НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Приладобудівний факультет
Кафедра автоматизації та систем неруйнівного контролю

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Юрій КИРИЧУК
«___»_____2024 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою
«Комп'ютерно-інтегровані системи та технології в приладобудуванні»
зі спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»
на тему: «Система охоронної сигналізації офісного приміщення»

Виконав:
студент II курсу, групи ПМ-31мп
Півень Назар Олександрович _____

Науковий керівник:
Доцент, кандидат технічний наук
Богдан Галина Анатоліївна _____

Консультант з розробка стартап-проектів:
Завідувач кафедри економічної кібернетики,
Доктор економічних наук, професор
Бояринова Катерина Олександрівна _____

Рецензент:
Доцент, кандидат технічний наук
Козир Олег Васильович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Приладобудівний факультет
Кафедра автоматизації та систем неруйнівного контролю

Рівень вищої освіти – другий (магістерський)
Спеціальність – 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»
Освітньо-професійна програма «Комп’ютерно-інтегровані системи та технології в приладобудуванні»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Юрій КИРИЧУК

«___»_____2024 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Півню Назару Олександровичу

1. Тема дисертації «Система охоронної сигналізації офісного приміщення» науковий керівник дисертації доцент, кандидат технічний наук кафедри АСНК Богдан Галина Анатоліївна, затверджені наказом по університету від «07»11. 2024 р. №_4987-с

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження: процес забезпечення безпеки офісного приміщення.

4. Вихідні дані: предмет дослідження – система охоронної сигналізації офісного приміщення.
5. Перелік завдань, які потрібно зробити: проаналізувати існуючі вимоги до параметрів безпеки офісних приміщень; Провести огляд і порівняння аналогів систем охоронної сигналізації, що використовуються для захисту офісів; озробити структурну схему автоматизованої охоронної системи; Здійснити підбір елементної бази для системи, включаючи датчики, модулі керування та засоби сповіщення; Розробити алгоритми виявлення загроз, обробки сигналів та передачі повідомлень; Створити макет системи охоронної сигналізації для офісного приміщення.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: 5 плакатів

7. Орієнтовний перелік публікацій:

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розробка стартап-проектів	Завідувач кафедри економічної кібернетики, Доктор економічних наук, професор Бояринова Катерина Олександрівна		

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Формулювання завдання магістерської дисертації	02.09.2024	Виконано
2	Аналітичний огляд існуючих систем охорони	20.09.2024	Виконано
3	Розроблення структурної схеми системи	01.10.2024	Виконано
4	Вибір елементної бази	15.10.2024	Виконано
5	Розробка алгоритмів обробки та передачі даних	02.11.2024	Виконано
6	Розробка макету автоматизованої системи	10.11.2024	Виконано
7	Розробка стартап-проекту	20.11.2024	Виконано
8	Формулювання висновків та оформлення пояснювальної записки та презентації	25.11.2024	Виконано

Студент Назар ПІВЕНЬ

Науковий керівник Галина БОГДАН

РЕФЕРАТ

Актуальність теми

Сьогодні проблема забезпечення безпеки офісних приміщень від несанкціонованого доступу набуває все більшої актуальності. Використання сучасного обладнання та цінної інформації в офісах вимагає створення надійної охоронної системи, здатної попереджати загрози та оперативно реагувати на надзвичайні ситуації.

Розвиток цифрових технологій та інтеграція IoT рішень відкривають нові можливості для вдосконалення охоронних систем. Це дозволяє знижувати їхню собівартість, розширювати функціонал, підвищувати точність роботи та швидкість реагування.

У цій роботі розроблено систему охоронної сигналізації для офісних приміщень, що базується на платформі Arduino UNO та сучасних датчиках, включаючи інфрачервоні, магнітні, ультразвукові та інші типи сенсорів. Система забезпечує моніторинг і захист приміщень у режимі реального часу та дозволяє відстежувати інформацію через веб-інтерфейс.

Запропоноване рішення також підтримує підключення додаткових модулів, наприклад, датчиків диму, полум’я або розбиття скла, що розширює функціональні можливості системи. Система автоматично реєструє події, передає дані на сервер для зберігання та аналізу, а також інформує власника про будь-які порушення через мобільний додаток або повідомлення.

Розроблена система орієнтована на безперебійну цілодобову роботу, здатна попереджати про надзвичайні ситуації та оперативно реагувати на них.

Мета і задачі дослідження

Метою дослідження є розробка автоматизованої системи охоронної сигналізації, яка забезпечить комплексний захист офісних приміщень, використовуючи сучасні технології для моніторингу та реагування на спроби несанкціонованого доступу.

Для досягнення цієї мети вирішено такі **завдання:**

1. Аналіз вимог до охоронних систем для офісних приміщень.
2. Огляд існуючих аналогів охоронних систем.
3. Розробка структурної схеми охоронної системи.
4. Створення прототипу системи на основі Arduino UNO.
5. Оптимізація алгоритмів обробки та передачі даних.
6. Розробка веб-інтерфейсу для моніторингу та керування системою.
7. Оцінка економічної доцільності розробленого рішення.

Об'єкт дослідження — процес забезпечення безпеки офісних приміщень.

Предмет дослідження — автоматизована система охоронної сигналізації для офісів.

Методи дослідження: Для вирішення завдань використовувалися методи моделювання, програмування, автоматизованого контролю, а також інструменти математичної статистики для аналізу та обробки результатів.

Наукова новизна

1) Вдосконалено підхід до створення охоронних систем шляхом використання інтегрованих рішень для моніторингу, обробки та збереження даних.

Практичне значення

1) Реалізовано автоматизовану систему охорони офісних приміщень, що поєднує гнучкість налаштувань із високим рівнем захисту.

Ключові слова

Охоронна сигналізація, офісне приміщення, Arduino UNO, мікропроцесорна система, безпека.

ABSTRACT

Relevance of the topic

Today, the problem of ensuring the security of office premises from unauthorized access is becoming increasingly important. The use of modern equipment and valuable information in offices requires the creation of a reliable security system capable of preventing threats and responding quickly to emergencies.

The development of digital technologies and the integration of IoT solutions open up new opportunities for improving security systems. This allows them to reduce their cost, expand their functionality, and increase their accuracy and response speed.

In this paper, we have developed a security alarm system for office premises based on the Arduino UNO platform and modern sensors, including infrared, magnetic, ultrasonic, and other types of sensors. The system provides real-time monitoring and protection of premises and allows tracking information via a web interface.

The proposed solution also supports the connection of additional modules, such as smoke, flame, or glass break detectors, which extends the system's functionality. The system automatically registers events, transmits data to the server for storage and analysis, and informs the owner of any violations via a mobile application or notification.

The developed system is focused on uninterrupted round-the-clock operation, capable of warning of emergencies and responding promptly to them.

Research goal and objectives

The aim of the study is to develop an automated security alarm system that will provide comprehensive protection of office premises using modern technologies to monitor and respond to unauthorized access attempts.

To achieve this goal, the following tasks were solved:

1. Analysis of requirements for security systems for office premises.

2. Review of existing analogues of security systems.

3. Development of a structural diagram of the security system.

4. Creating a prototype system based on Arduino UNO.

5. Optimization of data processing and transmission algorithms.

6. Development of a web interface for monitoring and controlling the system.

7. Evaluation of the economic feasibility of the developed solution.

The object of research is the process of ensuring the security of office premises.

Subject of research - an automated security alarm system for offices.

Research methods: To solve the problems, we used the methods of modeling, programming, automated control, as well as mathematical statistics tools for analyzing and processing the results.

Scientific novelty

1) An improved approach to the creation of security systems through the use of integrated solutions for monitoring, processing and storing data.

Practical significance

1) An automated office security system has been implemented that combines flexibility of settings with a high level of protection.

Keywords

burglar alarm, office premises, Arduino UNO, microprocessor system, security.

Зміст

СПИСОК СКОРОЧЕНЬ

IoT – Internet of Things;

DTMF – Dual-Tone Multi-Frequency;

АТС – автоматичні телефонні станції;

АЦП – аналого-цифровий перетворювач;

БЖ – блок живлення;

БК – блок керування;

КС – комп’ютерна система;

МК – мікроконтролер;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СОС – система охоронної сигналізації;

ШІМ – широтно-імпульсна модуляція.

ВСТУП

З кожним роком проблема захисту житла від незаконного проникнення та крадіжок залишається однією з найважливіших для правоохоронних органів. За даними статистики, протягом одного року в Україні було зафіксовано 10 470 випадків квартирних крадіжок, більшість із яких залишилися нерозкритими [1].

Одним із найбільш ефективних способів запобігання несанкціонованому доступу до приміщень є встановлення системи охоронної сигналізації. Така система забезпечує надійний захист об'єктів, що перебувають під охороною, та дозволяє підтримувати високий рівень безпеки.

Головна функція охоронної сигналізації полягає в швидкому й надійному інформуванні правоохоронців та власників про спробу незаконного проникнення. Для досягнення цієї мети важливо вибрати якісні технічні засоби й ефективні методи передачі даних.

Охоронна сигналізація із сиреною може відлякати зловмисників і повідомити сусідів про спробу вторгнення. Однак найвищу ефективність система демонструє, якщо підключена до центрального пульта спостереження охоронної служби.

