАМА, IDE, SIMULIDE, СЕГМЕНТ, ПРОМІНЬ

THE ABSTRACT

Explanatory note: 83 p., 29 fig., 8 tabl., 30 sources, 3 app.

Object of research - a system for protecting against FPV drones.

The purpose of the work is to design and develop a modular system for protecting against hostile FPV drones.

Results - the work analyzes modern means of protecting against hostile drones, identifies the advantages and disadvantages of existing means. A modular system for protecting against FPV drones is proposed, its structure and principle of operation are designed, and a functional diagram of the protection system module is developed. The hardware and software required for the development of the protection system module are described, the algorithm and program for the module are developed, and the program is tested on a simulator.

UAV, DRONE, FPV-DRONE, SECURITY, PROTECTION, SYSTEM, MODULE, ARDUINO, COUNTERACTION, PROGRAM, IDE, SIMULIDE, SEGMENT, BEAM.

ЗМІСТ

	С.
ПЕРЕЛІК СКОРОЧЕНЬ.....	8
ВСТУП.....	9
1 АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ВІД ВОРОЖИХ БПЛА	11
1.1 Актуальність проблеми захисту від БПЛА в Україні	11
1.2 Огляд БПЛА військового типу	14
1.3 Методи виявлення та нейтралізації ворожих дронів	20
1.4 Аналіз сучасних засобів захисту від FPV-дронів	24
1.5 Проблеми існуючих засобів захисту від БПЛА.....	27
2 ПРОЄКТУВАННЯ СТРУКТУРИ ТА ПРИНЦИПУ ДІЇ МОДУЛЬНОЇ СИСТЕМИ ЗАХИСТУ ВІД FPV-ДРОНІВ	31
2.1 Структура та принцип дії запропонованої модульної системи	31
2.2 Функціональна схема модуля системи захисту	35
3 ОПИС АПАРАТНИХ ТА ПРОГРАМНИХ ЗАСОБІВ.....	37
3.1 Платформа Arduino.....	37
3.2 Дешифратор.....	41
3.3 Шинні формувачі	43
3.4 Оптопара для генерації та прийому світлового променя	45
3.5 Програмні засоби	48
4 РОЗРОБКА АЛГОРИТМУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МОДУЛЯ СИСТЕМИ ЗАХИСТУ	51
4.1 Алгоритм роботи модуля системи захисту	51
4.2 Програмна реалізація роботи модуля системи захисту	53
4.3 Перевірка роботи програми	55
ВИСНОВКИ.....	60
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	62
ДОДАТОК А КОД ПРОГРАМИ.....	66
ДОДАТОК Б СЛАЙДИ ПРЕЗЕНТАЦІЇ.....	69
ДОДАТОК В ПУБЛІКАЦІЯ ЗА ТЕМАТИКОЮ РОБОТИ	79

ПЕРЕЛІК СКОРОЧЕНЬ

БПЛА – безпілотний літальний апарат;

NATO (NATO, North Atlantic Treaty Organisation) – Організація Північноатлантичного договору;

ППО – протиповітряна оборона;

РЕБ – радіоелектронна боротьба;

РЕР – радіоелектронна розвідка;

DIR (Direction) – пін в Arduino для керування напрямком;

IDE (Integrated Development Environment) – інтегроване середовище розробки Arduino або програмне забезпечення Arduino;

HALE (High-Altitude Long-Endurance) – БПЛА висотного тривалого польоту,

MALE (Médium-Altitude Long-Endurance) – БПЛА середньовисотного тривалого польоту,

FPV-дрон (First Person View Drone) – дрон, керування яким здійснюється за допомогою відеокамери в реальному часі,

UAV (Unmanned Aerial Vehicle) – безпілотний літальний апарат, БПЛА,

USB (Universal Serial Bus) - універсальна послідовна шина;

UVSI (Association for Unmanned Vehicle Systems International) – Міжнародна асоціація з безпілотних літальних систем;

VTOL (Vertical Take-Off and Landing) – технологія вертикального зліту та посадки.

ВСТУП

Збройні конфлікти останніх років чітко демонструють, що кількість інцидентів із навмисним руйнівним використанням безпілотних літальних апаратів (БПЛА) або дронів суттєво зростає. Особливо актуальною є ця проблема в Україні після початку повномасштабного вторгнення рф. Масове застосування агресором бойових дронів призводять до постійних уражень та потенційних загроз військовим та мирним людям, житловому фонду, об'єктам критичної інфраструктури країни тощо. Ці тенденції стимулюють динамічний розвиток систем, які мають використовуватися для захисту не тільки військових частин і критично важливих об'єктів країни, але і мирних міст.

Безпілотні літальні апарати становлять велику загрозу для будівель, споруд, транспортних шляхів тощо. Всі перелічені об'єкти потребують надійного захисту від дронів. Оскільки БПЛА здатні діяти як окремі літальні апарати, кількість способів їх використання для ворожої військової діяльності практично необмежена. Тому при виборі системи захисту або розробці нових засобів протидії необхідно враховувати велику кількість параметрів.

Сьогодні існують та активно використовуються різноманітні методи та засоби протидії ворожим БПЛА [1, 2]. Існуючі методи захисту поділяють на пасивні та активні. До пасивних методів відносяться інженерні захисні споруди, захисні каркаси, металеві сітки, маскувальні засоби, захисні загородження, димова завіса а також використання радіогоризонту. До активних методів відносяться: засоби радіоелектронної боротьби (РЕБ), мобільні комплекси РЕБ для захисту рухомих об'єктів, різні системи виявлення та збиття БПЛА тощо [1, 2]. Аналіз засобів безпеки, що застосовуються, свідчить про існування деяких недоліків в певних засобах захисту. Також не існує універсального методу, який би гарантував абсолютний захист. При цьому систематичне застосування ворогом різних видів БПЛА значною мірою мінімізує безпеку на як на

передовій, так і у тилу. І це змушує шукати інноваційні методи та розробляти нові технічні рішення для протидії існуючим загрозам від БПЛА.

Дана кваліфікаційна робота присвячена дослідженню вже існуючих засобів протидії ворожим дронам та розробка модульної системи захисту від FPV-дронів. Аналіз інформаційних джерел за темою роботи [1 – 14] підтвердив важливість та актуальність цієї теми, саме тому дана кваліфікаційна робота є актуальною.

1 АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ВІД ВОРОЖИХ БПЛА

1.1 Актуальність проблеми захисту від БПЛА в Україні

Частково з 2014 року і повномасштабно з 2022 року на території України триває вторгнення російської федерації, представники якої широко використовують проти України майже всі існуючі види засобів ураження, в тому числі й ті, використання яких заборонено на міжнародному рівні [3].

З 24 лютого 2022 року країна-агресор масово застосовує артилерійські системи, авіаційні бомби, крилаті ракети різних типів базування (повітряного, наземного, морського), реактивні системи залпового вогню, бойові безпілотні літальні апарати (БПЛА) тощо. Найбільш болючим є факт того, що представники рф застосовують різні види зброї не тільки на полі бою, але також вони цілеспрямовано обстрілюють цивільне населення, об'єкти критичної та цивільної інфраструктури, житлові квартали міст та селищ тощо, чим грубо порушують норми міжнародних прав людини.

На початок травня 2026 року зафіксовано понад 256 тисяч воєнних злочинів [4], що порушують закони та звичаї війни.

Здійснюючи посягання на державний суверенітет, територіальну цілісність та недоторканність кордонів України, а також демонструючи зухвале нехтування нормами міжнародного гуманітарного права, зокрема законами та звичаями ведення війни, російська федерація веде регулярні й планомірні повітряні атаки. Для ударів по українській території ворог масовано застосовує БПЛА ударного типу. Ворожі атаки систематично спрямовані на ключові елементи життєзабезпечення (об'єкти критичної інфраструктури), квартали щільно заселених міст та інші цивільні об'єкти по всій державі. Головною метою цих дій є навмисне створення гуманітарної катастрофи та умов, за яких подальше проживання й існування цивільного населення стає неможливим. Для реалізації цієї злочинної стратегії країна-агресор залучає широкий спектр

– спеціалізовані БПЛА військового призначення, які були спроектовані та виготовлені безпосередньо для вогневого ураження, ліквідації живої сили та руйнування об'єктів;

Статистику застосування ворожих дронів проти України від початку масованих атак повномасштабного вторгнення до кінця січня 2026 року наведено на рис. 1.1 [5].



Згідно з даними від джерела [5] кількість ракетних атак трималася всі 4 роки приблизно на одному рівні, але з початку 2026 року відбувається нарощування кількості масованих ракетних атак, крім того значну частку ракет зараз становлять балістичні ракети, які є найбільш небезпечними. Що стосується БПЛА, то ця статистика більш негативна, кількість ворожих БПЛА з кожним роком суттєво зростає, що показано на рис. 1.1 та 1.2 [6].

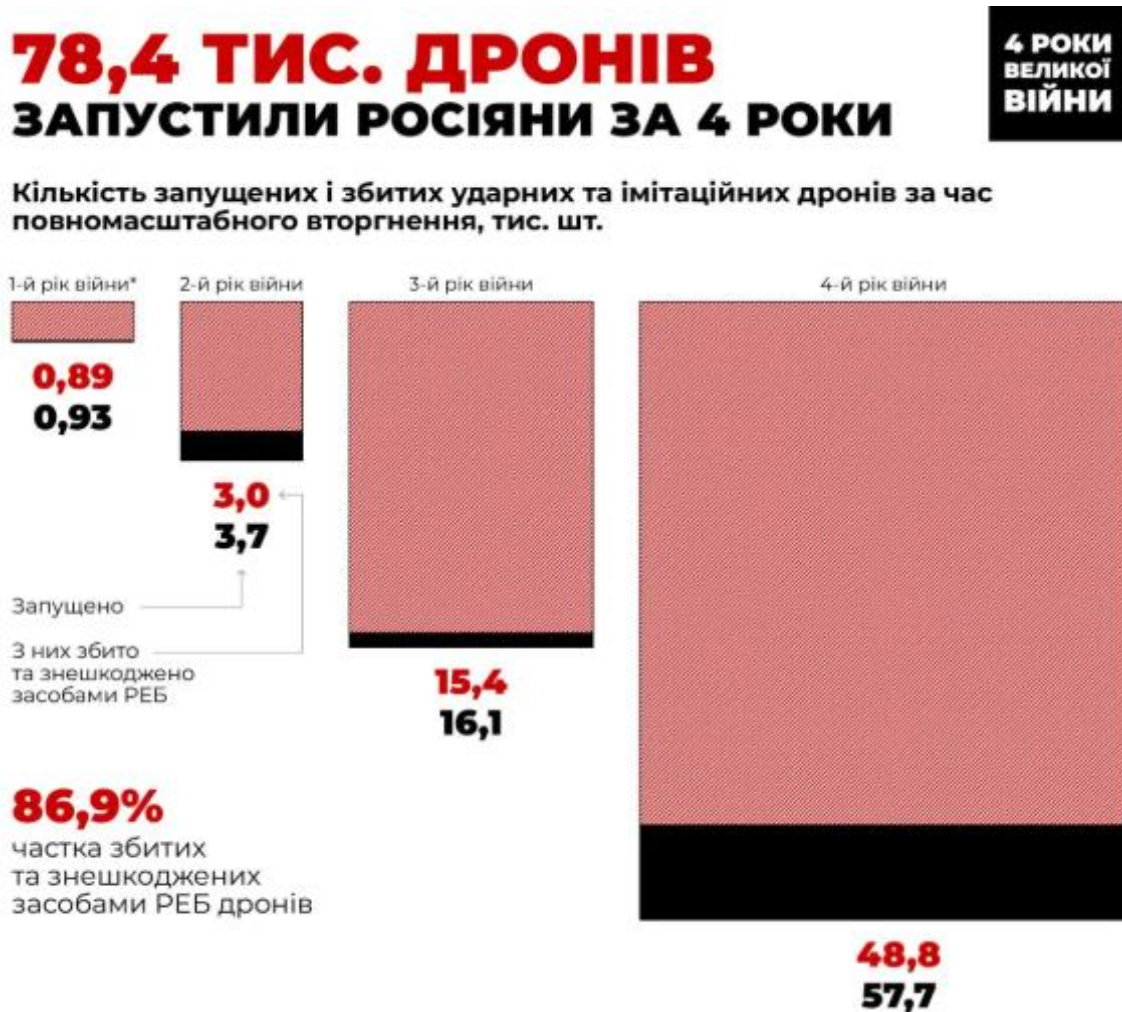


Рисунок 1.2 – Статистика запущених по Україні дронів за 4 роки війни [6]

Дана інфографіка демонструє тільки перші чотири роки війни, а в 2026 році кількість БПЛА продовжує зростати ще інтенсивніше. Саме тому проблема захисту від БПЛА в Україні є надзвичайно актуальною, вона потребує глибокого аналізу та впровадження надійних та новітніх засобів захисту.

1.2 Огляд БПЛА військового типу

Безпілотний літальний апарат (БПЛА) це повітряне судно без пілота, яким можна керувати дистанційно або яке може працювати автономно за допомогою вбудованого програмного забезпечення та бортових датчиків.

Військові БПЛА найчастіше використовуються для перенесення вибухового пристрою. Вибух цього пристрою впливає на об'єкт атаки через різку зміну тиску, випромінювання інфрачервоного випромінювання, тобто тепла, сейсмічної хвилі, якщо вибух відбувається близько до землі, та акустичної хвилі, тобто шуму. БПЛА є універсальною зброєю, яка може атакувати ціль з різної висоти, з різною швидкістю, за різними траєкторіями польоту та з різним бортовим обладнанням [7].

Також БПЛА використовуються для спостереження за важливими для безпеки об'єктами. Сучасні дрони зазвичай оснащені камерами. Ці камери дозволяють досягти спостереження на великій відстані. Вони оснащені системою автофокусування та оптикою найвищої якості, що дозволяє записувати зображення високої якості. Камери, що працюють у діапазоні видимого світла, можуть бути доповнені інфрачервоними датчиками. Така камера дозволяє записувати зображення в умовах дефіциту видимого світла, а також ідентифікувати компоненти системи. Камери дозволяють спостерігати за людьми та отримувати дані про технології, що використовуються на об'єкті, що спостерігається, топографію об'єкта, що спостерігається, тощо. Також можливе використання дронів для прослуховування радіозв'язку персоналу, включаючи інтернет-зв'язок [7].

БПЛА умовно поділяються на 2 типи: військові та цивільні. БПЛА військового типу можуть виконувати різні військові задачі, але в цілому вони мають ряд переваг над пілотованою авіатехнікою [3]. Переваги військових БПЛА наведено на рис. 1.3.



Рисунок 1.3 – Переваги військових БПЛА

Дуже велике різноманіття військових БПЛА систематизують за різними видами класифікацій, які відіграють велику роль при виборі БПЛА для використання у конкретних військових цілях, або при створенні засобів захисту від ворожих БПЛА. Згідно довіднику Служби безпеки України [3] БПЛА розрізняють за призначенням, масштабами завдань, кількістю застосувань, типом двигунів, висотою та швидкістю польоту та багатьма іншими характеристиками. Деякі з класифікацій наведено на рис.1.4.

UVSI (Міжнародна асоціація з безпілотних літальних систем) визначає БПЛА чотирьох груп [8, 9]: малі, тактичні, стратегічні та спецпризначення (табл.1.1).

Використовується також система класифікації НАТО. Для забезпечення оперативної сумісності між силами союзників, НАТО класифікує типи військових БПЛА на три основні класи, безпосередньо узгоджуючи оперативні можливості з ешелонами військового командування [9].



Рисунок 1.4 – Класифікація військових БПЛА [3]

Системи I класу (вагою менше 150 кг) розгортаються на рівні тактичного підрозділу. Системи цього класу поділяються на мікро, міні та малі дрони. Вони пропонують локалізовану розвідку в умовах швидкоплинних, динамічних бойових умов.