Хоча на ринку вже існує чимало компаній, що пропонують системи сигналізації, їхня ціна залишається досить високою, що робить розробку доступної охоронної системи актуальною.

Метою цієї кваліфікаційної роботи є створення системи охоронної сигналізації для цілодобової охорони офісних приміщень. Вона буде розроблена з використанням мікропроцесорних технологій і сучасної елементної бази.

Для досягнення мети необхідно виконати такі завдання:

– провести огляд і аналіз аналогічних рішень,доступних на ринку;

– створити загальну структурну схему системи офісної охоронної сигналізації;

– розробити електричну схему модуля, який буде керувати роботою

системи;

– описати алгоритми роботи основних програмних функцій і модулів;

– створити програмне забезпечення, що забезпечить коректну роботу системи.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

У цьому розділі кваліфікаційної роботи розглянуто вимоги до системи охоронної сигналізації офісного приміщення. Проведено аналіз аналогічних рішень, доступних на ринку, визначено їхні сильні та слабкі сторони. Також було досліджено можливі підходи до виконання поставлених задач.

1.1 Аналіз вимог до системи побутової охоронної сигналізації

Система охоронної сигналізації (СОС) являє собою комплекс технічних засобів, призначених для захисту від небажаних дій як всередині, так і ззовні приміщення. Під технічною системою безпеки розуміють сукупність обладнання та технологічних рішень, що забезпечують охорону і контроль. Сучасні охоронні системи є високотехнологічними комплексами, що включають відеоспостереження, охоронну та пожежну сигналізацію, системи контролю і управління доступом, а також інше спеціалізоване обладнання, інтегроване в одну систему.

Згідно з технічним завданням, комп’ютерна СОС повинна відповідати таким ключовим вимогам:

– функціонування в реальному часі;

– автоматичне увімкнення сирени та запуск інформування при виявленні спроби несанкціонованого проникнення;

– сповіщення користувача про всі спроби несанкціонованого доступу до приміщення;

– дистанційний моніторинг стану приміщення за допомогою бездротових технологій зв'язку;

– відображення показників датчиків на дисплеї.

Однією з ключових вимог технічного завдання є можливість автоматичного запуску звукового сповіщення при виявленні несанкціонованого проникнення в приміщення. Для реалізації цієї функції система повинна включати

датчики руху, контролю відкриття дверей і розбиття скла. Також у системі має бути передбачений генератор звукових сигналів.

Згідно з вимогами технічного завдання, одним з основних елементів системи є пристрій на базі мікроконтролера, що відповідає за опитування датчиків і загальне управління системою. Вибір конкретної моделі мікроконтролера здійснюється на основі порівняння доступної елементної бази.

Оскільки технічне завдання вимагає можливість дистанційного моніторингу стану приміщення, необхідно вибрати технологію, що забезпечить відправку сповіщень користувачу в режимі віддаленого доступу.

1.2 Аналіз можливих рішень поставленого завдання

Охоронна сигналізація – це система, призначена для захисту об’єктів від небажаних подій і потенційних загроз. Для збору інформації про стан об'єкта використовуються різні типи датчиків, а центральним елементом системи є контрольна панель, яка приймає сигнали від датчиків через інформаційні канали. Датчик – це пристрій, розміщений безпосередньо на об'єкті, що фіксує його стан і перетворює дані у форму, зручну для передачі по вибраному каналу зв’язку. Датчики в системах охоронної сигналізації (СОС) зазвичай вимірюють неелектричні величини, що вимагає високої надійності [2].

До найбільш популярних типів датчиків для охоронних сигналізацій належать [3, 4]:

– інфрачервоні датчики присутності і руху;

– датчики розбиття скла;

– мікрохвильові датчики;

– вібраційні сенсори;

– фотоелектричні сенсори;

– магнітні датчики;

– ультразвукові сенсори.

Охоронна система призначена для виявлення спроб несанкціонованого доступу до захищеної території, подачі сигналу тривоги на пульт охорони та активації виконавчих пристроїв, таких як освітлення або звукова сирена. СОС складається з керуючих модулів, чутливих елементів (датчиків і сенсорів), виконавчих приладів і засобів сповіщення.

Блок керування (БК) є основним елементом СОС і працює на базі мікроконтролера, який виконує усі функції системи. БК можна під’єднати до комп'ютера для обробки і реєстрації сигналів тривоги, аналізу стану датчиків і ефективності роботи системи. Керуючі модулі управляють виконавчими приладами, вмикаючи освітлення, звукову сирену або відправляючи повідомлення на телефон власника приміщення.

Основна мета охоронних систем – попередити власників про спробу вторгнення. СОС поділяються на:

– дротові;

– бездротові;

– комбіновані.

У дротових системах сигнал від датчиків до центрального модуля передається по кабелю, а в бездротових – через радіоканал. Комбіновані системи об’єднують ці два типи, що дозволяє передавати сигнал як через радіоканал, так і через кабель. Раніше дротові системи були більш популярними, оскільки бездротові технології не забезпечували належного рівня безпеки і часто давали збої. Сучасні бездротові рішення значно підвищили свою надійність і стали серйозною альтернативою дротовим, пропонуючи більшу гнучкість, масштабованість і простоту монтажу [2].

Дротові системи частіше застосовуються там, де датчики потребують підключення до зовнішнього джерела живлення. В таких системах використовується топологія «зірка», при якій модуль керування розташований у центрі, а всі інші прилади з’єднуються з ним кабелями. Бездротові системи належать до

новітнього покоління охоронних технологій, забезпечуючи комплексний захист об’єктів без значних зусиль на встановлення, обслуговування та оновлення [5].

СОС включає різноманітні методи і засоби, що забезпечують охорону об'єкта через взаємодію різних компонентів і пристроїв. У межах даної роботи розглядається система побутової охоронної сигналізації, яка складається з мережі інтегрованих електронних пристроїв, що взаємодіють із центральним блоком керування для захисту від зловмисників. Сьогодні такі системи стали звичними, оскільки кількість злочинів, крадіжок та грабежів зросла. Чимало будинків і підприємств піддаються спробам проникнення через вікна чи двері. На рисунку 1.1 показана структура типової СОС та її основні компоненти [6].

Рисунок 1.1 – Структура типової СОС

Статистичні дані свідчать, що наявність охоронної сигналізації в приміщенні найчастіше запобігає спробам несанкціонованого проникнення. Злочинці зазвичай віддають перевагу менш захищеним об'єктам, уникаючи приміщень, обладнаних охоронними системами [6]. Згідно з дослідженнями, навіть базова система сигналізації значно знижує ймовірність спроб проникнення в охоронюваний об'єкт [2].

Сучасна охоронна сигналізація, отримавши сигнал про потенційне проникнення або спробу злому, може активувати дуже гучний звуковий сигнал або

надіслати сповіщення власнику, якщо система передбачає таку функцію. З огляду на зростання рівня злочинності важливо забезпечувати захист будівель і майна за допомогою сучасних охоронних систем, вартість яких залежить від їх конструкції та технологій [6].

Найбільш ефективними є охоронні засоби, що використовують радіоканал для передачі сигналів від датчиків, оскільки сучасні технології можуть значно підвищити захищеність радіоканалу від перешкод і збільшити дальність передачі даних [7].

1.3 Огляд існуючих систем побутової охоронної сигналізації

На українському ринку зараз представлено широкий вибір систем домашньої охоронної сигналізації. Розглянемо коротко основні рішення від провідних виробників, їхні особливості та основні характеристики [2].

1.3.1 Система бездротової сигналізації MAKS PRO

MAKS PRO – це система, розроблена для захисту важливих об'єктів (рис. 1.2). Вона може працювати автономно та підтримує підключення до охоронного пульта. Налаштування і загальне управління системою здійснюється через мобільні пристрої на базі iOS та Android [8].

Важливою особливістю MAKS PRO є режим енергозбереження: при відключенні основного живлення система переходить на живлення від акумулятора. Передача сповіщень відбувається через кілька каналів зв’язку, зокрема GSM/GPRS і Ethernet.

Рисунок 1.2 – Система безпровідної сигналізації MAKS PRO

Система MAKS PRO має можливість масштабування на велику кількість об’єктів, дозволяючи підключення до двохсот різноманітних пристроїв, таких як датчики, пульти, клавіатури, сигналізатори тощо.

1.3.2 Система бездротової сигналізації Kit GSM

Kit GSM – це система бездротової GSM-сигналізації, яка миттєво реагує на проникнення в приміщення, відправляючи сигнал тривоги, здійснюючи голосові дзвінки та надсилаючи SMS-повідомлення на вказані телефонні номери (див. рис. 1.3).

Цю систему виробляє компанія ATIS, і вона дозволяє керувати системою двома способами: через пульт дистанційного керування або за допомогою смартфона [9].

Рисунок 1.3 – Система безпровідної сигналізації Kit GSM

GSM-інтерфейс в цій системі виконує роль основного каналу зв'язку. Для підтримки безперебійної роботи всіх компонентів передбачено вбудований літієвий акумулятор, який активується при відключенні електрики.

Рідкокристалічний екран слугує для взаємодії з користувачем, відображаючи важливу інформацію про стан системи.

1.3.3 Система безпеки Ajax StarterKit

StarterKit – це система безпеки, що базується на охоронній сигналізації і забезпечує захист приміщень від зловмисників, які можуть проникнути через двері та вікна (див. рис. 1.4). Система надсилає тривожні сигнали на пульт охорони та на смартфон власника, використовуючи технології Ethernet і GSM. Керування здійснюється за допомогою мобільного додатку [10].

Рисунок 1.4 – Система безпеки StarterKit від компанії Ajax

Суть роботи цієї системи полягає в регулярному опитуванні чутливих датчиків, які моніторять стан дверей і вікон, а також виявляють рух у приміщенні. Хаб StarterKit відповідає за передачу сигналів тривоги. Базовий комплект системи можна розширити, підключивши додаткові датчики для виявлення затоплення чи пожежі. До StarterKit також можна приєднати відеокамери та різноманітні засоби автоматизації.

1.3.4 Безпровідна охоронна сигналізація Ajax HomeSiren

HomeSiren – це бездротова система охорони для дому, яка забезпечує звукове сповіщення про тривогу у разі активації датчиків. Вона встановлюється

всередині приміщення, щоб відлякати зловмисників або попередити про небезпеку【11】.

У цій системі є можливість регулювати рівень гучності та тривалість звучання сирени при спрацюванні датчика. Якщо потрібно, до сирени можна підключити зовнішній світлодіод, який можна встановити поза приміщенням для моніторингу стану охоронної системи (див. рис. 1.5).

Рисунок 1.5 – Безпровідна кімнатна охоронна
сигналізація HomeSiren від компанії Ajax

Висновки до першого розділу

Таким чином можна зробити висновок, що система охоронної сигналізації, по своїй суті, являє собою комплекс технічних засобів, які призначені для забезпечення захисту об'єктів від небажаних дій. Сучасні системи повинні забезпечити інтеграцію різних технологій, таких як відеоспостереження, контроль доступу та пожежна сигналізація, з можливістю дистанційного моніторингу. Більшість з них активують звукові або світлові сигнали у разі спрацьовування датчиків. Деякі більш вартісні моделі мають можливість надсилати користувачам повідомлення на смартфони.

В залежності від функцій покладених на охорону систему до її складу млжуть входити різноманітні сенсори (інфрачервоних, мікрохвильових,

магнітних тощо). Головним елементом будь-якої системи є мікроконтролер, який сприймає інформацію від датчиків, перетворює її та керує пристроями візуального та звукового поередження. Вибір конкретного мікроконтролера залежить від вимог до функціональності системи, елементної бази та способів передачі сигналів

З цього аналізу випливає, що одним із найперспективніших напрямків у сфері побутової охорони є розробка систем, що використовують технології GSM.

РОЗДІЛ 2 ПРОЕКТНА ЧАСТИНА

2.1 Розробка структури системи охоронної сигналізації офісного приміщення

При створенні системи охоронної сигналізації застосували принцип модульності, за яким розроблена система поділяється на окремі модулі, кожен з яких виконує конкретну функцію. Схематичне зображення загальної структури і функціональних частин побутової охоронної сигналізації представлено на рис. 2.1.

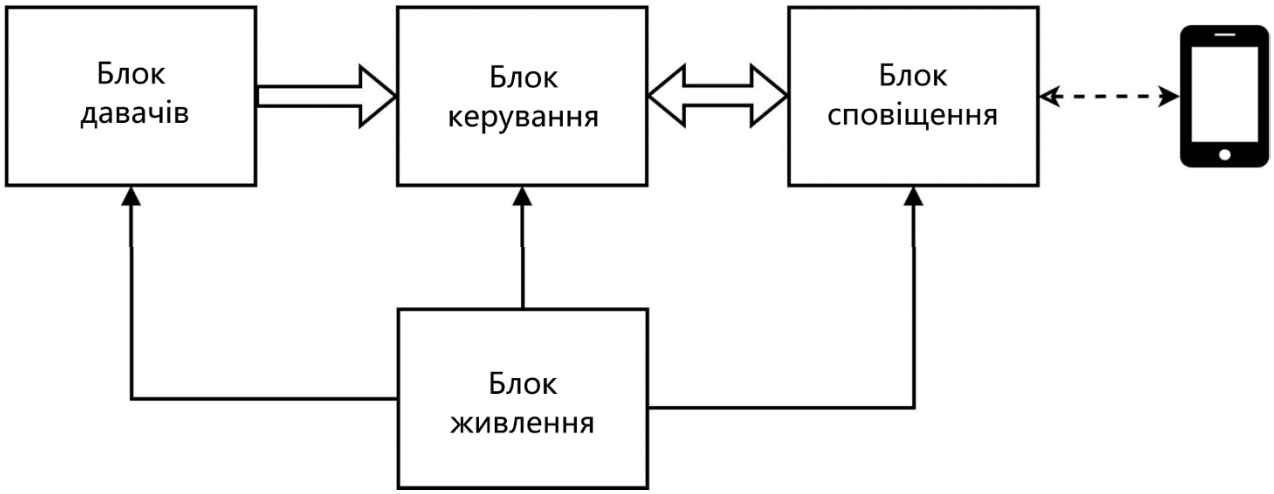

Рисунок 2.1 – Узагальнена структурно-функціональна схема системи побутової охоронної сигналізації

Проєктована система складається з чотирьох блоків:

- блок давачів;
- блок керування;
- блок сповіщення;
- блок живлення.

Оскільки головною метою СОС є моніторинг стану приміщення, виникає потреба в застосуванні давачів. Усі вони згруповані в окремий модуль. Також необхідний модуль обробки даних – блок керування. Для забезпечення автономності роботи потрібна акумуляторна батарея з перетворювачем і системою

підзарядки, що об'єднуються в окремий блок живлення. Для реагування на несанкціоновані дії корисно виділити окремий модуль сповіщення. Подробиці структурної схеми побутової охоронної сигналізації можна побачити на рис. 2.2.

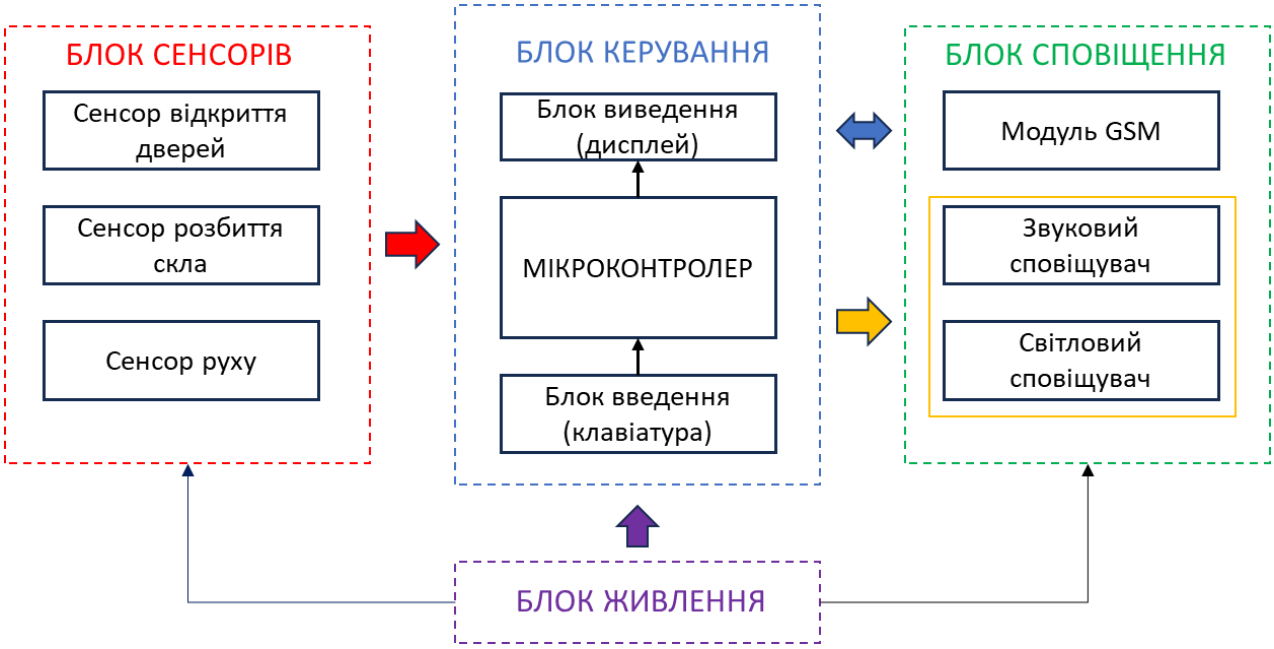

Рисунок 2.2 – Деталізована структурна схема системи побутової охоронної сигналізації

Модуль датчиків розроблений для збору інформації про стан приміщення та її передачі в керуючий блок. До його складу входять такі датчики:

– датчик відкриття дверей;

– датчик розбиття скла;

– інфрачервоний датчик руху.

Цей набір сенсорів дозволяє керуючому модулю отримувати повну інформацію про стан приміщення та спроби несанкціонованого проникнення. Датчики можуть живитися від різних джерел, що забезпечує можливість їхньої установки без необхідності підключення до централізованого блоку живлення. Наприклад, датчик відкриття дверей використовує гальванічні елементи живлення, а деякі моделі взагалі не потребують зовнішньої енергії, працюючи на основі логічних схем.