Таблиця 1.1 – Класифікація БПЛА згідно UVSI [7]

Група	Тип	Льотна маса, кг	Дальність польоту, км	Висота польоту, км	Тривалість польоту, г
Малі БПЛА	Нано БПЛА	< 0,025	< 1	100	< 0,5
	Мікро БПЛА	< 5	< 10	250	1
	Міні БПЛА	20 - 150	< 30	150 - 300	< 2
Тактичні	Легкі БПЛА для контролю переднього краю оборони	25 - 150	10 - 30	3000	2 - 4
	Легкі БПЛА з малою дальністю польоту	50 - 250	30 - 70	3000	3 - 6
	Середні БПЛА	150 - 500	70 - 200	5000	6 - 10
	Середні БПЛА за великою тривалістю польоту	500 - 1500	> 500	8000	10 - 18
	Мало висотні БПЛА для проникнення вглиб оборони супротивника	250 - 2500	> 250	50 - 9000	0,5 - 1
	Мало висотні БПЛА з високою тривалістю польоту	15 - 25	> 500	3000	> 24
	Середньовисотні БПЛА з великою дальністю польоту	1000 - 500	> 500	5000 - 8000	24 - 48
	Висотні БПЛА з великою дальністю польоту	2500 - 5000	> 2000	20000	24 - 48
Стратегічні	Бойові БПЛА (Ударні)	> 1000	1500	12000	2
	БПЛА оснащені бойовою частиною летальної дії	150 - 1000	300	4000	3 - 4
	БПЛА – хибні цілі	150 - 500	0 - 500	50 - 5000	< 4
Спец-призначення	Стратосферні БПЛА	> 2500	> 2000	> 20000	> 48
	Екзостратосферні БПЛА	> 2500	> 2000	> 30500	> 48

II клас (вагою 150 кг – 600 кг) працює на рівні бригади. БПЛА II класу несуть складні датчики цілевказання, радіолокаційні системи та канали передачі даних за межами прямої видимості для підтримки операцій середньої дальності.

Системи III класу (вагою понад 600 кг) є оперативними та стратегічними платформами. Вони виконують тривалі операції розвідки та реагування на події, складну радіоелектронну боротьбу та високоточні удари на відстані тисяч кілометрів [9].

Таблиця 1.2 – Класифікація БПЛА згідно НАТО [8]

Клас	Категорія	Рівень воєнних дій	Висота застосування	Радіус дії	Приклад платформи
Клас I	Мікро	Підрозділ	До 60 м	До 5 км	Black Widow
	Міні	Підрозділ	До 900 м	До 25 км	Skylark
	Малі	Формування	До 1500 м	До 50 км	Scan Eagle, PD-2
Клас II	Тактичні	Тактичний	До 5500 м	До 200 км	Hermes 450
Клас III	MALE	Оперативний	До 14000 м	Необмежений	Bayraktar, TB-2
	HALE	Стратегічний	До 20000 м	Необмежений	Global Hawk
	Ударні	Стратегічний	До 20000 м	Необмежений	Reaper

Заслуговує уваги класифікація за конструкцією (рис. 1.5), згідно якої БПЛА поділяються на 5 типів:

- літаки,
- мультироторні БПЛА,
- тейлсіттери (що об'єднують в собі наявність крил та мультироторів),
- VTOL (БПЛА з можливістю вертикального зліту/посадки),
- дирижаблі та аеростати (надлегкі апарати).

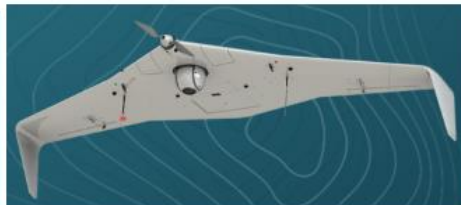
Літаки**Крила****Тейлсіттери****VTOL****Аеростати****Мультиротори**

Рисунок 1.5 – Класифікація військових БПЛА за конструкцією [8]

БПЛА з фіксованими крилами (літаки) та мультироторні БПЛА служать різним цілям, з ключовими відмінностями у витривалості та варіантах використання. БПЛА з фіксованими крилами переважають у тривалому польоті та охопленні великої площі, тоді як мультироторні БПЛА краще підходять для точних завдань та маневреності у вузьких просторах [10].

До мультироторних БПЛА відносяться також FPV-дрони. FPV-дрони – це окремий вид БПЛА, що мають дистанційне керування, яке забезпечується за допомогою технології First Person View (FPV). FPV-дрони мають в своїй конструкції камеру, що дозволяє передавати відео оператору в режимі реального часу і таким чином надають оператору можливість управління процесами польоту дрону [11, 12].

FPV-дрони мають кілька ключових переваг:

- максимальна точність наведення (пілот бачить пряму трансляцію відеопотоку з мінімальною затримкою, що гарантує точну корекцію траєкторії польоту та безпомилкове ураження статичних і рухомих цілей під час ударних місій);

- високі аеродинамічні характеристики (вони забезпечують високу кутову швидкість і маневреність, здатні ефективно огинати перешкоди та виконувати завдання у зонах зі складним рельєфом, міською забудовою, густою рослинністю тощо),

- компактність і швидкість (завдяки малим габаритам, низькій злітній вазі та високій швидкості польоту апарат має низьку візуальну та акустичну помітність, що ускладнює його виявлення та перехоплення засобами ППО чи іншою зброєю),

- невисока ціна (собівартість компонентів FPV-дрона є низькою в порівнянні з іншими розвідувальними або оперативно-тактичними БПЛА, що дозволяє масово застосовувати їх як дрони-камікадзе без суттєвого фінансового навантаження на бюджет підрозділу у разі втрати борту).

Порівняння FPV-дронів зі звичайними БПЛА наведено в табл. 1.3.

Таблиця 1.3 – Порівняння FPV-дронів зі звичайними БПЛА

Характеристики	FPV-дрони	Звичайні БПЛА
Тип керування	Через окуляри чи шолом від першої особи (оператор)	Автоматично або через екран від третьої особи
Маневреність	Висока	Обмежена
Керування	Змішане, ручне, потребує навичок та досвіду	У більшості випадків – автоматизоване
Призначення	Розвідка, ударні місії	Польоти на великі відстані, транспортування вантажу
Камера	Невелика з відмінними технічними параметрами	Камера зі стабілізацією
Вартість	Нижча	Вища
Придатність до ремонту	Легко ремонтується, піддається модифікації	Дорожчий ремонт

Завдяки своїм перевагам FPV-дрони широко використовуються під час сучасних воєнних конфліктів для розвідувальних операцій (спостереження за супротивником, розміщенням техніки, коригування вогню тощо) та для бойових атак (перенесення вибухового заряду та спрямування його точно на ціль). Саме тому ворожі FPV-дрони потребують уваги та спеціальних засобів протидії.

Таким чином при виборі або розробці систем захисту від ворожих БПЛА необхідно враховувати особливості конкретних видів БПЛА, протидію яким при цьому має бути забезпечено.

1.3 Методи виявлення та нейтралізації ворожих дронів

Сучасні системи виявлення дронів, які є елементами систем боротьби з дронами, що захищають об'єкти, працюють з використанням різних функцій БПЛА. Характеристики БПЛА, які можна виявити, включають:

- тепло, що випромінюється літальним апаратом,
- шум, що випромінюється пропелерами та двигунами,
- шум, що виникає внаслідок обтікання БПЛА повітряними струменями,
- форму літального апарата,
- електромагнітне випромінювання різних частот, що випромінюється системами зв'язку, що працюють під час польоту [7].

Дрони також можуть бути виявлені за допомогою радарів.

Методи виявлення дронів наведено на рис.1.6.



Рисунок 1.6 – Методи виявлення дронів

Методи нейтралізації дронів наведено на рис. 1.7. Одним із методів нейтралізації дрона є його знищення лазерним променем, що призведе до падіння дрона після ураження. Ці системи ефективні за гарних погодніх умов.

Можна зловити дрон у сітку [7, 13]. Таку сітку запускають з мережної гармати, якою керує на землі персонал охорони об'єкта. Цей метод ефективний, коли постріл здійснюється з близької відстані, яка може становити до 30 метрів.

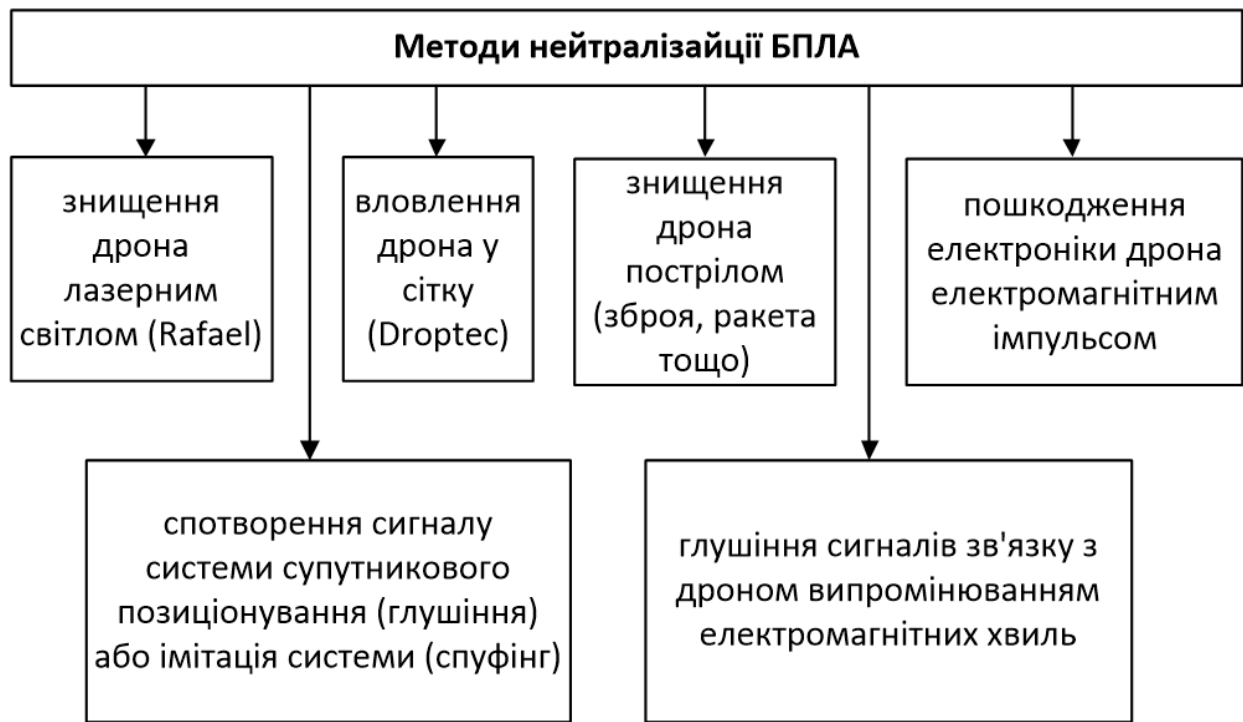


Рисунок 1.7 – Методи нейтралізації дронів

Можна нейтралізувати дрон пошкодивши його електроніку високоенергетичним електромагнітним імпульсом, що може зруйнувати електронні компоненти дрона, такі як його комп'ютер або електронні системи контролю швидкості. Дальність дії цього типу імпульсу може становити кілька кілометрів.

Пристрої глушіння сигналів зв'язку між БПЛА та наземною станцією випромінюють електромагнітне випромінювання на різних частотах, включаючи частоти, що використовуються БПЛА. Зв'язок між БПЛА та наземною станцією порушується випромінюванням електромагнітної хвилі з плоским спектром та рівномірною для всіх випромінюваних частот інтенсивністю шуму [7].

Часто використовуваним методом нейтралізації БПЛА є спотворення сигналу системи супутникового позиціонування (глушіння) або імітація системи (спуфінг). Пристрій, що створює перешкоди, випромінює сигнал на частотах, на яких працює система позиціонування.

Враховуючи різноманіття засобів захисту від дронів за можливості варто використовувати їх комплексно. Існують системи боротьби з дронами, вони складаються з датчиків та ефекторів, які працюють разом для виявлення та нейтралізації дронів [13]. Такі системи боротьби з дронами можуть бути стаціонарними та мобільними. Крім того, автори роботи [14] пропонують комплексну модель системи від дронів у цивільному середовищі, що складається з кількох підсистем (рис. 1.8).



Рисунок 1.8 – Комплексна модель захисту від дронів

Така система використовує різноманітні можливості для виявлення, ідентифікації та нейтралізації дронів, що значно підвищує ступінь захисту від дронів.

В будь-якому разі принцип роботи, архітектура та процедури використання пристроїв і систем боротьби з дронами тісно пов'язані з функціями, експлуатаційним використанням та технічними параметрами сучасних дронів. Для ефективної протидії шкідливому впливу дронів система боротьби з дронами повинна ідентифікувати ворожі дрони, класифікувати їх та

вживати проти них заходи нейтралізації. Слід враховувати важливу роль однозначної ідентифікації та класифікації об'єктів, що спостерігаються системою боротьби з БПЛА [14].

1.4 Аналіз сучасних засобів захисту від FPV-дронів

Існують різні способи протидії ворожим FPV-дронам (рис. 1.9), які широко застосовуються в Україні в час війни [1]. Обов'язковою умовою належного захисту від ворожих FPV-дронів є їх своєчасне виявлення, яке може бути реалізоване за допомогою: радіочастотних аналізаторів, акустичних датчиків (мікрофонів), оптичних датчиків (камер) та радарів.



Рисунок 1.9 – Способи протидії ворожим FPV-дронам

Порівняльний аналіз способів захисту від ворожих FPV-дронів наведено в табл. 1.4.

Таблиця 1.4 - Порівняння способів захисту від FPV-дронів

№	Спосіб захисту	Опис	Переваги	Недоліки
1	Фізичний захист (різні сітки , рамки, бар'єри тощо)	Сітка заплутує дрон, що призводить до втрати керування та падіння дрона	Позбавляє дрон керування; має можливість швидкої зміни або видалення конструкції	Захищає тільки окремий об'єкт, одноразовість
2	Збиття зі стрілецької зброї	Збиття дронів вогнепальною зброєю (автомати, кулемети, гладкоствольні рушниці тощо)	Висока ефективність для захисту стаціонарних цілей; можливість використання картечі для збільшення ймовірності ураження цілі	Складність прицілювання та своєчасного виявлення через високу швидкість та маневреність дрона
3	Використання БПЛА з сітчастими пристроями	Сітчасті гармати або підвішені сітки для зупинки дрона шляхом блокування лопатей ротора	Ефективна зупинка дрона; низький ризик рикошету та падіння уламків; збереження дрону для доказів; екологічність	Обмежена дальність і точність; проблема з нейтралізацією дронів з високою швидкістю
4	Захист димовою завісою	Встановлення димової завіси, щоб запобігти влучанню дрона	Блокування візуального контакту; дезорієнтація оператора та дрона; широкий спектр захисту	Залежність від погодних умов; безсильність проти тепловізорів; ризик для своїх підрозділів

Продовження табл 1.4

№	Спосіб захисту	Опис	Переваги	Недоліки
5	Використання дронів-перехоплювачів	Працюють як мобільне ППО, швидко виявляють, супроводжують, наближаються до ворожих БПЛА та оперативно їх знищують	Дешевше класичних систем ППО; зручний при раптових загрозах; висока точність; дозволяє знизити навантаження на ППО	Має залежність від розвідки (потребує якісних радарів, операторів з високим рівнем навичок пілотування тощо); має вразливість до погодніх умов
6	Використання сіток для маскування	Приховування особового складу, техніки та фортифікацій від повітряної та наземної розвідки	Маскування (візуальне злиття з навколишнім середовищем) і дезорієнтація дронів; затримування дронів; низька вартість; швидкість розгортання	Має обмеження мобільності; недовговічність; не знешкоджує дрон, а тільки запобігає виявленню позицій; тимчасовий захист
7	Радіогоризонт	Використання перешкод для блокування сигналів дронів	Зменшує ефективність ворожих атак і розвідки	Легко обійти за допомогою підвищення антен або ретрансляційних радарів

Закінчення табл 1.4

№	Спосіб захисту	Опис	Переваги	Недоліки
8	Розвідувальні заходи	Виявлення ліній ВОЛЗ та аналіз супутникових даних для підготовки атак	Допомагає у плануванні інших видів контрзаходів	Потребує часу та спеціалізованого обладнання
9	Радіoeлектронна боротьба	Стаціонарні та мобільні системи РЕБ, що створюють потужні перешкоди і блокують зв'язок дрона з оператором	Дешевше ніж ППО; можливість захисту транспорту у русі; багатофункціональність	Має обмеження, пов'язані з потужністю; потребує джерела живлення; створює перешкоди для своїх підрозділів БПЛА

Жоден з методів протидії ворожим FPV-дронам не забезпечує повного захисту від поразки, крім того їхня ефективність може змінюватися залежно від умов та ситуації.