Інфрачервоний датчик руху здійснює моніторинг активності всередині приміщення. При виявленні об'єкта, що випромінює інфрачервоне тепло, він подає сигнал у блок керування.

Датчик відкриття дверей визначає, чи змінюється положення дверей з закритого стану на відкритий, що є важливим для контролю доступу, адже двері часто слугують головним шляхом проникнення.

Датчик розбиття скла контролює вікна, які можуть бути потенційним місцем проникнення. У разі розбиття скла датчик фіксує характерні акустичні коливання і надсилає відповідний сигнал у керуючий блок.

Таким чином, обрані датчики забезпечують контроль усіх можливих точок входу в приміщення та фіксують переміщення всередині нього.

Керуючий блок містить такі функціональні елементи:

– модуль плати управління на основі мікроконтролера;

– матричну клавіатуру;

–модуль I2C;

– LCD-екран.

Ключовим елементом проєктованої системи є модуль плати управління на основі мікроконтролера, що відповідає за координацію всіх компонентів системи. Матрична клавіатура в парі з LCD-екраном забезпечує користувацький інтерфейс для введення пароля, необхідного для активації та деактивації сигналізації. Ці елементи також дозволяють змінювати пароль пристрою. У проєктованій системі використовується клавіатура з дванадцяти кнопок, розташованих у вигляді матриці 3 х 4, де кнопки розташовані на перетині ліній. Завдяки модулю I2C підключення LCD-дисплея потребує меншої кількості проводів.

Блок сповіщення включає такі елементи: – GSM-модуль; – п'єзодинамік; – світлодіод.

GSM-модуль відповідає за передачу даних на віддалений пункт моніторингу та сповіщення власника через смартфон. П’єзодинамік забезпечує

звукове оповіщення при спрацьовуванні сигналізації, а світлодіод сигналізує про стан тривоги світловим індикатором.

2.2 Обґрунтування вибору апаратного забезпеченнясистеми побутової охоронної сигналізації

2.2.1 Модуль плати управління на основі мікроконтролера

Основним модулем для керування роботою проєктованої системи обрано плату Arduino UNO. Це рішення обґрунтоване її доступною ціною та наявністю широкого асортименту додаткових модулів і програмних бібліотек для зручного налаштування. Зовнішній вигляд цієї плати показано на рис. 2.3.

Рисунок 2.3 – Зовнішній вигляд модуля Arduino UNO

Arduino Uno R3 побудована на базі мікроконтролера ATMega328P-PU [21]. Основні технічні характеристики:

Мікроконтролер	ATmega328
робоча напруга	5 В
Вхідна напруга (рекомендована)	7-12 В
Вхідна напруга (гранична)	6-20 В

Цифрові входи/виходи	14 (6 з яких можуть використову ватися як виходи ШІМ)
Аналогові входи	6
Постійний струм через вхід/вихід	40 мА
Постійний струм для виведення 3.3	50 мА
Флеш пам `ять	32 Кб (ATmega328) з яких 0.5 Кб використовуються для завантажувача
ОЗУ	2 Кб (ATmega328)
Енергонезалежна пам'ять	1 Кб (ATmega328)
Тактова частота	16 МГц

Arduino Uno оснащена 8-бітним мікроконтролером ATMEGA328P, розпіновка виводів наведено на рис. 2.4.

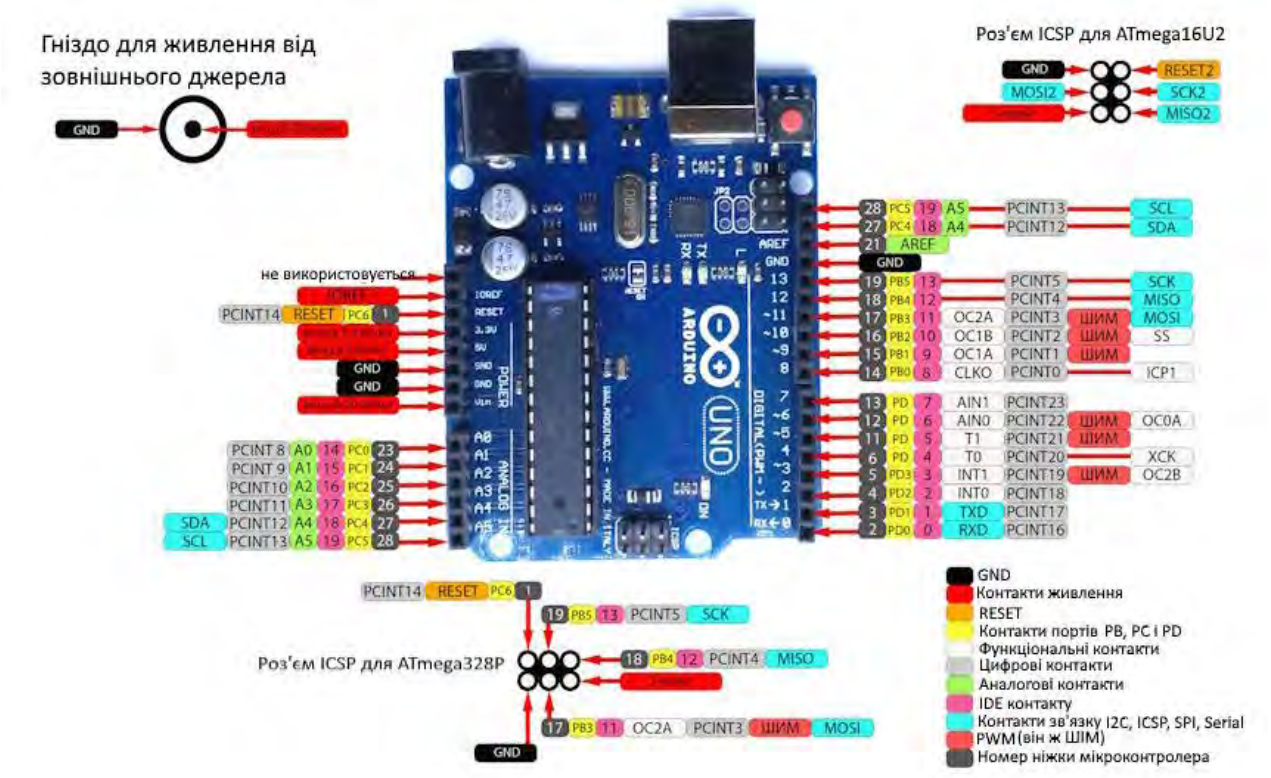

Рисунок 2.4 – Позначення виводів контролера ATmega328P

Arduino UNO складається з мікроконтролера ATmega328P як головного процесора, мікроконтролера ATmega16U2 для зв'язку з ПК через порт USB, USB роз'єму для завантаження програм, ICSP роз'ємів для прошивки ATmega16U2 і ATmega328P, шини живлення, шин цифрових та аналогових входів, кнопки RESET, світлодіодів живлення, передачі даних UART (RX, TX) та світлодіода, підключеного до контакту 13 плати [22] (рис. 2.5).

Рисунок 2.5 Мікроконтролер ATmega328P

ATmega328 - 8-розрядний мікроконтролер, має три типи пам'яті:

1.Флеш-пам'ять: 32 Кб енергонезалежної пам'яті (зберігання програми).

2.Пам'ять SRAM: 2 Кб енергозалежної пам'яті (зберігання змінних даних).

3.Пам'ять EEPROM: 1 КБ енергонезалежна пам'ять.

З периферії мікроконтролер ATmega328 має:

2х 8-бітний таймер/лічильник зі спеціальним регістром періодів і порівнянням каналів;

1х 16-розрядний таймер/лічильник із спеціальним регістром періоду, записом вхідних даних і каналами порівняння;

1х USART з генератором дробової швидкості передачі даних і визначенням початку кадру;

1х контролер/периферійний послідовний периферійний інтерфейс (SPI);

1х дворежимний контролер/периферійний I2C;

1х аналоговий компаратор (АС) з масштабованим опорним входом;

Сторожовий таймер з окремим вбудованим генератором;

Шість каналів ШІМ;

Переривання та пробудження при зміні PIN-коду.

Плата може живитись через USB або від зовнішнього джерела живлення. При цьому тип джерела вибирається автоматично. Для зовнішнього джерела живлення (без USB) може використовуватися мережевий адаптер в межах від 7 до 12 В.

Мікроконтролер на платі має 14 цифрових виходів і входів, які керуються функціями pinMode(), digitalWrite() і digitalRead(). Рівень напруги на виходах обмежений 5В. Максимальний струм на цифрових виходах становить 40 мА.

2.2.2 Модуль давача руху

Для виявлення небажаних переміщень у проєктованій охоронній системі використовується модуль піроелектричного інфрачервоного датчика руху PIR на основі чутливого елемента HC-SR501. Цей датчик визначає рух людей у своїй зоні покриття, реагуючи на інфрачервоне випромінювання, яке випромінюють живі істоти. Крім того, він може вловлювати інші об'єкти, що виділяють тепло. Вигляд датчика руху представлено на рис. 2.6.