1.5 Проблеми існуючих засобів захисту від БПЛА

Стрімкий розвиток та масштабування використання ворогом FPV-дронів призводить до збільшення загроз від цього типу зброї. Зараз спостерігається значне збільшення виробництва та застосування ворогом БПЛА типу FPV. Тому питання захисту особового складу, техніки, зброї, цивільного населення та споруд від дронів-камікадзе є надзвичайно актуальним. На жаль, існуючі способи захисту не гарантують стовідсоткової ефективності. Різні способи захисту є ефективними в залежності від умов, але вимагають обов'язкового

проведення випробувань. Крім того, полігонні випробування можуть суттєво відрізнятися від реальних бойових умов [1].

Різні системи виявлення дронів противника мають свої конкретні труднощі та проблеми.

Виявлення БПЛА за шумом з допомогою мікрофона є відносно складним. Супротивним може використовувати різні методи зменшення шуму, крім того, звук дрона може бути приглушений шумом, що випромінюється навколишнім середовищем системи виявлення. Якщо об'єкт, що охороняється, знаходиться в населеному пункті, джерелом звуку може бути громадський транспорт, автомобілі, звуки від сусідніх промислових підприємств та шум літаків, що приземляються в місті.

Виявлення БПЛА за допомогою методів зору можливе виключно за гарних погодних умов, погані умови суттєво знижують ефективність камер. Система аналізу зображень повинна чітко визначати об'єкт спостереження, варто застосовувати технологію штучного інтелекту та ідентифікувати дрон на основі вивчених алгоритмів. Недоліком цієї системи є складність навчання системи правильно розпізнавати об'єкт. Таке навчання – це тривалий і складний процес. Крім того, зловмисник може будувати дрони незвичайної форми. У разі атаки таким дроном система розпізнавання зображень буде обдурена [7].

Виявлення БПЛА шляхом виявлення зв'язку між дроном та наземною станцією зараз є ненадійним та неефективним. Однією з причин низької ефективності виявлення є можливість виконання безпілотної місії без необхідності зв'язку з наземною станцією під час польоту. Під час планування місії, ворог може використовувати програмне забезпечення, в якому він позначає точки, до яких має летіти БПЛА на карті, а в більш просунутих системах він може вказати, що БПЛА має виконувати в заданій точці, наприклад, транспортний засіб може скинути вантаж і зробити фотографію.

Множина частот, на яких відбувається зв'язок, а також можливість використання нестандартних частот, є причиною, чому виявлення є складним. Пристрій виявлення повинен сканувати весь частотний спектр

електромагнітного випромінювання і вирішувати, які частоти використовуються для зв'язку дрона та наземної станції, а які для інших цілей.

Для роботи з обладнанням радіоелектронної боротьби та обладнанням для виявлення дронів потрібен достатній рівень підготовки персоналу [1].

Ефективність виявлення дрона з використанням радіолокаційних систем зростає зі зменшенням відстані між дроном та антеною радара. При цьому збільшується співвідношення сигнал/шум радара. Ефективність радіолокації сильно залежить від розташування об'єкта. Низький політ дрона над нерівною, вибоїстою місцевістю є причиною, чому радар його не виявить. Дрон також не буде виявлено, якщо територія навколо об'єкта, що охороняється, заросла кущами або деревами [7].

Існуючі методи нейтралізації дронів також не є повністю ефективними.

Знищення дрона лазерним світлом (Rafael) є малоефективним при поганих погодних умовах. Крім того, дрон, нейтралізований цим методом, падає на землю неконтрольовано, що може мати серйозні негативні наслідки.

Пошкодження електроніки дрона електромагнітним імпульсом може впливати на інші електронні пристрої, включаючи ті, що використовуються для керування технологічними процесами на об'єкті, що захищається.

Пристрої глушіння сигналів зв'язку між літаком та наземною станцією є неефективними, якщо пілот запрограмує дрон перед зльотом, що дозволяє йому виконувати місію в повністю автономному режимі [7].

Низька ефективність існуючих систем нейтралізації дронів також змушує шукати нові рішення.

Більшість систем боротьби з дронами використовують компоненти військового класу для досягнення остаточного знищення шкідливих дронів. Однак, під час розміщення системи боротьби з дронами військового класу в цивільних районах виникають певні труднощі. Військові заходи боротьби з дронами зазвичай використовують системи глушіння для відключення каналу керування цільовим дроном. Глушіння генерує надзвичайно високу амплітуду радіочастотного сигналу в цільовому діапазоні частот, щоб запобігти зв'язку. У

військових сценаріях об'єкт контролюється військовими, і оператор попередньо отримує відповідний польовий посібник з експлуатації для умов глушіння, тому побічний ефект глушіння можна ігнорувати або контролювати. Однак для невійськових застосувань радіочастотне глушіння для нейтралізації високошвидкісних дронів ризикує тимчасовим блокуванням існуючих бездротових мережевих систем, таких як мережі мобільного доступу або бездротові сенсорні мережі [14]. Таким чином надійні рішення, такі як глушіння або зенітна зброя, забезпечують прийнятні результати для потреб зупинки дронів, але створюють велике навантаження на регулювання та фінансовий бюджет.

2 ПРОЄКТУВАННЯ СТРУКТУРИ ТА ПРИНЦИПУ ДІЇ МОДУЛЬНОЇ СИСТЕМИ ЗАХИСТУ ВІД FPV-ДРОНІВ

2.1 Структура та принцип дії запропонованої модульної системи

В даній роботі пропонується створення модульної системи захисту від FPV-дронів на основі контролю певного простору. Така система створюватиме контрольоване поле у вигляді світлової сітки, при порушенні якого система виявлятиме місце появи дрону та спрямовуватиме в це місце постріл для знищення дрону. Система захисту матиме модульну структуру, тому буде легко масштабуватися для збільшення площі захисту. За допомогою модулів можна створювати захисні куполи для різних об'єктів захисту (рис. 2.1 – 2.2). Така система дозволить посилити захист окремих позицій з мінімальними технічними та фінансовими витратами.

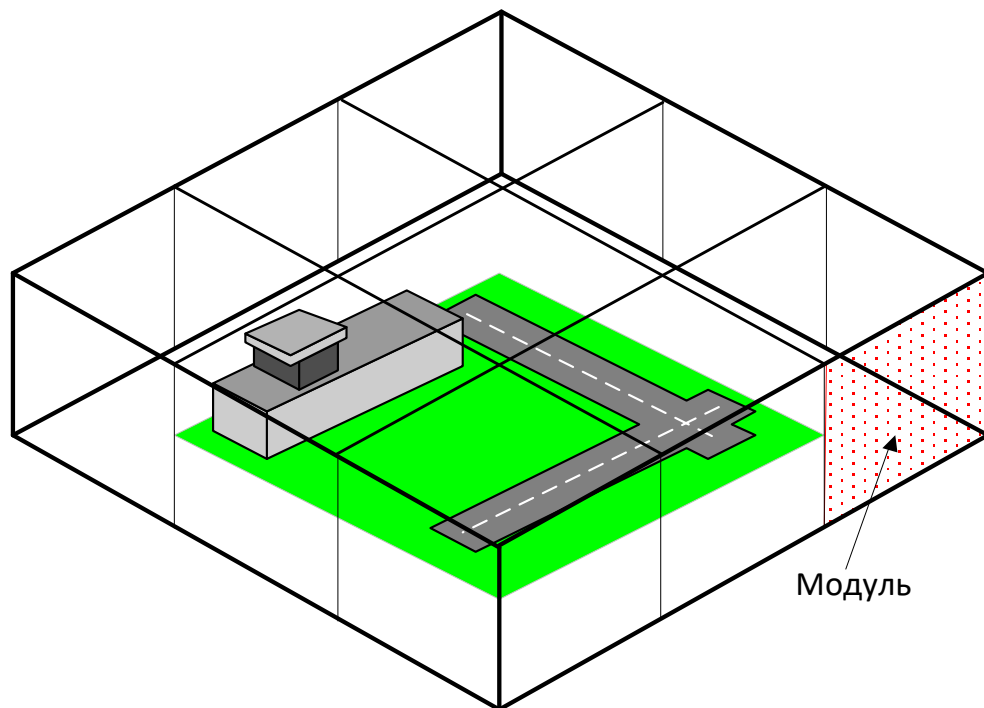


Рисунок 2.1 – Захисний купол для будівлі або певної території

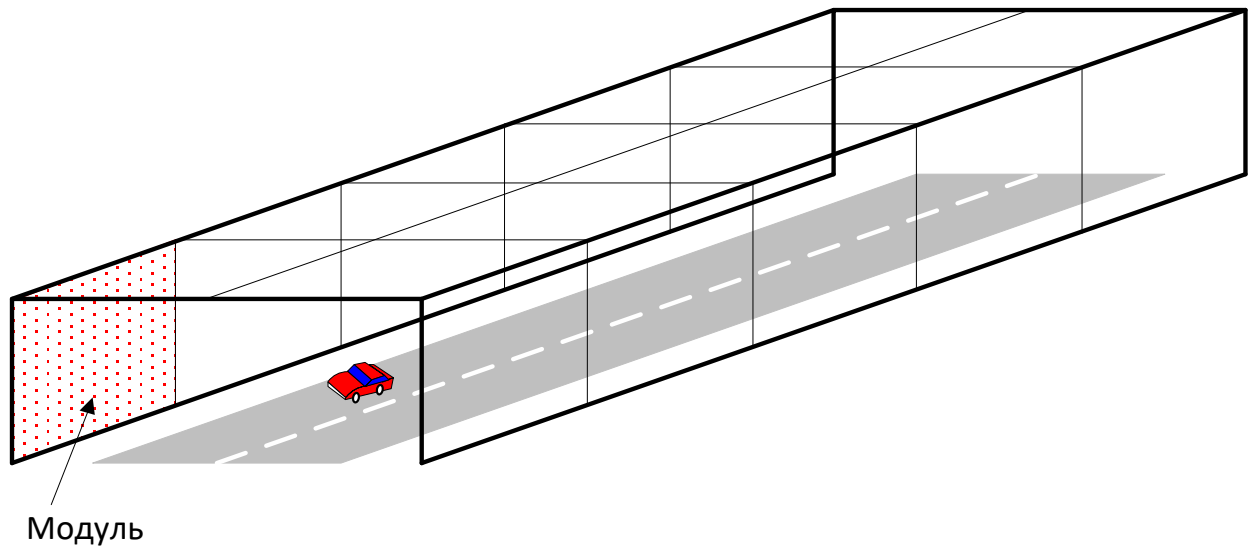


Рисунок 2.2 – Захисний купол для транспортного шляху

Кожен захисний купол містить чотири (або дві для транспортних шляхів) бокові та одну стельову поверхні, що складаються зі з'єднаних між собою модулів. Кожен модуль містить в собі певну кількість сегментів (в нашому випадку 5).

В залежності від того, яким чином буде організовано ліквідацію виявленої ворожої цілі, можна розробити два різні варіанти світлової сітки і відповідно два варіанти модуля.

1-й варіант: кожен сегмент модуля (рис. 2.3) має по 8 вертикальних випромінювачів світлових променів та відповідно по 8 фотоприймачів. Таким чином сітка складається з паралельних світлових променів, які знаходяться на такій відстані один від одного, яка не дозволить пролетіти дрону між ними не зачепивши жодного променя. При використанні такого модуля знищення цілі має відбуватися поруч з сіткою паралельно проміням з боку фотоприймача, який не отримав світловий промінь, оскільки поява дрону порушила в цьому місці світлову сітку.

2-й варіант: кожен сегмент модуля (рис. 2.4) має по 8 горизонтальних та 8 вертикальних випромінювачів світлових променів та відповідно стільки ж фотоприймачів. При використанні такого модуля можна виявляти точні координати появи дрону, оскільки перетин двох порушених променів

(вертикального і горизонтального) надасть точні координати дрона. В такому випадку для знищення ворожої цілі потрібна зброя, яка буде спрямовувати постріл в точному напрямку ворожого дрону.

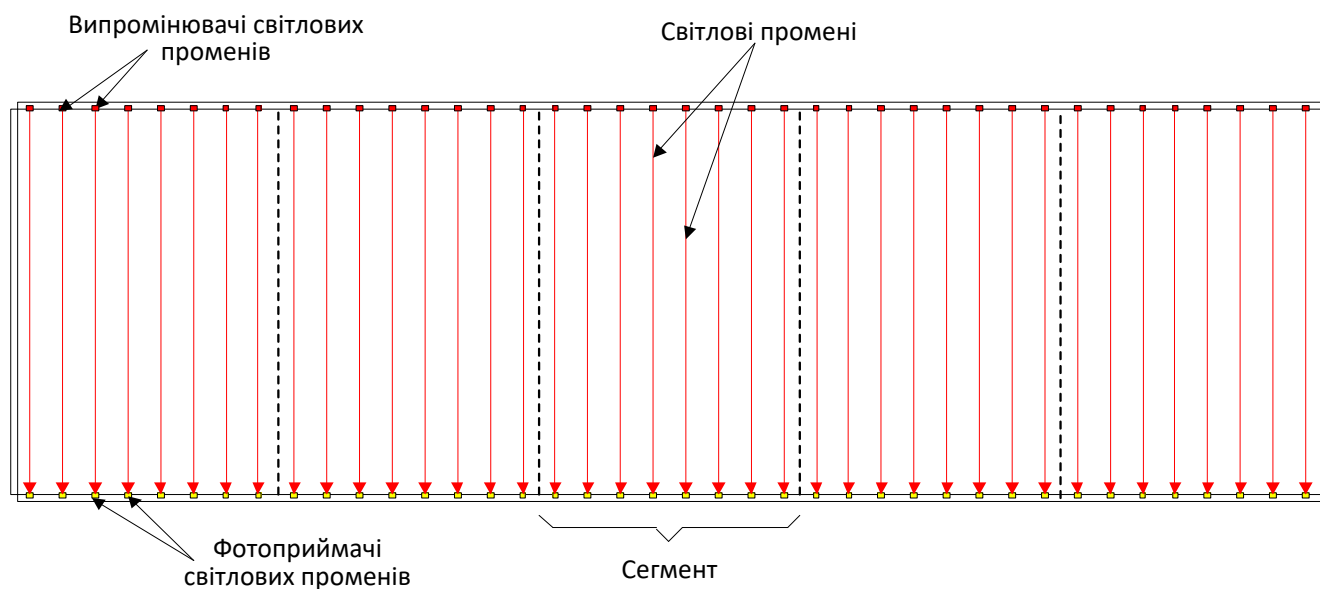


Рисунок 2.3 – 1-й варіант модуля виявлення ворожого дрону

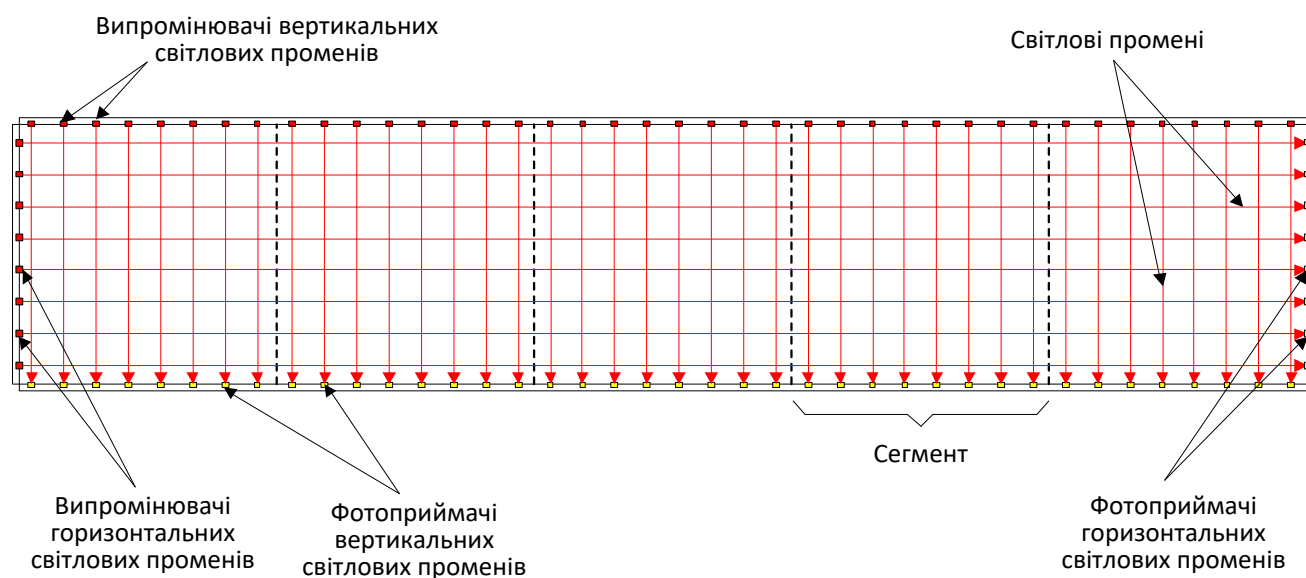


Рисунок 2.4 – 2-й варіант модуля виявлення ворожого дрону

Світлова сітка створюється за допомогою виключно вертикальних (1-й варіант модуля) або вертикальних та горизонтальних (2-й варіант модуля) вузькоспрямованих випромінювачів якісних світлових променів. За допомогою даної системи захисту можна виявити та протидіяти будь-яким дронам. Але оскільки FPV-дрони мають камери, то світлові промені мають бути невидимими для камер. Крім того, відстані між промінями мають бути дещо меншими за розміри дрона, щоб при перетині стельової або бокової поверхні захисного купола на дрон обов'язково потрапили світлові промені. Оскільки

Розміри модуля можуть бути різними, але в першу чергу вони залежать від дальності, яку долає промінь без розсіювання, без погіршення якості, з отриманням чіткої світлової точки на приймачі та стабільної роботи системи. За допомогою інфрачервоних лазерів (940 нм або 980 нм) можна реалізувати якісні промені довжиною 10 метрів. В даній роботі розробляється захист від розвідувальних та ударних FPV-дронів, які мають габарити 7 – 10 дюймів (тобто ширина/довжина таких дронів становить 30 – 40 см плюс розмір пропелерів), тому для виявлення таких дронів достатньо буде відстані між променями 25 см. Таким чином модуль може мати загальні розміри 10 на 10 метрів з вертикальними променями через кожні 25 см, кожен сегмент має по 8 променів, тому його ширина буде 2 метри.

Принцип роботи системи захисту складається з двох основних етапів:

- 1) виявлення дрону,
- 2) нейтралізація дрону.

Виявлення дрону відбувається наступним чином. Коли дрон перетинає бокову або стельову поверхню купола, то він перекриває собою деякі світлові промені і відповідні приймачі не отримують цих променів. Визначивши місце перетину відсутніх променів можна визначити місцезнаходження дрону.

Нейтралізація дрону відбувається за допомогою пострілу в тому напрямку, де було виявлено дрон. Розрахувавши швидкість дрону можна точно спрямувати постріл у ціль.

2.2 Функціональна схема модуля системи захисту

В даній роботі буде реалізовано 1-й варіант модуля виявлення ворожого втручання. Функціональна схема одного такого модуля наведена на рис. 2.5.

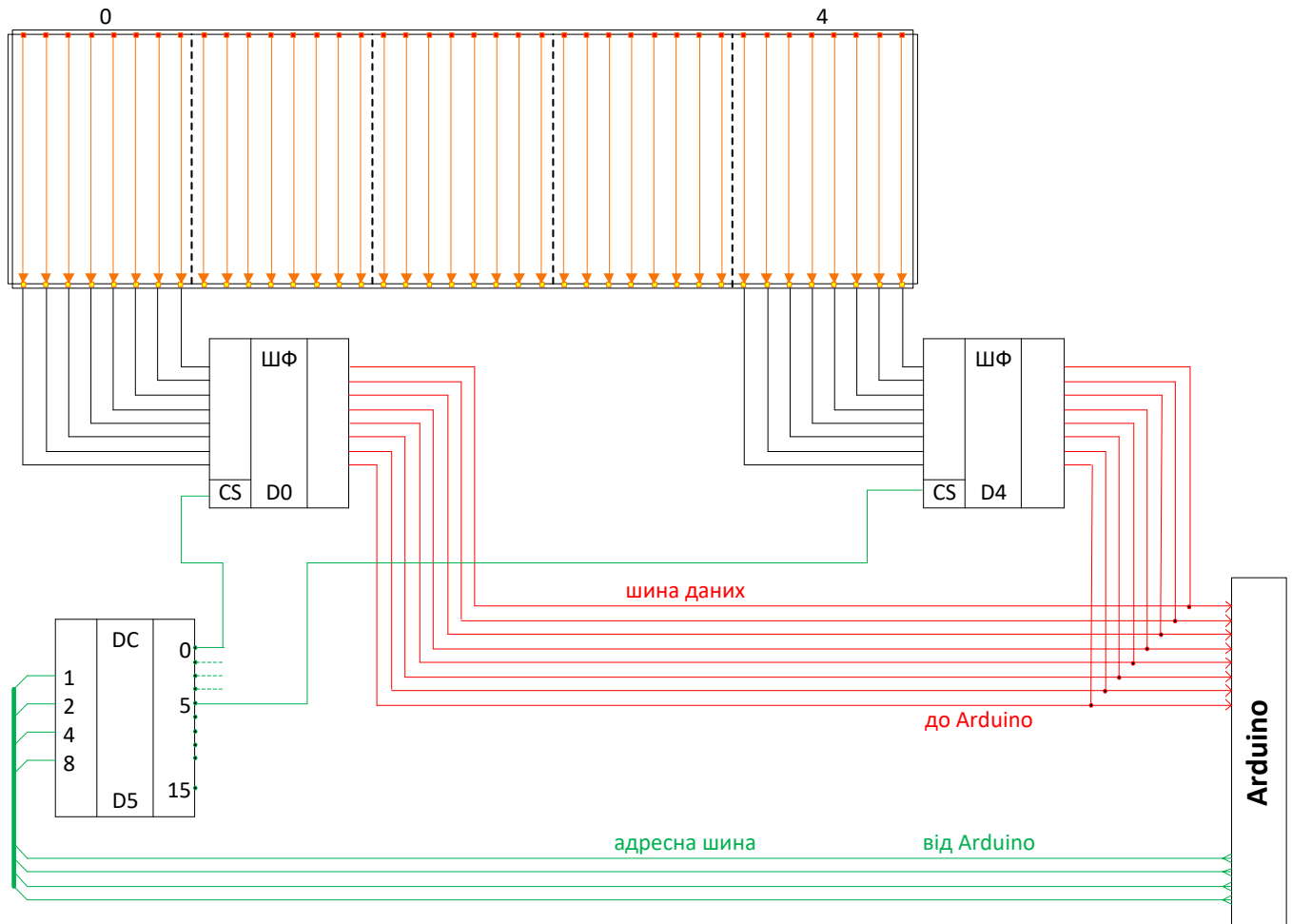


Рисунок 2.5 – Функціональна схема модуля виявлення дрона

Принцип дії модуля виявлення заключається в наступному. Цей модуль виявлення керує всією системою. В модулі є поле, що складається з 5 восьмирозрядних сегментів. Дешифратор по черзі буде опитувати (перевіряти стан) 5 шинних формувачів. Як тільки з'явиться ворожий об'єкт, він порушить світлову сітку, на відповідний фотоприймач не надійде промінь і на мікроконтролері висвітиться адреса порушення. Саме таким чином буде виявлено ворожий дрон, який необхідно знищити пострілом.

Порядок опитування сегментів визначає програма, вона буде виконувати це послідовно. Відповідно, для того щоб стан одного сегмента не заважав іншому (щоб вони не накладалися один на інший), необхідно їх розв'язати за допомогою шинних формувачів. У мікроконтролері генерується номер сегмента та визначається номер розряду. У випадку порушення одного з восьми розрядів будь-якого сегменту на виході мікроконтролера буде відображатися кодова комбінація адреси порушеного сегменту.

Для організації 2-го варіанту модуля виявлення, необхідно було б додати випромінювачі та приймачі горизонтальних світлових променів та один додатковий шинний формувач для отримання інформації від цих приймачів. Програмна реалізація такого модуля суттєво відрізнятиметься від програмної реалізації модуля 1-го варіанту.

Варто зазначити, що розміри модуля можуть бути суттєво змінені при необхідності. По перше, не завжди потрібна висота купола в 10 м (наприклад при захисті бліндажа), тоді можна висоту зменшити до потрібної. По друге, можна збільшити ширину модуля (якщо це 1-варіант і не використовуються горизонтальні промені, оскільки саме дальність якісного променя обмежує ширину модуля). В такому випадку можна збільшити кількість сегментів у модулі з 5 до 16 (1 дешифратор може опрацювати 16 сегментів). Але при цьому система може працювати повільніше, крім того виникає потреба в будівельному укріпленні конструкції.

В даній роботі програма буде написана для модуля з 5 сегментів, але при необхідності програму можна досить просто змінити і переорієнтувати на потрібну кількість сегментів.

3 ОПИС АПАРАТНИХ ТА ПРОГРАМНИХ ЗАСОБІВ

3.1 Платформа Arduino

Arduino – це електронна платформа з відкритим вихідним кодом, що базується на простому у використанні апаратному та програмному забезпеченні. Arduino є зручною платформою, що дозволяє дуже швидко розробляти електронні пристрої. Завдяки простому та доступному інтерфейсу користувача, Arduino використовувався в багатьох різних проєктах та застосуваннях. Програмне забезпечення Arduino просте у використанні для початківців, але достатньо гнучке для досвідчених користувачів. Воно працює на Windows, Mac та Linux. Початківці використовують його для створення недорогих наукових приладів або для початку роботи з програмуванням та робототехнікою. Професійні користувачі створюють інтерактивні прототипи, інсталяції, експерименти з новими інструментами та багато різноманітних проєктів.

Існує багато інших мікроконтролерів та платформ мікроконтролерів, доступних для фізичних обчислень. Parallax Basic Stamp, BX-24 від Netmedia, Phidgets, Handyboard від MIT та багато інших пропонують подібну функціональність. Усі ці інструменти поєднують складні деталі програмування мікроконтролерів у простий у використанні пакет [15]. Arduino також спрощує процес роботи з мікроконтролерами, але пропонує певні переваги в порівнянні з іншими системами (рис. 3.1).

Плата Arduino містить 8-бітний або 32-бітний мікроконтролер, а також кілька інших компонентів. Моделі, такі як Uno, також пропонують інтерфейс USB, аналогові вхідні контакти, а також низку цифрових вхідних/вихідних контактів [16].

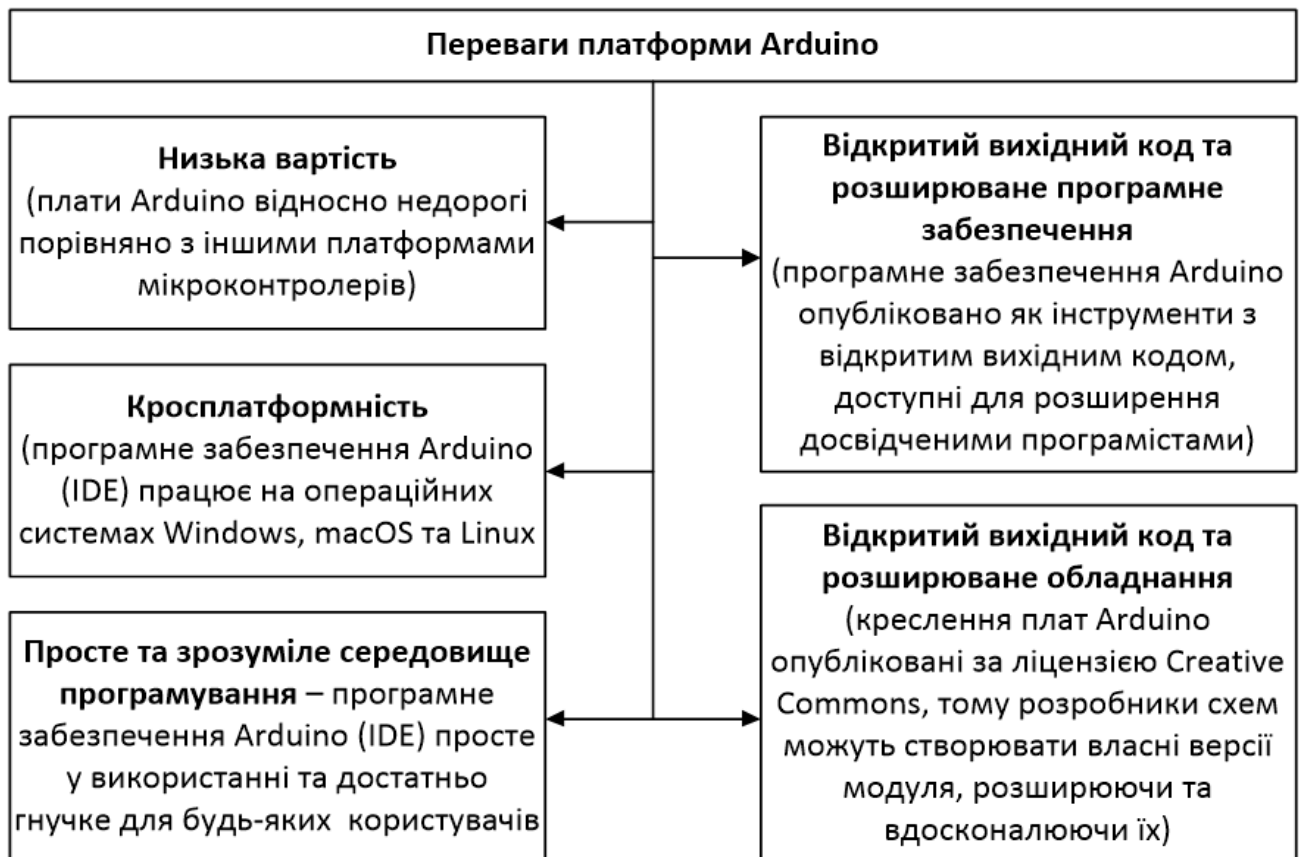


Рисунок 3.1 – Переваги платформи Arduino

Концепція розробки Arduino полягає у спрощенні побудови інтерактивних об'єктів або середовищ та їх доступності. З цією метою він був розроблений недорогим та простим у використанні, що дозволяє користувачам створювати пристрої та проекти, які взаємодіють з навколишнім середовищем за допомогою датчиків та виконавчих механізмів.