Модуль датчика оснащений лінзою Френеля, яка фокусує інфрачервоне випромінювання на піроелектричний сенсорний елемент. Датчик вважається пасивним, оскільки для виявлення руху йому не потрібна додаткова енергія, окрім тієї, що виділяється самими об’єктами. Чутливий елемент складається з

двох частин. Керуюча мікросхема аналізує зміни сигналів від обох частин і, на основі їх коливань, визначає наявність об’єктів, що випромінюють інфрачервоне тепло. Основні технічні характеристики модуля наведено в таблиці 2.1.

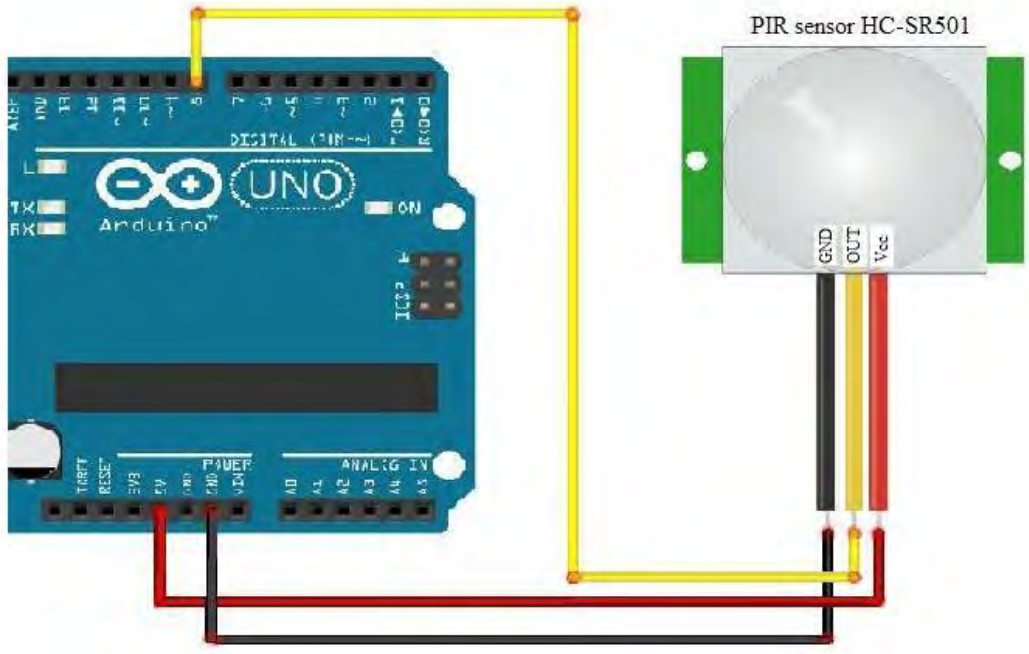

Рисунок 2.6 – Зовнішній вигляд модуля давача руху PIR HC-SR501

Таблиця 2.1 – Технічні параметри давача руху [23]

Параметр	**Значення**
Розміри	приблизно 3.2 см x 2.4 см x 1.8 см
Напруга живлення	4.5 DC V - 20V
Струм на OUT	< 60uA
Напруга на виході	Високі і низькі рівні в 3.3 V TTL логіці
Дистанція виявлення	3 — 7м (настроюється)
Кут виявлення	до 120°-140° (в залежності від конкретного датчика і лінзи)
Тривалість імпульсу при виявленні	5 — 200сек.(настроюється)
Час блокування до наступного виміру	2.5 сек. (але можна змінити заміною SMD-резисторів)
Робоча температура	-20 — +80°C
Режим роботи	L — одиночний захоплення, H — повторювані виміру

Запропонований модуль має компактні розміри, легко використовується,

відзначається високою надійністю та низьким споживанням енергії. Це робить його зручним для пристроїв, що працюють від автономних джерел живлення. Чутливість модуля зменшується з ростом відстані. Важливо уникати впливу теплових джерел і яскравого світла, які можуть освітлювати лінзу модуля.

2.2.3 Давач відкриття дверей

Одним із головних датчиків системи, є сенсор для виявлення відкриття дверей. Було обрано сумістний з платой Arduino UNO герконовий сенсор відкриття дверей МС-38 представлений на рисунку 2.7.

Рисунок 2.7 – Зовнішній вигляд давача відкриття дверей МС-38

Сенсор складається з геркона та магніту, залитих у пластик для герметичності та захисту від пошкоджень [24]. Обидві деталі мають два отвори кріплення і оснащені двостороннім скотчем .Номінальна потужність - 10 Вт; максимальний струм споживання - 500 мА. Герконовий датчик МС-38 спрацьовує на відстані 18 мм з допустимою похибкою 6 мм. Цей датчик має нормальне замикання, що означає, що електричне коло замикається, коли перемикач закривається під впливом магніту. При зачинених дверях, якщо магніт знаходиться в близькості до датчика, його контакти залишаються замкнутими, а при відкритті дверей — розмикаються.

2.2.4 Модуль давача розбиття скла

Для системи охорони було обрано звуковий модуль KY-037 як датчик для виявлення розбиття скла. Цей модуль можна налаштувати на реагування на конкретні звукові сигнали. Зовнішній вигляд датчика KY-037 представлений на рисунку 2.8.

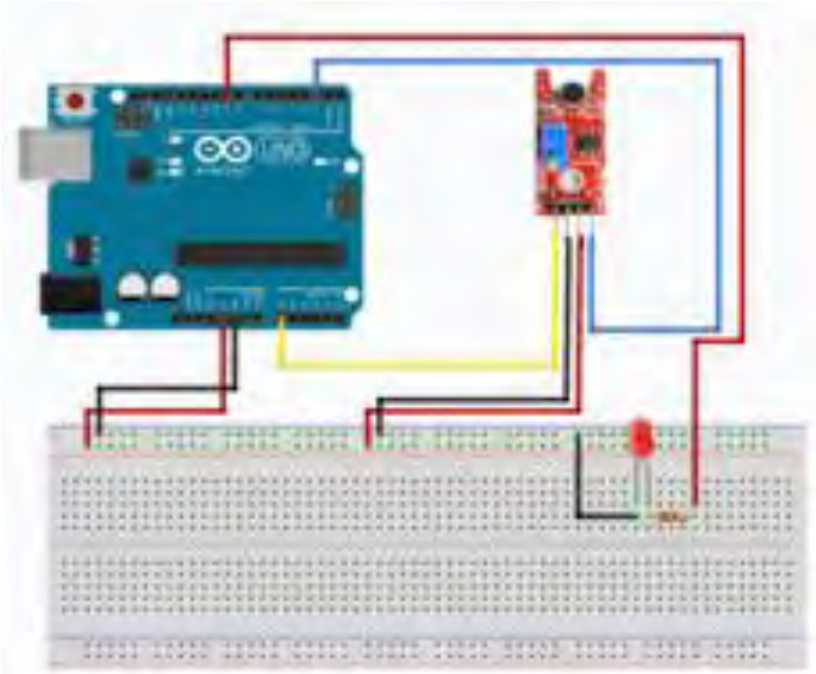

Рисунок 2.8 – Зовнішній вигляд модуля KY-037

Принцип роботи датчика KY-037 заснований на тому, що звукові хвилі викликають коливання мембрани мікрофона. Це, в свою чергу, призводить до зміни ємності конденсатора, що викликає коливання рівня напруги на виходах звукового датчика, відповідно до звукових сигналів. Модуль KY-037 розроблений для виявлення гучних звукових сигналів, зокрема, звуків розбитого скла. Він не реагує на тихі звуки, такі як людська розмова.

Технічні характеристики [25]:

Живлення: 3.5-5.5V

Розмір: 34 x 16 мм

2.2.5 GSM модуль SIM800L

Бездротова передача інформації в охоронній системі реалізовано на базі GSM модуля SIM800L, зовнішній вигляд якого представлений на рисунку 2.10. Даний модуль SIM800L може здійснювати та приймати дзвінки, відправляти SMS, а також підключатися до Інтернету, використовуючи протоколи TCP/IP, GPRS та інші [26]. Окрім цього, модуль підтримує роботу в чотирьох діапазонах мережі GSM. Він збазується на мікросхемі SIM800L, розробленій компанією SimCom.

Рисунок 2.10 – Зовнішній вигляд GSM модуля SIM800L

Модуль SIM800L обладнаний вбудованою антеною, але для покращення якості сигналу можна підключити додаткову зовнішню антену. На нижній стороні плати модуля є роз’єм для SIM-картки. Для зв'язку з мікроконтролером використовується UART-інтерфейс, що дозволяє досягати максимальної швидкості передачі даних до 115200 біт/с.