Мікроконтролер Arduino потрібно запрограмувати, і це вводить програмний елемент у вигляді інтегрованого середовища розробки (IDE), яке працює на персональних комп'ютерах. За його допомогою користувачі пишуть програми за допомогою мов програмування C або C++ [16].

Мікроконтролер Arduino постачається із завантажувачем, який значно спрощує завантаження програм у флеш-пам'ять плати. Конкуренти Arduino зазвичай потребують використання зовнішнього програматора. Відповідно до

принципів Arduino, це максимально спрощує програмування, дозволяючи виконувати його за допомогою персонального комп'ютера.

Роз'єми на платах Arduino є стандартними, і тому можна розширити базові можливості Arduino, включивши попередньо зібрані друковані плати. Завдяки конструкції блоків роз'ємів, їх можна складати один до одного, що дозволяє створювати великі та складні проекти [16].

Доступна велика кількість версій Arduino. Наприклад Uno, Duemilanove, Diecimila, Mega та інші. Усі вони розроблені для використання з певними типами проектів і тому мають різні характеристики. Версія Uno є найпопулярнішою та може використовуватися для найширшого кола проектів.

Arduino UNO (рис. 3.2) надає низку функцій, що роблять її гарною універсальною платою.

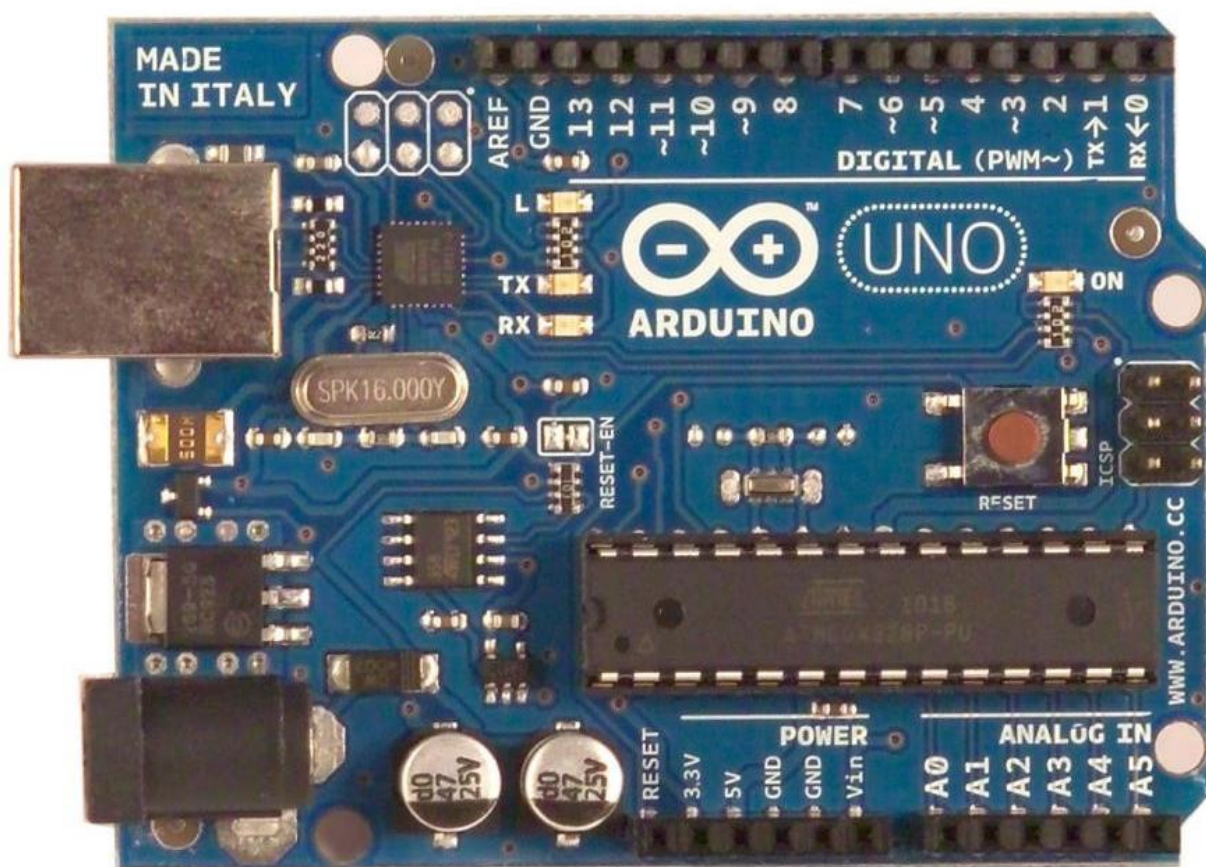


Рисунок 3.2 – Arduino UNO

Існує багато видів плат Arduino UNO. Однією з найновіших є Arduino UNO Q 4GB LPDDR4/32GB eMMC ABX00173 Qualcomm. Вона має найкращі технічні характеристики, але і коштує вона достатньо дорого (близько 4000 грн). Для нашого проєкту можна використати більш просту та дешеву плату Arduino UNO. Наприклад, Arduino UNO R3, характеристики якої наведено в табл. 3.1, коштує така плата в двадцять разів дешевше (180 грн [17]).

Таблиця 3.1 – Технічні характеристики плати Arduino UNO R3

Тип мікроконтролера	ATmega328P
Напруга живлення мікроконтролера	5 В
Рекомендоване напруга живлення плати	6 – 20 В
Цифрові входи-виходи	14 (з них 6 підтримують ШІМ)
Виходи ШІМ модуляції	6
Аналогові входи	6
Допустимий струм цифрових виходів	20 мА
Допустимий струм виходу 3,3 В	50 мА
Обсяг флеш пам'яті (FLASH)	32 кБ (з яких 0,5 кБ використовується завантажувачем)
Об'єм оперативної пам'яті (SRAM)	2 кБ
Обсяг енергонезалежної пам'яті (EEPROM)	1 кБ
Частота тактування	16 мГц
Довжина плати	68,6 мм
Ширина плати	53,4 мм
Вага	25 г

Для створення модуля системи захисту від дронів було обрано платформу Arduino UNO R3, характеристики якої достатні для виконання поставлених задач, при цьому має невелику вартість.

3.2 Дешифратор

Згідно технічному завданню необхідно використовувати таку модель дешифратора – 74НС138 [18 – 21]. Дешифратор 74НС138 є важливим компонентом в цифрових електронних схемах, він використовується для перетворення бінарних кодів в активні вихідні сигнали. Цей дешифратор застосовується в різних проектах, зокрема в системах управління, в додатках та схемах на основі Arduino. 74НС138 ефективний у високопродуктивних швидкісних системах, оскільки затримка від цього декодера є незначною [21]. Зовнішній вигляд та логічна схема дешифратора 74НС138 наведені на рис. 3.3.

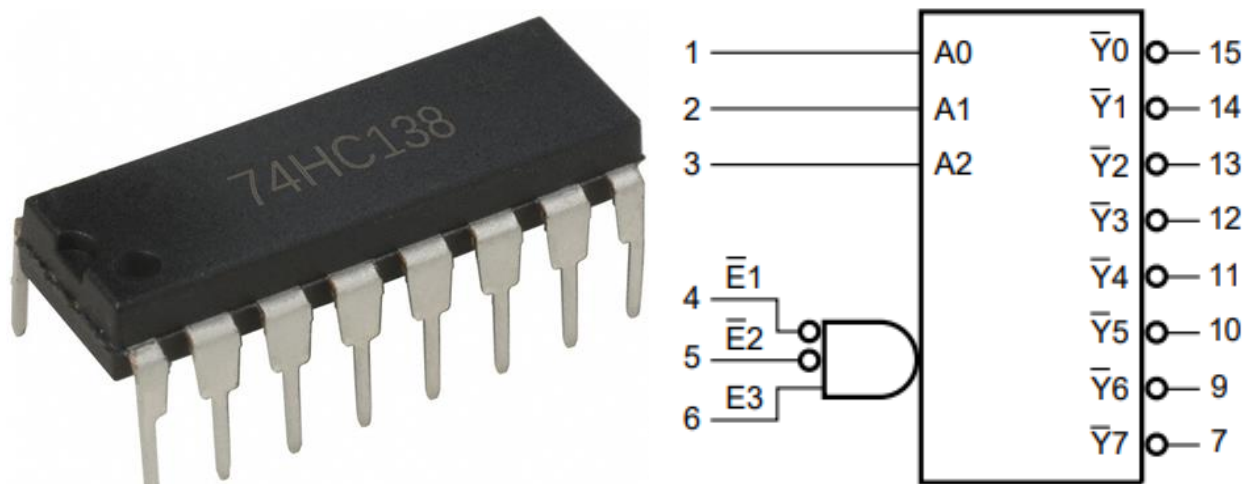


Рисунок 3.3 – Дешифратор 74НС138

Дешифратор 74НС138 – це інтегрована мікросхема, що містить декодер/демультиплексор з 3 – 8 рядками. Він приймає три двійкові входи та декодує їх в один з восьми виходів. Кожна вихідна лінія відповідає унікальній комбінації вхідних сигналів [18, 20]. Цей 3-вхідний дешифратор може активувати один із восьми виходів залежно від стану вхідних сигналів. Дешифратор 74НС138 має:

- три входи (A0, A1, A2), які приймають бінарний код,
- вісім виходів (Y0-Y7), які можуть бути активовані,

– три входи для керування (E1, E2, E3), що дозволяють вмикати або вимикати роботу дешифратора.

Технічні характеристики дешифратора 74НС138 наведено в табл. 3.2.

Таблиця 3.2 – Основні технічні характеристики 74НС138

1	Тип логіки	дешифратор 3 на 8, демультиплексор
2	Напруга живлення	від 2В до 6В
3	Робоча напруга	5В
4	Вихідний струм	+5,2 мА
5	Вхідний струм	max 1 мкА
6	Температурний діапазон	від –40°C до +125°C
7	Корпус	DIP-16, SOIC-16, TSSOP-16
8	Вартість	10 – 15 грн
9	Виробник	Texas Instruments

Принцип роботи 74НС138 базується на логічних операціях. Коли на входах будуть встановлені певні комбінації, відповідний вихід ставатиме активним і прийматиме низький рівень (0В), інші виходи залишатимуться на високому рівні (5В). Це дозволяє використовувати дешифратор для вибору певних пристроїв або сигналів, залежно від заданої логіки.

Схема підключення 74НС138 дуже проста. На входи A0, A1 і A2 подаються сигнали керування, а виходи Y0-Y7 підключаються до пристроїв, які необхідно активувати. Входи E1, E2 і E3 мають бути правильно налаштовані для активації дешифратора. При включенні всіх цих трьох входів на низькому рівні дешифратор буде активний [18, 20].

Для підключення дешифратора в схемах з Arduino входи A0, A1 та A2 підключаються до цифрових виводів Arduino, а виходи Y0-Y7 до світлодіодів або інших пристроїв. Це дозволяє керувати станом кожного пристрою в залежності від стану вхідних сигналів.

При виборі дешифратора 74НС138 важливо враховувати кілька факторів:

- напруга живлення має відповідати вимогам проекту;
- варто враховувати кількість входів та виходів, що вимагає проект;
- важливо перевірити швидкість роботи мікросхеми, особливо якщо вона використовуватиметься у високошвидкісних додатках.

Логіка роботи дешифратора 74HC138 ґрунтується на комбінації логічних рівнів. При подачі на входи певних значень дешифратор генерує відповідний вихідний сигнал. Наприклад, якщо на входах A0, A1 і A2 встановлено значення 101, активується вихід Y5, а інші виходи залишаються неактивними. Розуміння логіки роботи дешифратора дозволяє ефективно використовувати його у проектах.

3.3 Шинні формувачі

Згідно технічному завданню необхідно використовувати таку модель шинних формувачів – 74HC245/74LS245 [22, 23]. 74HC245/74LS245 - це мікросхема, розроблена як восьмиканальний шинний приймач-передавач (трансивер) з 3-ма виходами, що дозволяє двонаправлену передачу даних між різними частинами цифрової системи [22]. Зовнішній вигляд та логічна схема шинних формувачів 74HC245/74LS245 наведені на рис. 3.4.

Шинні трансивери 74HC245/74LS245 призначені для асинхронного двостороннього зв'язку між шинами даних. Реалізація функції керування мінімізує вимоги до зовнішньої синхронізації.

Пристрій дозволяє передавати дані з шини А на шину В або з шини В на шину А залежно від логічного рівня на вході керування напрямком (DIR). Вхід увімкнення (G) може бути використаний для вимкнення пристрою, щоб шини були ефективно ізольовані.

Керування напрямком потоку даних виконується за допомогою входу напрямку (DIR). Коли встановлюється DIR у значення HIGH (високе), дані переміщуються з шини А до шини В, а коли встановлюється DIR у значення LOW (низьке), дані переміщуються з шини В до шини А.

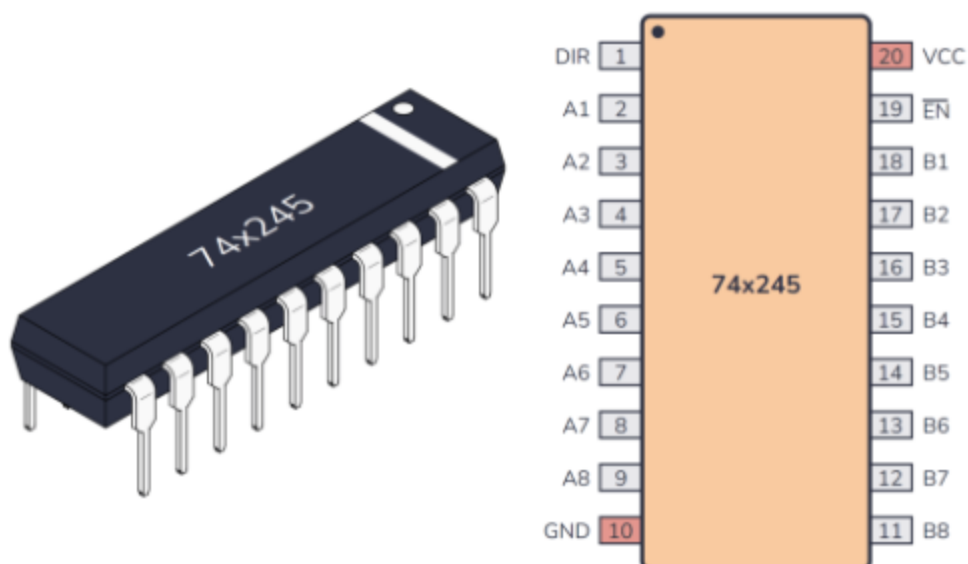


Рисунок 3.4 – Шинний формувач 74HC245/74LS245

Технічні характеристики 74HC245/74LS245 наведено в табл. 3.3.

Таблиця 3.3 – Основні технічні характеристики 74HC138

1	Тип логіки	шинний трансивер, 74HC245 – CMOS, 74LS245 – TTL
2	Напруга	74HC245 – від 2В до 6В, 74LS245 – 5В
3	Кількість цоколів	20
4	IOL (струм споживання)	24 мА
5	IOH (струм джерела)	15 мА
6	Типовий час затримки поширення між портами	8 нс
7	Типовий час увімкнення/вимкнення	17 нс
8	Корпус	високощільний, 20-контактний
9	Вартість	14 – 30 грн
10	Виробник	Futurlec

За допомогою входу ввімкнення (EN) можна вмикати/вимикати виходи. Коли цей контакт має низький рівень, трансивер працює над передачею даних. Якщо він має високий рівень, шини роз'єднуються, так що обидві сторони переходять у стан високого імпедансу. Цей стан високого імпедансу допомагає запобігти перешкодам з іншими пристроями на тій самій шині [23].

Основним призначенням шинних трансиверів 74HC245/74LS245 є керування двосторонньою передачею цифрових даних між двома шинами, зокрема мікроконтролером та периферійними пристроями.

3.4 Оптипара для генерації та прийому світлового променя

Для реалізації модуля системи захисту потрібні якісні малопотужні вузькоспрямовані випромінювачі світлових променів, які мають бути невидимими і для людського ока, і для камер (оскільки FPV-дрони обладнані камерами).

Людина може бачити видиме світло (довжина хвилі від 380 до 750 нм), у камер чутливість вище і вони бачать деякі невидимі спектри (це залежить від особливостей камер). Саме тому для поставленої задачі найкращим рішенням є ІЧ-випромінювач (інфрачервоний лазер) з довжиною хвилі 940 нм. Промінь 940 нм повністю невидимий для людського ока і для більшості камер. Деякі камери нічного бачення здатні таке світло побачити, але тільки в темряві і у вигляді слабкої точки. Тому випромінювач має бути спрямований так, щоб камера не бачила саму точку падіння променя (можна використати непрозорі трубки на приймальній стороні).

Лазери з довжиною хвилі 940 нм є вузькоспрямованими (кут розсіювання 5° – 15° , що дозволяє створити світлову точку на прийомі, а не широку пляму), вони дають найбільш чіткий і вузький промінь на великій відстані.

Для побудови запропонованої системи знадобиться пара пристроїв, що працюють у спектрі 940 нм, що забезпечить повну візуальну скритність.

Перший пристрій - це випромінювач - ІЧ-лазерний діод або готовий лазерний модуль на 940 нм. На відміну від звичайного світлодіода, лазер дає надзвичайно вузький промінь, який майже не розсіюється на відстані. Для поставленої мети достатньо модуля на 5–10 мВт (mW), він малопотужний і створює чітку точку для приймача.

Другий пристрій - це приймач. Потрібен фотодіод або фоторезистор, що мають пік чутливості в районі 950 нм. Щоб приймач не спрацьовував на сонячне світло чи лампи, перед ним обов'язково ставиться ІЧ-фільтр (темне скло), яке пропускає лише промінь лазера.

Існують деякі готові рішення, що використовуються в охоронних системах. Вони вже мають вологозахист, лінзи для фокусування та реле для підключення. Випромінювач 940nm 5mW Infrared Laser Diode Module має вбудовану систему фокусування, що дозволяє отримати тонку точку на відстані до 10 – 15 метрів. Він схожий на модуль KY-008, але з довжиною хвилі 940 нм. Такий модуль є недешевим [24]. Приймач – ІЧ-фотодіод 5мм 940нм (наприклад, KY-022, аналоги BPW34 або стандартні діоди з наборів Arduino).

В роботі пропонується використати просту пару світлодіод + фотодіод F5 інфрачервоний IR 940нм (рис. 3.5), вона є дешевою та енергоефективною [25].



Рисунок 3.5 – Оптипара F5 IR 940нм

F5 IR 940nm – це звичайний двопіновий елемент, який працює як аналоговий датчик. Він потребує поміщення у тонку трубку (бленду) для захисту від бокового світла. Технічні характеристики оптопар F5 IR 940nm наведено в табл. 3.4.

Таблиця 3.4 – Технічні характеристики F5 IR 940nm

1	Довжина хвилі		940 нм
2	Тип корпусу		5 мм (F5)
3	Світлодіод	Пряма напруга	1,2–1,6 В при 100 мА
		Максимальний струм	100 мА (піковий 200 мА)
		Інтенсивність випромінювання	40 – 200 мВт/ср при 100 мА
		Кут огляду	$\pm 17^\circ$
		Час наростання/спаду	15 нс/15 нс
4	Фотодіод	Діапазон чутливості	780–1050 нм
		Зворотний темний струм	0,1 нА (типово)
		Зворотний струм світла	60 мкА при 1 мВт/см ² , 940 нм
		Кут чутливості	$\pm 20^\circ$
		Час наростання/спаду	80 нс/60 нс
5	Робоча температура		– 40°C до +85°C
6	Матеріал корпусу		Пластик (прозорий для світлодіода, чорний для фотодіода)

F5 IR 940nm забезпечує швидку передачу в реальному часі (завдяки малому часу наростання/спаду світлодіода та фотодіода), надійність та точність (завдяки високій чутливості фотодіода) [25].

При фінансовій можливості можна використовувати пару випромінювач 940nm 5mW Infrared Laser Diode Module + приймач KY-022 (на базі VS1838B або аналогів).

Обидва варіанти оптопарі мають інвертовану логіку роботи і два стани:

1) логічний 0 (LOW) – це стан «Норма» (промінь проходить): лазер постійно світить чітко в приймач, внутрішня мікросхема приймача розпізнає частоту променю (38 кГц), відкриває внутрішній транзистор і притискає вихідний сигнал до землі, функція `digitalRead(pin)` повертає 0 або LOW – це означає, що порушень немає;

2) логічний 1 (HIGH) – стан «Тривога» (промінь перекрито): об'єкт перетинає промінь (або лазер вимкнено), приймач перестає бачити частоту 38 кГц, внутрішній транзистор закривається, завдяки вбудованому підтягуючому резистору, напруга на виході піднімається до живлення (5V), функція `digitalRead(pin)` повертає 1 або HIGH – це означає перетин променю або наявність порушення.

3.5 Програмні засоби

Для роботи на платформі Arduino використовується мова програмування Arduino (фреймворк Wiring на основі C++) та програмне забезпечення Arduino (IDE), засноване на Processing [16].

Структура більшості програм Arduino дуже схожа, тому що широко застосовується процедурне програмування, при якому програми складаються з невеликих окремих підпрограм (процедур). Найменшим і неподільним кроком процедурного програмування є команда (оператор або інструкція). Програма працює послідовно від команди до команди. За допомогою програми програміст дає мікроконтролеру вказівки, в якій послідовності потрібно діяти. Метою цього принципу програмування є простота розробки і можливість повторного використання фрагментів вихідного коду.

При послідовному програмуванні основна частина програми виконується як нескінченний цикл, де повторюються окремі процедури. Якщо виникає потреба перервати послідовне виконання програми, використовується переривання `Interrupt`. Якщо відбудеться переривання (зовнішнє або

внутрішнє), основний цикл Main-Loop перерветься і відбудеться перехід в програму обробки переривань Interrupt-Routine, де юде виконано якесь спеціальне завдання. Потім робота знову триватиме в основному циклі, в якому також можуть виконуватися допоміжні операції.

Програма для Arduino містить в собі такі основні частини: коментарі (опис програми), заголовки файлів, підключення бібліотек, опис змінних, стандартне налаштування (порти і конфігурація) – *void setup ()*, основна частина (цикл) – *void loop ()*, власні процедури.

Інтегроване середовище розробки Arduino або програмне забезпечення Arduino – IDE – містить текстовий редактор для написання коду, область повідомлень, текстову консоль, панель інструментів з кнопками для виконання поширених функцій та низку меню. Воно підключається до обладнання Arduino для завантаження програм та взаємодії з ними [26].

Програмне забезпечення IDE необхідно завантажити з офіційного сайту [27], де можливо обрати версію IDE для конкретної операційної системи (рис. 3.6).



Arduino IDE 2.3.10

[Release notes](#)

The new major release of the Arduino IDE is faster and even more powerful! In addition to a more modern editor and a more responsive interface it features autocompletion, code navigation, and even a live debugger. For more details, check the [Arduino IDE 2.0 documentation](#).

Windows Win 10 or newer (64-bit)

Windows Win 10 or newer (64-bit) ✓

Windows MSI installer

Windows ZIP file

Linux AppImage (64-bit X86-64)

Linux ZIP file (64-bit X86-64)

macOS Intel 12 Monterey or newer (64-bit)

macOS Apple Silicon 12 Monterey or newer (64-bit)

DOWNLOAD

Рисунок 3.6 – Завантаження IDE

Arduino IDE – це безкоштовне та відкрите середовище розробки, що дає можливість програмувати додатки широкого спектру на платах Arduino. Завдяки спрощеному діалекту C++, Arduino IDE дозволяє перевіряти та компілювати код, а також завантажувати його безпосередньо на плату.

Arduino IDE має інтуїтивно зрозумілий інтерфейс. Вкладки у верхній частині дозволяють працювати над кількома проєктами одночасно. Редактор коду містить такі інструменти, як підсвічування синтаксису, автозаповнення та перевірка на помилки, які допомагають мінімізувати помилки програмування [28].

Виведення коду відображається внизу екрана, де можна перевірити, чи є помилки у програмуванні, або чи процес компіляції був успішно завершений. Після компіляції можна завантажити програму на плату Arduino безпосередньо з Arduino IDE, якщо вона підключена та налаштована в додатку. Крім того, Arduino IDE дозволяє контролювати плату в режимі реального часу, що є незамінним інструментом для налагодження проєктів [28].

4 РОЗРОБКА АЛГОРИТМУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МОДУЛЯ СИСТЕМИ ЗАХИСТУ

4.1 Алгоритм роботи модуля системи захисту

Для програмної реалізації модуля системи захисту від дронів перед написанням коду програми необхідно розробити алгоритм роботи модуля. Суть алгоритму роботи модуля системи захисту полягає в наступному:

- спочатку задається кількість сегментів в одному модулі ($N = 5$), кількість фотоприймачів вертикальних світлових променів ($M = 8$) та признак роботи системи ($k = 1$);

- потім задається перший номер сегменту ($n = 0$), перший номер фотоприймача в сегменті ($m = 0$) та перевіряється наявність променю на відповідному фотоприймачі;

- якщо променю немає ($F_{ij} = 1$) – це означає, що промінь порушений дроном і подається сигнал для організації пострілу зі зброї в напрямку $n = i$, $m = j$ для ліквідації ворожої цілі;

- якщо промінь наявний ($F_{ij} = 0$) – це означає, що контрольоване поле не порушено і необхідно перейти до перевірки наступного фотоприймача;

- після перевірки всіх фотоприймачів у першому сегменті, відбувається перехід до наступного сегменту ($n = n + 1$) і перевіряються послідовно всі фотоприймачі цього сегменту;

- таким чином перевіряються всі фотоприймачі всіх сегментів і там де виявляється порушення – подається сигнал на постріл;

- після перевірки всіх сегментів, починається нове коло перевірки спочатку;

- система буде так працювати до її вимкнення ($k = 0$).

Алгоритм роботи модуля виявлення та ліквідації ворожої цілі наведено на рис. 4.1.

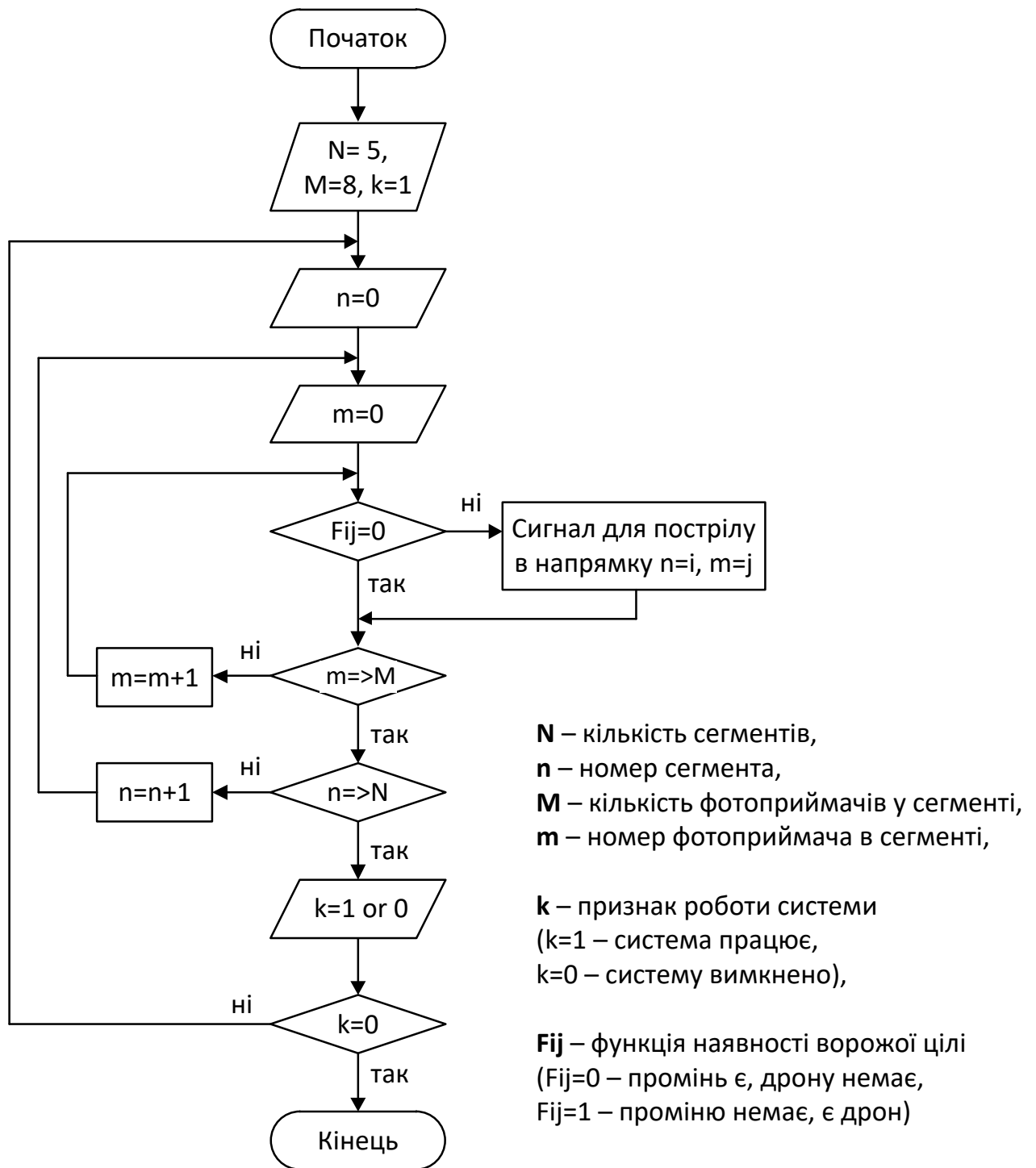


Рисунок 4.1 – Алгоритм роботи модуля системи захисту

Створення блок-схеми алгоритму є важливим етапом розробки, бо воно дозволило сформувати послідовність процесів та візуалізувати логіку роботи модуля системи захисту від дронів, дало змогу виявити неточності і помилки та оптимізувати певні кроки до написання коду.

4.2 Програмна реалізація роботи модуля системи захисту

Спочатку необхідно завантажити та встановити середовище розробки та написати програму, потім необхідно підключити пристрої, встановити драйвери, запустити Arduino IDE, відкрити код програми, обрати в меню відповідну модель Arduino (Tools > Board > Arduino Uno), обрати та підключити необхідний послідовний порт (Tools > Serial Port > COM9) і далі вже працювати з програмою та її налагодженням.

Запропонований алгоритм (рис. 3.6) був реалізований у вигляді програми для Arduino на мові C++ в інтегрованому середовищі IDE. Код програми представлено в додатку А.

На рис. 4.2 – 4.5 показано процес розробки програми.

Рядки програми з 1 по 15 – це опис змінних, налаштування пінів, задання кількості сегментів та датчиків в кожному сегменті (рис. 4.2).

В рядках з 16 по 28 – прописана функція ініціалізації (рис. 4.2). Функція ініціалізації – це спеціальний фрагмент коду, який готує систему до роботи (встановлює початкові значення, виділяє пам'ять, підключає бази даних або завантажує налаштування перед тим, коли програма почне цим користуватися).

Налаштування виходів, показано на рис. 4.3 – це рядки з 29 по 38. Тут варто звернути увагу, що у плати Arduino Uno 14 цифрових входів/виходів, 8 з них (0 – 7) в даній роботі було використано в якості цифрових входів, а інші 6 (8 – 13) – в якості цифрових виходів. Оскільки для проєкту потрібно 8 виходів, то було задіяно 2 аналогові виходи (A3 та A4), оскільки вони можуть бути використані як цифрові.