Характеристики [26]**:**

- Напруга живлення: від 3.4В до 4.4В

- Рекомендована напруга живлення: 4В
- Струм режиму очікування: 0.7 мА
- Максимальний струм: 500 мА
- Максимальна напруга високого рівня інтерфейсу UART: 2.8
- Швидкість UART: 1200-115200 бод
- Робочі діапазони EGSM900, DCS1800, GSM850, PCS1900
- Потужність передачі DCS1800, PCS1900: 1 Вт
- Потужність передачі GSM850, EGSM900: 2 Вт
- Режим мережі: 2G
- Опір динаміка, що підключається: 8 Ом
- Мікрофон: електретний
- Керується командами AT через UART: (3GPP TS 27.007, 27.005 SIMCOM enhanced AT Commands)
- Автоматичне визначення швидкості передачі AT команд
- Надсилання та отримання GPRS даних (TCP/IP, HTTP тощо)
- Макс швидкість передачі даних: 85.6 Кбод
- Кодування: CS-1, CS-2, CS-3 та CS-4
- GSM протокол: 07.10 протокол
- Підтримка пакетної передачі широкомовного каналу управління (PBCCH) CSD на швидкостях 2.4, 4.8, 9.6 та 14.4 Кбод
- Підтримка неструктурованих даних додаткових послуг USSD
- Підтримує PAP (протокол ідентифікації пароля)
- Підтримка годинника реального часу RTC
- Підтримує сімкарти з живленням 3В та 1.8В
- Робоча температура: - 30 до 75 ºС.
- Розміри: 25 х 25 мм

Підключення до послідовного порту мікроконтролера має свої особливості — лінію RXD не можна підключати безпосередньо до GSM модуля, оскільки цифровий вихід мікроконтролера ATmega328 працює на п’ятивольтовій логіці,

тоді як модуль SIM800L функціонує на 3,3 В. Тому доцільно використати схему подільника напруги з двох резисторів номіналом 5 кОм та 10 кОм для зниження рівня напруги. Призначення виводів модуля SIM800L показано на рисунку 2.9.

Максимальний струм споживання модуля може досягати 2 А, що робить неможливим його живлення від мікроконтролера. Він живиться від напруги в діапазоні від 3,3 В до 4,4 В, що дозволяє використовувати стандартну літієву акумуляторну батарею для цих цілей.

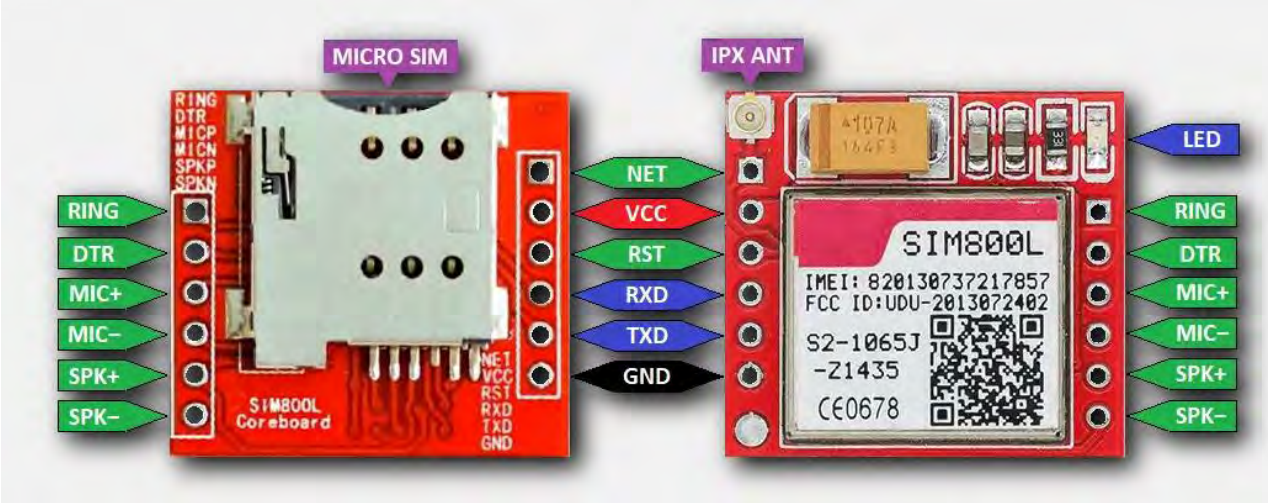

Рисунок 2.9 – Призначення виводів GSM модуля SIM800L

Назви контактів та функції сигналів:

- DTR додатковий сигнал UART
- VCC живлення
- MICP з'єднується з мікрофоном
- RST скидання
- MICN з'єднується з мікрофоном
- RXD до контакту TX мікроконтролера
- SPKP з'єднується з динаміком
- TXD до контакту RX мікроконтролера
- SPKN з'єднується з динаміком
- GND загальний контакт

2.2.6 Модуль контролю заряду-розряду АКБ

У технічному завданні зазначено, що система охоронної сигналізації має бути автономною та живитися від акумуляторної батареї. Тому в розроблюваній системі необхідно передбачити пристрій для заряджання акумулятора. Для цієї мети було обрано модуль на основі мікросхеми TP4056 (рис. 2.11). Процес зарядки акумулятора аналогічний заряджання смартфона. Завершення зарядки відзначається світінням яскравих світлодіодів.

Рисунок 2.11 – Зовнішній вигляд модуля TP4056

Живлення модуля можна подавати через роз’єм microUSB або за допомогою спеціальних контактів, до яких можна приєднати провідники шляхом пайки.

Характеристики [27]**:**

- вхідна напруга: 4.5 - 5.5В
- кінцева напруга зарядки: 4.2В
- напруга захисту розряду: 2.4В
- ток зарядки: 1А
- роз'єм підключення ЗУ: Type-C
- діапазон робочих температур: -10 ° до + 85 °
- Розмір: 27,75x17,25 мм

2.2.7 Модуль п’єзодинаміка

У розроблюваній системі було вирішено використовувати модуль п’єзодинаміка для звукового оповіщення у разі активації датчиків [28]. П’єзоди-

намік перетворює команди, отримані від мікроконтролера, на звукові сигнали. Зовнішній вигляд модуля п’єзодинаміка представлений на рисунку 2.12.

Рисунок 2.12 – Зовнішній вигляд модуля п’єзодинаміка

П’єзодинамік складається з металевої пластини, на поверхні якої нанесено керамічне покриття, здатне проводити електричний струм. Його робота ґрунтується на п’єзоелектричному ефекті, який викликає деформацію матеріалу під час пропускання струму. Внаслідок ударів по металевій пластині виникає звуковий сигнал певної частоти. Для цього в конструкції п’єзодинаміка передбачений генератор звукових частот. Основні характеристики модуля п’єзодинаміка:

- Робоча напруга: 3.3 - 5 В;
- Розмір друкованої плати: 3.3 см x 1.3 см;
- VCC: 3.3-5 В;
- GND: земля;
- Різновид: пасивний;
- I / O: I / O інтерфейс SCM.

2.2.8 Дисплей

LCD-дисплей в системі охорони призначений для відображення стану

датчиків та забезпечення взаємодії з користувачем під час введення пароля при активації або деактивації охорони приміщення. Зовнішній вигляд дисплея зображено на рисунку 2.13.

Рисунок 2.13 – Зовнішній вигляд дисплея

Функціонування цього дисплея забезпечується контролером HD44780 [29], який отримує інформацію від платформи Arduino через I2C-модуль.

LCD дисплей 1602 для Arduino має два ряди по 16 символів у кожному. Працює зі стандартною бібліотекою LiquidCrystal із постачання Arduino IDE.

Технічні характеристики:

- **Розміри**: 80 x 36мм
- **Робоча температура**: 0 ~ 50°C
- **Підсвічування**: зелене
- **Колір символів**: чорний
- **Розмір символу**: 4.35 x 2.95мм
- **Формат**: 16 x 2
- **Розміри точки**: 0.5 x 0.5мм
- **Інтерфейс**: HD44780
- **Видима область**: 64.5 x 13.8мм
- **Живлення**: 5В

2.2.9 Модуль I^2C

Для оптимізації використання виводів мікроконтролера та спрощення передачі даних на LCD-дисплей використовується I^2C -модуль на основі мікросхеми PCF8574T [30]. Зовнішній вигляд I^2C модуля представлено на рисунку 2.14.

Рисунок 2.14 – Зовнішній вигляд модуля I^2C

Вихід SDA підключається до відповідного входу мікроконтролера, тоді як вихід SCL з'єднується з цифровим виводом плати Arduino. Через ці лінії здійснюється передача даних до I2C-модуля, а потім до LCD-дисплея.

Характеристики:

- Інтерфейсна мікросхема: PCF8574AT/T
- Інтерфейс: I2C
- Діапазон адрес I2C:
- PCF8574T - 0x20-0x27
- PCF8574AT - 0x38-0x3f
- Максимальна кількість під'єднаних однотипних модулів: 8
- Напруга живлення: 5 В
- Розмір: 5.2 х 1.8 х 1.4 см
- Сумісність: РКІ 1602 и 2004

2.2.10 Модуль клавіатури

Клавіатура в цій системі використовується для введення коду доступу при деактивації охорони приміщення. Крім того, вона може бути використана для зміни налаштувань системи, наприклад, для оновлення коду доступу. Для цих цілей підходить модуль, що складається з 12 мембранних кнопок, організованих у матрицю 3x4, де кнопки розташовані на перетинах ліній. Зовнішній вигляд дванадцятикнопкової мембранної клавіатури представлено на рис. 2.15.

Рисунок 2.15 – Зовнішній вигляд мембранної клавіатури

Виводи клавіатурного модуля з'єднуються з портом мікроконтролера, з яких три призначені для сканування, а чотири — для перевірки їхнього стану.