На рис. 4.4 показано основну частину програми (рядки 39 – 62), в якій послідовно перевіряється кожен датчик кожного сегмента на наявність порушення, та при виявленні порушення генерується адреса, за якою має бути спрямований постріл для ліквідації ворожого об'єкта.

На рис. 4.5 показано заключні моменти програми (рядки 63 – 75), де встановлюються адреси на A0 – A2 у двійковому коді та задається затримка.

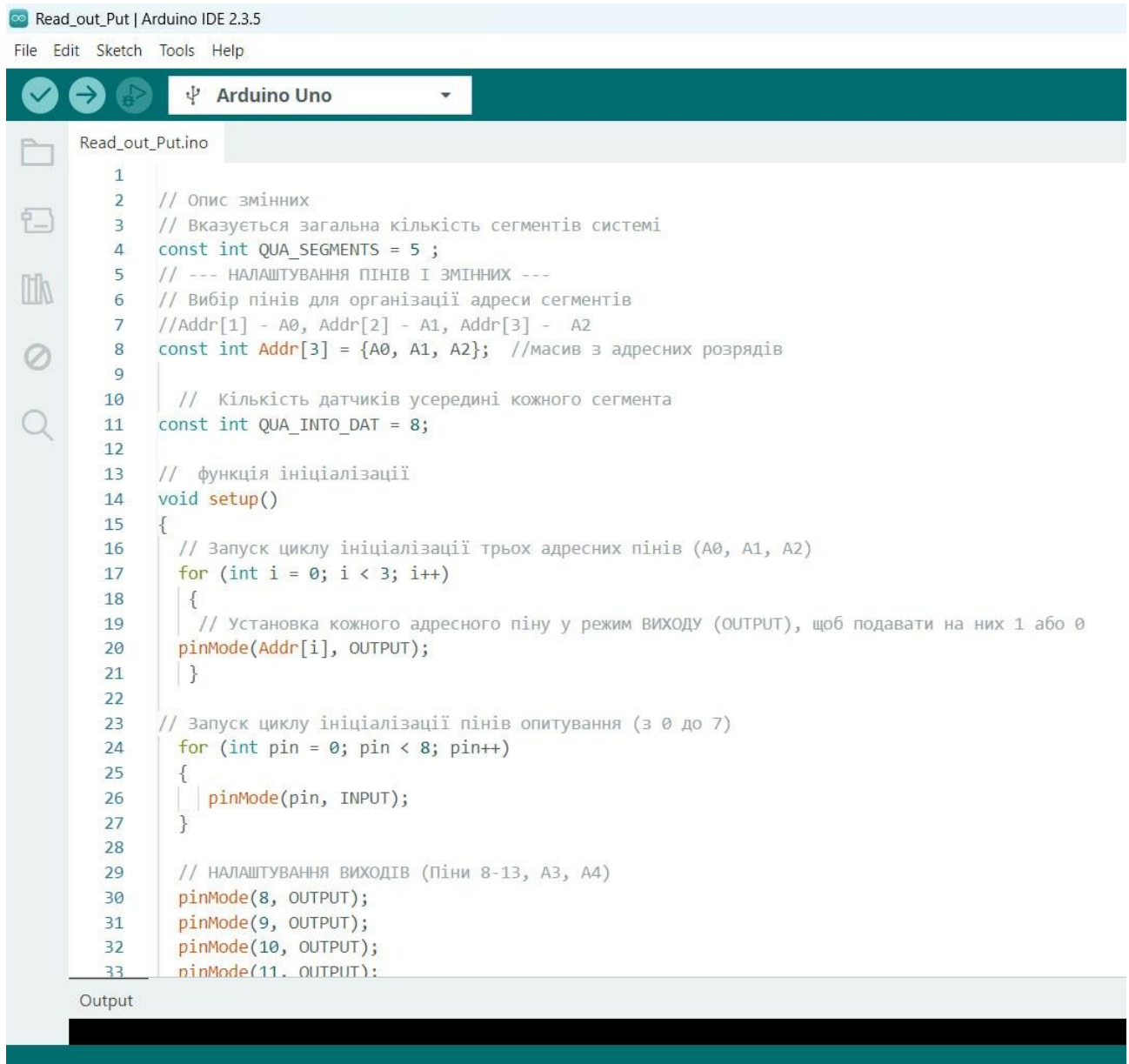


Рисунок 4.2 – Початок програми

```

28
29 // НАЛАШТУВАННЯ ВИХОДІВ (піни 8-13, A3, A4)
30 pinMode(8, OUTPUT);
31 pinMode(9, OUTPUT);
32 pinMode(10, OUTPUT);
33 pinMode(11, OUTPUT);
34 pinMode(12, OUTPUT);
35 pinMode(13, OUTPUT);
36 pinMode(A3, OUTPUT);
37 pinMode(A4, OUTPUT);
38 }

```

Рисунок 4.3 – Налаштування виходів

```

39 void loop()
40 {
41     readSensors();
42
43     // Пряма відповідність: ВХІД -> ВИХІД
44
45     // Якщо на піні 0 одиниця -> пін 8 дає команда постріл і нахше 0 і так далі 7 разів
46     if (digitalRead(0) == HIGH) { digitalWrite(8, HIGH); } else { digitalWrite(8, LOW); }
47
48     if (digitalRead(1) == HIGH) { digitalWrite(9, HIGH); } else { digitalWrite(9, LOW); }
49
50     if (digitalRead(2) == HIGH) { digitalWrite(10, HIGH); } else { digitalWrite(10, LOW); }
51
52     if (digitalRead(3) == HIGH) { digitalWrite(11, HIGH); } else { digitalWrite(11, LOW); }
53
54     if (digitalRead(4) == HIGH) { digitalWrite(12, HIGH); } else { digitalWrite(12, LOW); }
55
56     if (digitalRead(5) == HIGH) { digitalWrite(13, HIGH); } else { digitalWrite(13, LOW); }
57
58     if (digitalRead(6) == HIGH) { digitalWrite(A3, HIGH); } else { digitalWrite(A3, LOW); }
59
60     if (digitalRead(7) == HIGH) { digitalWrite(A4, HIGH); } else { digitalWrite(A4, LOW); }
61 }
62

```

Рисунок 4.4 – Основна частина програми

```

63 void readSensors()
64 {
65     for (int segment = 0; segment < QUA_SEGMENTS; segment++)
66     {
67         // Встановлення адреси сегмента на пінах A0, A1, A2 у двійковому коді
68         // segment переводиться в 3 бита: bit0 -> A0, bit1 -> A1, bit2 -> A2
69         digitalWrite(Addr[0], (segment & 0x01) ? HIGH : LOW); // pin 0 (A0)
70         digitalWrite(Addr[1], (segment & 0x02) ? HIGH : LOW); // pin 1 (A1)
71         digitalWrite(Addr[2], (segment & 0x04) ? HIGH : LOW); // pin 2 (A2)
72     }
73     delayMicroseconds(10); // затримка залежить від швидкодії системи
74 }
75

```

Рисунок 4.5 – Встановлення адрес у двійковому коді

4.3 Перевірка роботи програми

Для перевірки роботи написаної програми було використано симулятор SimulIDE.

SimulIDE – це простий симулятор електронних схем у реальному часі, призначений для експериментів з аналоговими та цифровими електронними схемами та мікроконтролерами. Він підтримує різні мікроконтролери та процесори, зокрема і Arduino.

Ключовими особливостями цього симулятора є простота, швидкість та зручність використання. З його допомогою можна моделювати та взаємодіяти зі схемами за лічені хвилини; просто створювати схему, запускати її та бачити, як вона працює [29].

Швидкість моделювання – одна з найважливіших характеристик цього симулятора. SimulIDE є оптимізований для досягнення відмінної швидкості та низького використання процесора.

SimulIDE має також редактор коду та відладчик для Arduino. В цьому симуляторі є можливість писати, компілювати та виконувати базове налагодження програми [29].

Процес перевірки програми для Arduino в симуляторі SimulIDE складається з двох основних кроків:

- створення електричної схеми,
- завантаження скомпільованого коду (.hex файла) у віртуальний мікроконтролер.

Симулятору для роботи потрібен скомпільований бінарний файл програми. Для цього використовується Arduino IDE: необхідно відкрити скетч, далі в меню перейти у налаштування (File > Preferences) та виконати компіляцію (Compilation). Після компіляції в нижній частині вікна можна знайти шлях до файла з розширенням .hex. Необхідно завантажити його в симулятор та включити симуляцію (кнопка Power Circuit). Після цього починається симуляція і можна спостерігати за роботою віртуальної схеми в режимі реального часу.

Для перевірки роботи написаної програми, спочатку було завантажено симулятор SimulIDE з офіційного сайту [29]. Потім було зібрано часткову схему з Arduino Uno, а саме з панелі компонентів відкрито Arduino Uno на робочому полі, додано необхідні елементи та з'єднано їх проводами у єдину схему (підключено три входи, на які подається сигнал, встановлено три кнопки). Відкрито файл скомпільованого коду та запущено симуляцію.

В даному проекті натискання кнопки перекриває подачу напруги та імітує

порушення, тобто відсутність прийому променя. Якщо кнопку натиснути – на відповідному виході засвічується вбудований світлодіод (рис. 4.6) і на виході отримуємо адресу, яка вказує на необхідність пострілу в напрямку, де виявлено порушення. В даному випадку на рис. 4.6 показано порушення на вході №6 та засвічення світло діоду на відповідному виході №13.

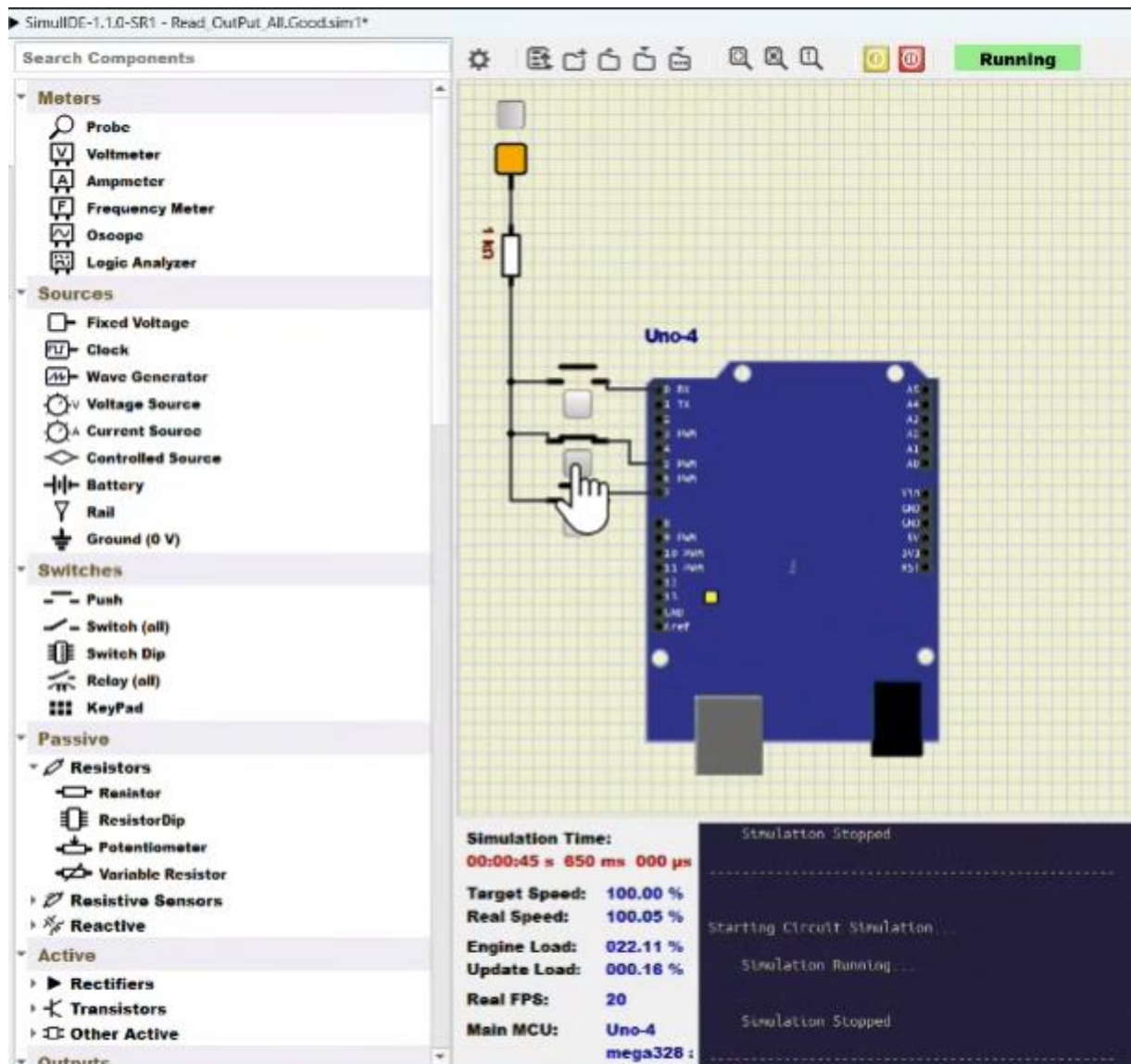


Рисунок 4.6 – Перевірка роботи програми (виявлення порушення)

Якщо кнопки не натискати – це означатиме відсутність порушень, жодні світлодіоди не будуть світитися та на виході не буде генеруватися адреса і сигнал для пострілу (рис. 4.7).

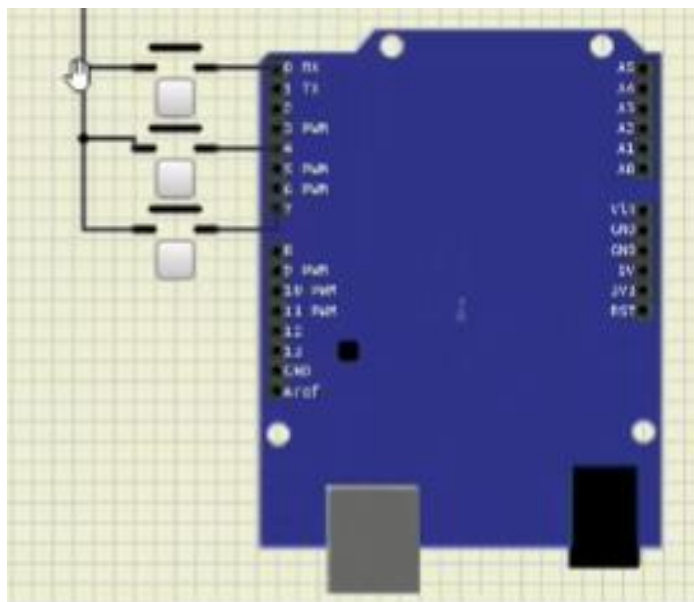


Рисунок 4.7 – Перевірка роботи програми (відсутність порушення)

На рис. 4.8 показано ще одну перевірку: використання осцилографа для відстеження генерування адреси сегмента в бінарному виді на виходах A0 – A2.

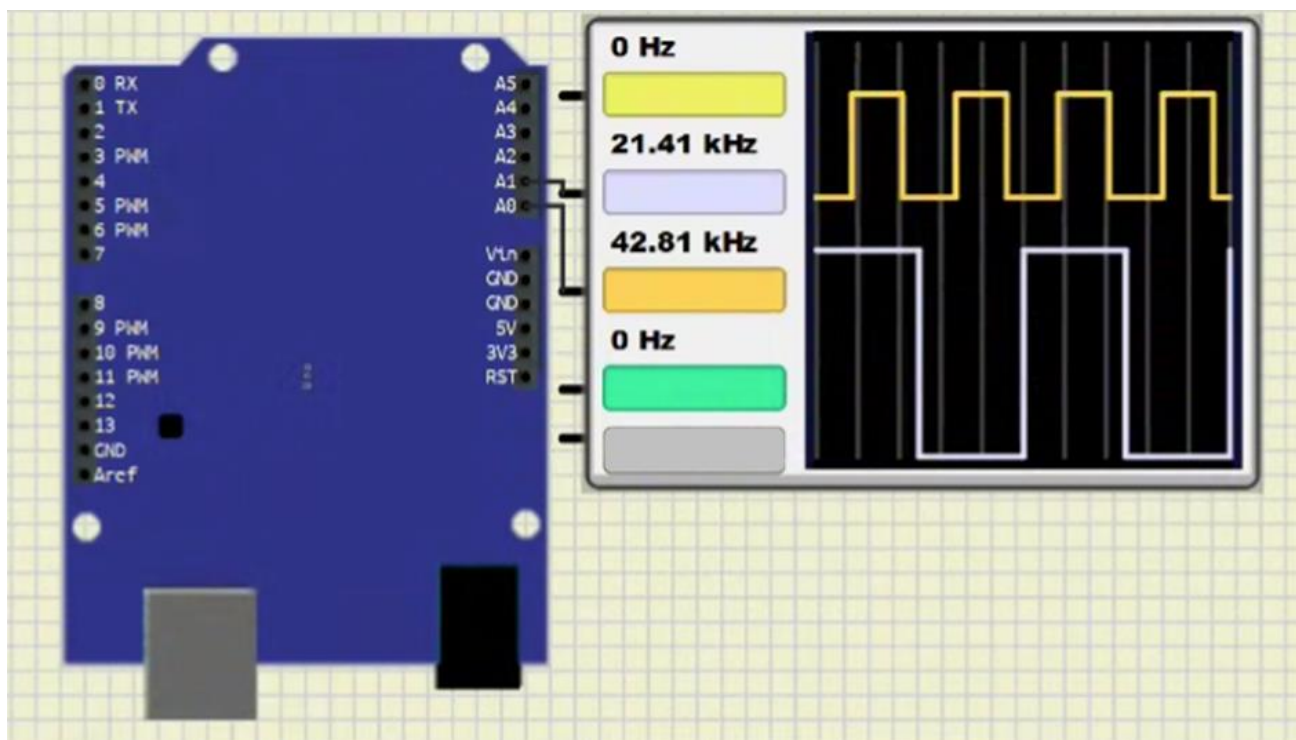


Рисунок 4.8 – Перевірка роботи програми (за допомогою осцилографа)

В даному проєкті аналогові входи A0, A1 та A2 використовуються як цифрові виходи (це є можливим, оскільки вони є багатофункціональними). Це реалізовано за допомогою програми: в рядках 14 – 22 дані адресні піни встановлено у режим виходів (рис. 4.2). Логіка генерування адреси сегмента показана на рис. 4.9.

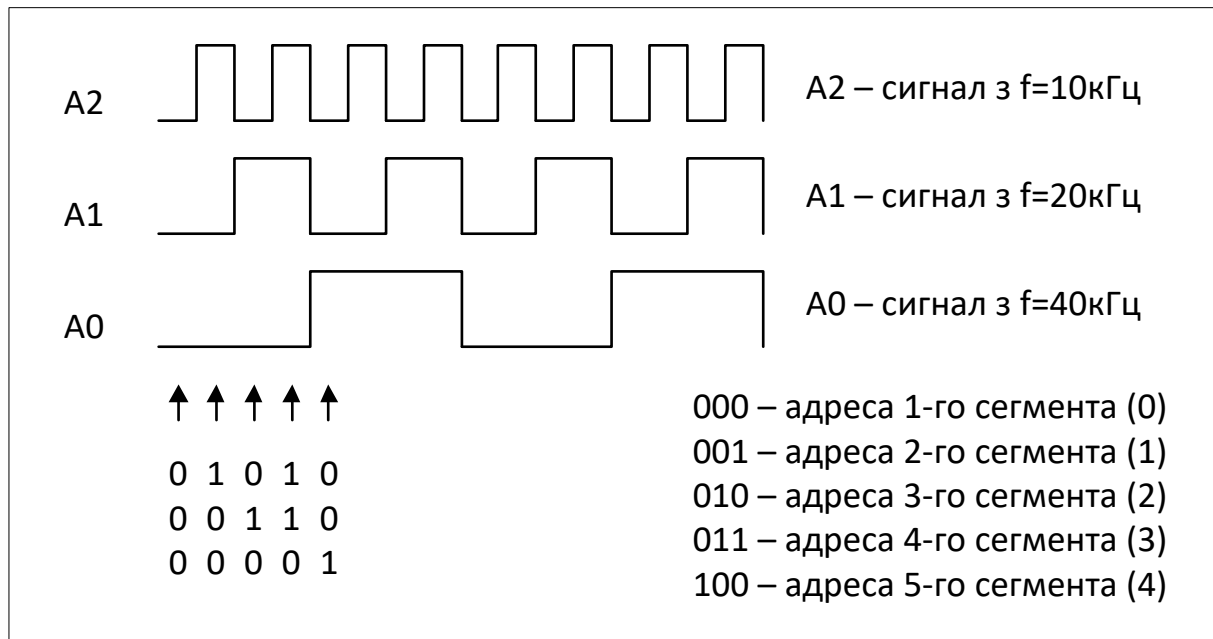


Рисунок 4.9 – Логіка генерування адреси сегмента

На рис. 4.8 було сгенеровано сигнали A0 та A1 , але цього достатньо, щоб побачити, що логіка успішно працює.

Отже, коли на якомусь датчику буде виявлено порушення, то в цей момент буде зафіксовано не тільки номер датчика, але і адреса сегмента, і саме туди буде спрямований постріл для знищення ворожої цілі.

Таким чином, за допомогою симулятора SimulIDE було перевірено роботу програми.

ВИСНОВКИ

В час війни ворожі БПЛА становлять велику загрозу для військових об'єктів, критичної інфраструктури, житлових будівель та людей. Поточні системи боротьби з дронами не є абсолютно ефективними, тому докладаються зусилля для пошуку нових, більш ефективних методів виявлення та нейтралізації дронів.

В роботі було розглянуто та проаналізовано ряд питань, що стосуються виявлення та протидії ворожим дронам в умовах війни. Для того, щоб запропонувати новий метод боротьби з дронами, було проведено аналіз наукової літератури та інших джерел, що описують існуючі системи боротьби з дронами.

В першому розділі розглянуто питання актуальності проблеми захисту від БПЛА в Україні, описано БПЛА військового типу, досліджено методи виявлення та нейтралізації ворожих дронів, виконано порівняльний аналіз сучасних засобів захисту від FPV-дронів та виявлено, що існуючі методи мають певні проблеми та не гарантують стовідсоткового захисту від ворожих БПЛА.

В другому розділі запропоновано модульну систему захисту від ворожих дронів, виконано проєктування її структури і принципу дії та розроблено функціональну схему модуля системи захисту.

В третьому розділі розглянуто апаратні та програмні засоби для створення модуля системи захисту. Описані платформа Arduino, дешифратор, шинні формувачі, варіанти оптопар для генерації та прийому світлових променів, а також програмні засоби (мова програмування Arduino - фреймворк Wiring на основі C++ та програмне забезпечення IDE) для розробки роботи модуля.

В четвертому розділі розроблено алгоритм та програмну реалізацію роботи модуля системи захисту, а також виконано перевірку роботи програми на симуляторі SimulIDE.

Створення всієї системи захисту від FPV-дронів – дуже велика і складна задача, що потребує вирішення багатьох питань, в тому числі не тільки інженерних, але і військових, і будівельних та ін. В роботі основна увага була зосереджена на розробці модуля виявлення ворожої цілі.

Результати роботи було частково представлено на 30-му Міжнародному молодіжному форумі "Радіoeлектроніка і молодь у ХХІ столітті» та за темою кваліфікаційної роботи були опубліковані тези доповіді [30] в збірнику конференції "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій".

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Countering FPV Drones: Insights from Ukraine's Combat Experience / O. Tytarenko, S. Abramov, M. Ktitorov, and Y. Synytsina. *Advances in Military Technology*. 2025. Vol. 20, No. 2. P. 421 – 434. ISSN 1802-2308. URL: <https://doi.org/10.3849/aimt.01998>.
2. Протидія FPV-дронам: системний підхід та створення спеціалізованих підрозділів. ГО Військова школа “Боривітер”. 19.08.2024. URL: <https://boryviter.org.ua/articles/protydiya-vorozhym-fpv-dronam/>.
3. Червяков О.І., Євтушенко І.В., Букреєв О.І., Білоус В.В. Безпілотні повітряні засоби ураження сил вторгнення рф. Харків : *Служба безпеки України*, 2023. 212 с. URL: https://sprotyvg7.com.ua/wp-content/uploads/2023/06/1.3._Довідник_БПЛА.pdf.
4. В Україні зафіксовано 256 тисяч злочинів, пов’язаних з агресією Росії – Кравченко. *ZMINA*. 08.05.2026. URL: <https://zmina.info/news/v-ukrayini-zafiksovano-ponad-250-tysyach-voyennyh-zlochyniv-rf-ofis-genprokurora/>.
5. Кельм Н., Шульман О., Головінський Н. П’ять графіків про чотири роки війни. Тривоги, «Шахеда», ракети і втрати. *Texty.org.ua*. 24.02.2026. URL: <https://texty.org.ua/articles/116934/chernetka-pyat-hrafikiv-pro-chotyry-roky-vijny-tryvohy-shaxedy-rakety-i-vtraty/>.
6. Дончевська В. За чотири роки Росія запустила по Україні понад 78 тисяч дронів. *Точка Сходу*. 24.02.2026. URL: <https://cxid.media/news/za-chotyry-roky-rosiia-zapustyla-po-ukraini-ponad-78-tysiach-droniv/>.
7. Łukasiewicz J. and Kobaszyńska-Twardowska A. Proposed method for building an anti-drone system for the protection of facilities important for state security. *Security and Defence Quarterly*. 2022. 39(3), P. 88–107. URL: <https://doi.org/10.35467/sdq/149268>.

8. Куцька Н. Інженер БПЛА. Базовий курс. *Інженерна школа БПЛА від DreamUkraine*. URL: https://courses.prometheus.org.ua/assets/courseware/v1/68ebc064390d45e9563400cfe630e96d/asset-v1:Prometheus+UAV_EB101+2023_T3+type@asset+block/1.4._Класифікації_Безпілотних_літальних_апаратів_БПЛА_.pdf.
9. 5 Types of Military Drone in 2026: An Expert Engineering Perspective. *China Moneypro. News*. URL: <https://www.moneyprouav.com/5-types-of-military-drone-in-2026-an-expert-engineering-perspective/> (дата звернення: 05.05.2026).
10. Channing Pear. Fixed-Wing vs. Multi-Rotor Drones: Endurance Comparison. *Anvil Labs*. 22.12.2024. URL: <https://anvil.so/post/fixed-wing-vs-multi-rotor-drones-endurance-comparison>.
11. Козацький О. FPV-дрони: зброя, що змінила сучасну війну. *Мілітарний*. 12.10.2023. URL: <https://militaryni.com/uk/articles/fpv-drony-zbroya-shho-zminyla-suchasnu-vijnu/>.
12. FPV-дрони проти класичних БПЛА: у чому різниця та що ефективніше? *ARM Drones*. 12.05.2025. URL: <https://armdrones.com.ua/blog/fpv-drony-proty-klasychnyh-bpla-u-chomu-riznyczya-ta-shho-efektyvnishe/>.
13. Anti-drone Sensors, Effectors, and Systems – A Concise Overview / D. Zmysłowski, P. Skokowski & J.M. Kelner. *International Journal on Marine Navigation and Safety of Sea Transportation*. 2023. Vol. 17, No. 2. P. 455 – 461. URL: <https://doi.org/10.12716/1001.17.02.23>.
14. Survey on Anti-Drone Systems: Components, Designs, and Challenges / S.Park , H. Tae Kim, S. Lee, H.Joo and H. Kim. *IEEE Access*. 2021. P. 42635 – 42659. URL: <https://doi.org/10.1109/ACCESS.2021.3065926>.
15. What is Arduino? *Arduino. Learn*. 25.01.2022. URL: <https://docs.arduino.cc/learn/starting-guide/whats-arduino/>.
16. Stuart Yarnold. *Arduino in Easy Steps*. Warwickshire, U.K. : In Easy Steps Limited, 2015. 192 с.
17. Arduino Uno R3 (ATmega328, CH340G). *Ardushop. Arduino*. URL: <https://ardushop.in.ua/arduino/arduino-uno-r3-atmega328-ch340g> (дата звернення: 10.06.2026).

18. 74HC138; 74HCT138 3-to-8 line decoder/demultiplexer; inverting Rev. 10 — 26 February 2024. Nexperia. URL: https://assets.nexperia.com/documents/data-sheet/74HC_HCT138.pdf (дата звернення: 15.06.2026).

19. 74LS138 Принцип роботи декодера, сценарії застосування та 7AHC138 проти 74LS138. *Ariat Technology Limited*. 16.04.2024. URL: <https://ua.ariat-tech.com/blog/74ls138-decoder-working-principle,application-scenarios-and-7ahc138-vs-74ls138.html>.

20. 7400 Series Guide: 74HC138/74LS138 (3-to-8 line decoder). *Build Electroni Circuits*. URL: <https://www.build-electronic-circuits.com/7400-series-integrated-circuits/74hc138-74ls138/> (дата звернення: 15.06.2026).

21. Дешифратор SN74HC138N DIP16. *Интернет-магазин "МікроАмпер"*. URL: https://uamper.com/Дешифратор-декодер-двоичный--SN74HC138N-DIP16-3-line-to-8-line?srsltid=AfmBOooucYz4oB9Ikj7mxKphcNHugoXpAz7RngLor0JyfgW7_W95dUw7 (дата звернення: 15.06.2026).

22. DM74LS245 3-STATE Octal Bus Transceiver. *Fairchild Semiconductor Corporation*. URL: <https://www.futurlec.com/Datasheet/74ls/74LS245.pdf> (дата звернення: 15.06.2026).

23. 7400 Series Guide: 74HC245/74LS245 (Octal Bus Transceiver). *Build Electroni Circuits*. URL: <https://www.build-electronic-circuits.com/7400-series-integrated-circuits/74hc245-74ls245/> (дата звернення: 15.06.2026).

24. 5mw 940nm Module Diode IR Infrared Dot Laser Sight. *Alibaba*. URL: https://www.alibaba.com/product-detail/5mw-940nm-Module-Diode-IR-Infrared_62130067922.html (дата звернення: 17.06.2026).

25. Світлодіод (фотодіод) F5 інфрачервоний IR 940нм. Мій проєкт. URL: <https://myproject.com.ua/svitlodiod-f5-infrachervonij-ir-940nm-ua.html> (дата звернення: 17.06.2026).

26. Overview of the Arduino IDE 1. *Arduino. Software tools*. 17.01.2024. URL: <https://docs.arduino.cc/software/ide-v1/tutorials/Environment/>.

27. Bring Your Projects to Life with Arduino Software. *Arduino. Software*. URL: <https://www.arduino.cc/en/software/> (дата звернення: 22.05.2026).

28. García A. Arduino IDE. The official app for Arduino programming. Uptodown. URL: <https://arduino-ide.en.uptodown.com/windows> (дата звернення: 22.05.2026).

29. SimulIDE Circuit Simulator. *SimulIDE*. URL: <https://simulide.com/p/> (дата звернення: 22.05.2026).

30. Чеботарьова Д.В., Малінін А.П., Перістий В.М. Розробка модуля системи захисту від FPV-дронів. *Матеріали 30-го Міжнародного молодіжного форуму "Радіoeлектроніка і молодь у XXI столітті", Харків, Україна, 22 – 24 квіт. 2026*. Харків: ХНУРЕ, 2026. Т.4: Конференція "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій". С. 139 – 140.