2.3 Проєктування електричної принципової схеми системи охоронної сигналізації офісного приміщення

2.3.1 Обґрунтування вибору середовища проектування електричних схем

Для розробки електричної схеми побутової охоронної сигналізації було вибрано програму EasyEDA. Це веб-орієнтоване крос-платформне середовище, яке автоматизує процес проектування електронних схем. Воно складається з таких компонентів:

– редактора для створення електричних принципових схем;

– середовища для розробки електронних компонентів;

– редактора для проектування топології друкованих плат;

– хмарного сховища для зберігання файлів;

– системи управління проектами;

– симулятора;

– інструментів для замовлення виготовлення друкованих плат.

Зовнішній вигляд головного вікна програми EasyEDA, встановленої на ПК, представлено на рисунку 2.16.

EasyEDA працює за клієнт-серверною моделлю. Клієнтська частина програми може функціонувати в браузері, який підтримує HTML5, а файли зберігаються на хмарному сервері. Також існує можливість встановити додаток EasyEDA на комп'ютер, у цьому випадку файли будуть зберігатися на локальному диску з можливістю синхронізації з хмарним сховищем.

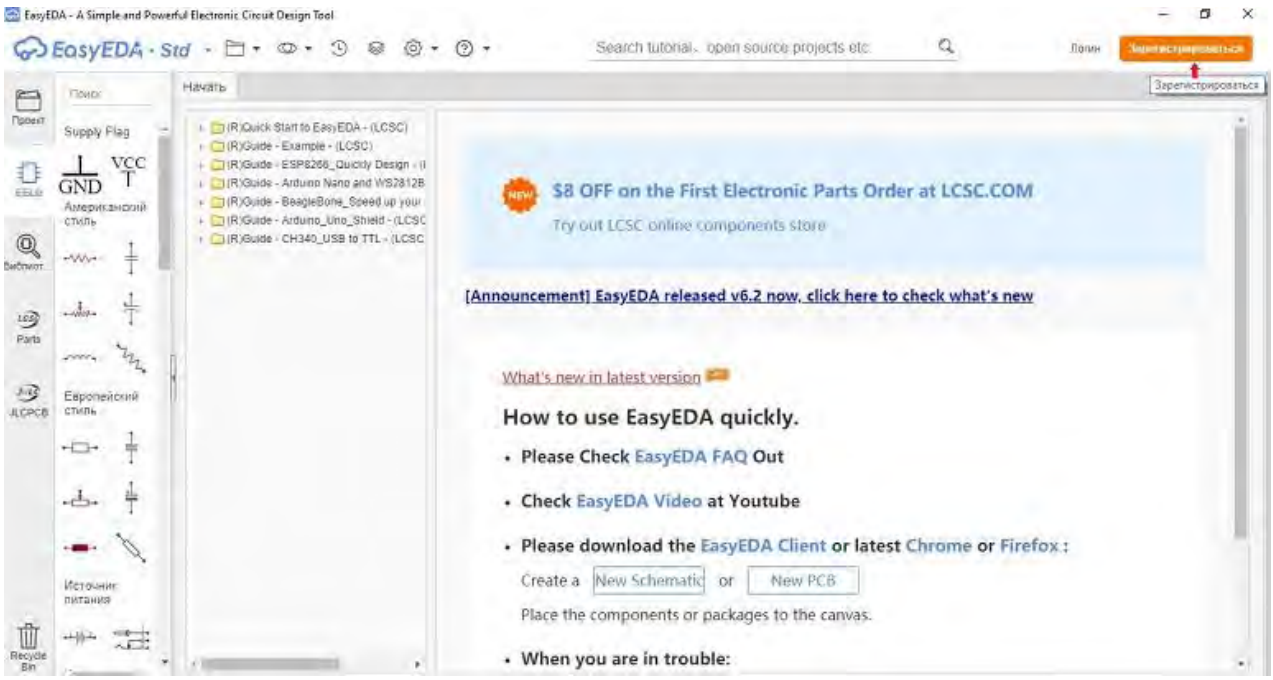

Рисунок 2.16 – Зовнішній вигляд додатку EasyEDA

2.3.2 Розробка електричної схеми пристрою

На рис. 2.17 представлена електрична принципова схема розробленої системи побутової охоронної сигналізації, створена в програмі EasyEDA.

Живлення для цієї схеми може надходити з двох джерел: через роз'єм DC1 від стандартного блоку живлення або від акумуляторної батареї B1 за допомогою модуля контролю заряду-розряду U7. Оскільки GSM-модуль SIM800L працює при напрузі 3,3 В, в схемі включено стабілізатор напруги LM390IT, який позначено як U4.

Виходи датчика руху (U1), датчика відкриття дверей (SW1) і датчика розбиття скла (U2) підключені до цифрових входів плати Arduino UNO, позначеної на схемі як U5. Модуль матричної клавіатури U3 має сім виводів: три з них відповідають за підключення стовпців клавіатури до входів мікроконтролера, а чотири — за підключення рядків.

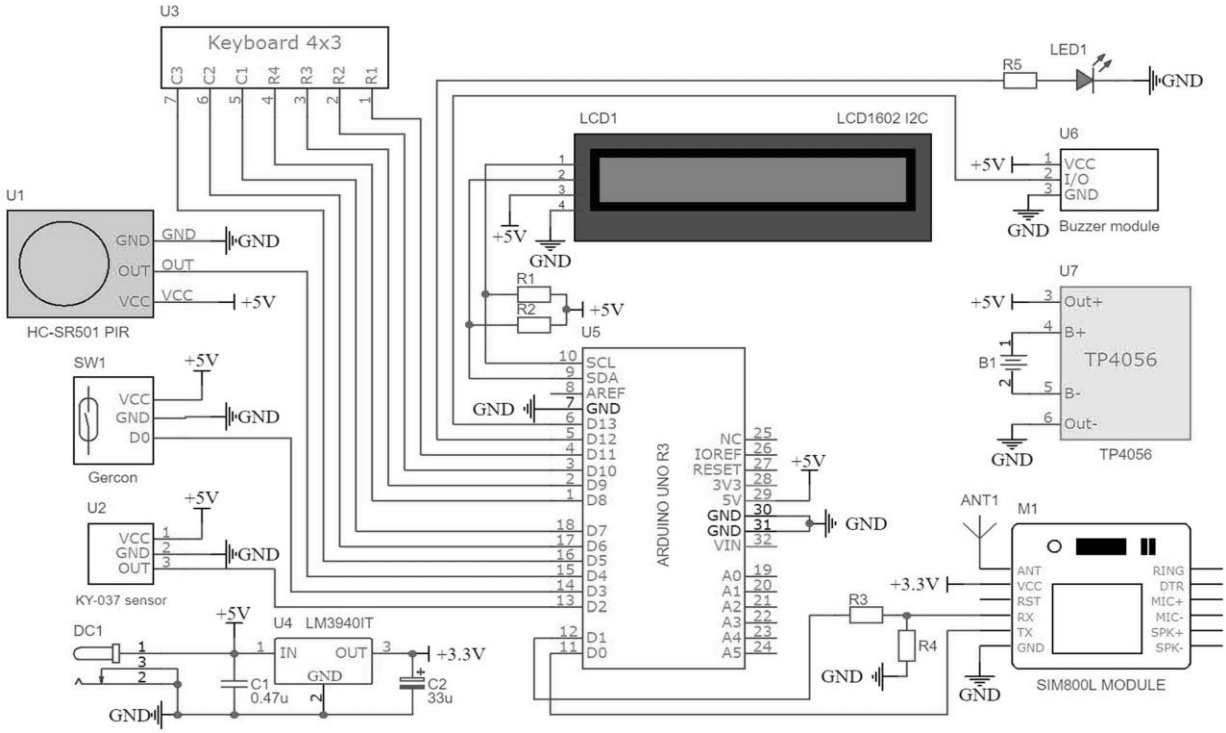

Рисунок 2.17 – Електрична принципова схема системи охоронної сигналізації офісного приміщення

Рідкокристалічний дисплей LCD1, який об’єднаний з I2C-модулем, обмінюється даними з мікроконтролером через лінії SDA та SCL. Резистори R1 та R2 з номіналом 10 кОм використовуються для підтяжки цих ліній до напруги +5 В, що забезпечує коректну роботу I2C-інтерфейсу.

GSM-модуль M1 обмінюється даними з мікроконтролером Arduino через інтерфейс UART. Резистори R3 та R4 формують подільник напруги для узгодження рівнів сигналів між модулями U5 та M1, оскільки у них різні значення живлення. Антена ANT1 підключена до GSM-модуля M1 для підсилення сигналу.

Висновки до другого розділу

В даному розділі було обрано структурну схему автоматизованої охоронної системи офісного приміщення.

На основі структурної схеми визначено та підібрано елементу базу. Наведено опис їх роботи та приведено технічні характеристики.

В якості основного елементу системи обрано модуль Arduino UNO з мікроконтролером ATMega328P-PU. Такий вибір обумовлено відносно низької ціною комплектуючих та простотою збирання та програмування.

Було подібрано сенсори системи (датчик руху, датчик розбиття скла та інші) сумісні з модулем Arduino UNO.

На основі структорної схеми та підібраної елементної бази створено електричну принципову схему у програмному забезпеченні EasyEDA.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Розробка алгоритмів роботи системи охоронної сигналізації офісного приміщення

Функціонування системи охоронної сигналізації (СОС) починається з її активації. Після цього блок керування аналізує сигнальні входи, до яких підключені засоби авторизації та датчики. Мікроконтролер порівнює показники датчиків із пороговими значеннями, що визначають нормальний стан системи. Ці значення задаються під час початкового налаштування перед першим використанням СОС. У разі, якщо стан одного з датчиків змінюється, блок керування негайно розпізнає цю подію та генерує сигнал для активації засобів сповіщення.

Система сповіщення представлена світловими та звуковими сигналами, а також передбачає роботу GSM-модуля, який надсилає повідомлення або здійснює дзвінок власнику приміщення. За необхідності сигнал може бути переданий до відділу охоронної компанії, якщо сигналізація підключена до їхньої мережі.

Щоб зняти приміщення з охорони, користувач вводить відповідний код. Після цього можна зайти в приміщення та змінити режим роботи системи. У такому режимі датчики продовжують працювати, але блок керування ігнорує зміни їхнього стану.

Програмне забезпечення мікроконтролера складається з двох основних частин. Перша частина виконується один раз одразу після подачі живлення на мікроконтролер та здійснює налаштування цифрових виходів і послідовного порту. Друга частина працює циклічно, доки на мікроконтролер подається напруга живлення. Алгоритм роботи СОС зображений на блок-схемах (рис. 3.1 та рис. 3.2).

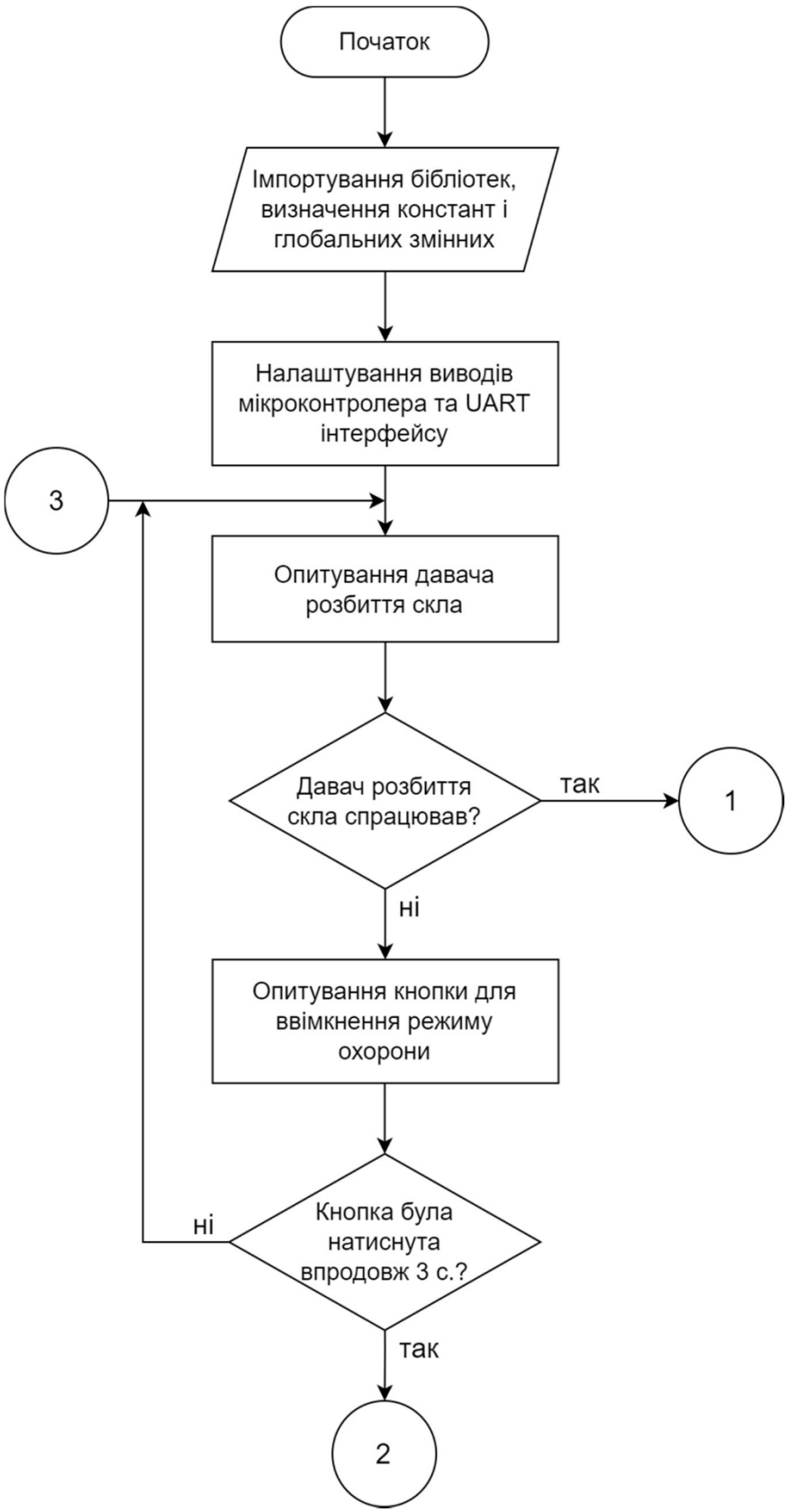

Рисунок 3.1 – Блок-схема алгоритму роботи системи побутової охоронної сигналізації

Рисунок 3.2 – Блок-схема алгоритму роботи системи побутової охоронної сигналізації (продовження)

Програма розпочинається з підключення необхідних бібліотек і налаштування режимів роботи входів і виходів мікроконтролера. Алгоритм роботи

програми базується на декількох перевірках: три з них відповідають за моніторинг та аналіз даних із датчиків, а дві — за контроль стану кнопки та клавіатури.

Щоб забезпечити модульність і зручність, програма розділена на такі функціональні частини:

1. **Модуль опитування вхідних сигналів** — зчитує дані з датчиків та інших вхідних пристроїв.
2. **Модуль зміни станів системи** — визначає режим роботи сигналізації.
3. **Модуль обробки станів** — реагує на зміни, наприклад, активацію сигналів тривоги.

Система охоронної сигналізації (СОС) працює в чотирьох основних режимах:

1. **Очікування** — датчики не активні, і система не реагує на зміни, приміщення використовується у звичному режимі.
2. **Охорона** — усі датчики активовані, система контролює стан приміщення.
3. **Тривога** — при спрацьовуванні датчика руху чи відкриття дверей у користувача є 15 секунд, щоб ввести секретний код.
4. **Спрацювання** — система запускає засоби оповіщення (звукові чи світлові сигнали).

Основний цикл програми починається із зчитування сигналів із підключених датчиків через цифрові та аналогові входи. Зчитані дані записуються у змінні для подальшого аналізу. Серед перевірених даних особливе місце займають показники клавіатури та кнопки, яка відповідає за активацію режиму охорони.

Для переходу в режим "Охорона" необхідно натиснути спеціальну кнопку та утримувати її протягом трьох секунд. Після цього користувачу надається 15 секунд для виходу з приміщення, протягом яких система не реагує на зміни стану датчиків. Це забезпечує можливість безперешкодного виходу без активації сигналізації.

Спочатку система перевіряє стан датчика розбиття скла. Якщо цей датчик передає сигнал про спрацювання, система автоматично переходить у режим «Спрацювання». Далі аналізуються дані від датчиків руху та відкриття дверей. У разі активації будь-якого з них система переходить у режим «Тривога».

Для налагодження роботи програми передбачений спеціальний блок коду, який забезпечує передачу значень змінних через послідовний порт. Це дозволяє в реальному часі відстежувати сигнали від датчиків і зміну режимів роботи системи [38, 39].

Наступний сегмент коду відповідає за управління режимами роботи системи. У залежності від активного режиму виконуються такі дії:

1. **Режим охорони**: засоби сповіщення (п’єзодинамік і світлодіоди) залишаються вимкненими, оскільки система перебуває в стані очікування.
2. **Режим тривоги**: запускається таймер. Якщо протягом заданого часу не буде введено правильний код, система автоматично переключиться в режим «Спрацювання».
3. **Режим спрацювання**: активуються всі засоби сповіщення. На виходи мікроконтролера, підключені до п’єзодинаміка та світлодіодів, подається високий рівень напруги. Крім цього, за допомогою стандартної бібліотеки генерується команда для відправлення SMS-повідомлення із заздалегідь підготовленим текстом, а також здійснюється дзвінок на вказаний номер.

Після завершення виконання цих дій управління передається назад до початку циклу, забезпечуючи безперервний моніторинг стану приміщення.

У наступному розділі буде детально розглянуто програмний код та функції, які реалізують описані алгоритми, а також особливості їх виконання.

3.2 Налаштування середовища для розробки ПЗ

3.2.1 Середовище розробки програмного коду для мікроконтролера

Для написання програм для мікроконтролерів, які використовуються в платформах Arduino, застосовується мова програмування Processing. Вона побудована на основі спрощеного варіанта мов C/C++ і доповнена спеціалізованими бібліотеками, що розширюють її функціональність. Для створення коду було обрано середовище розробки Arduino IDE, яке є кросплатформним додатком, створеним за допомогою мови Java. Інтерфейс основного вікна Arduino IDE представлений на рис. 3.3.

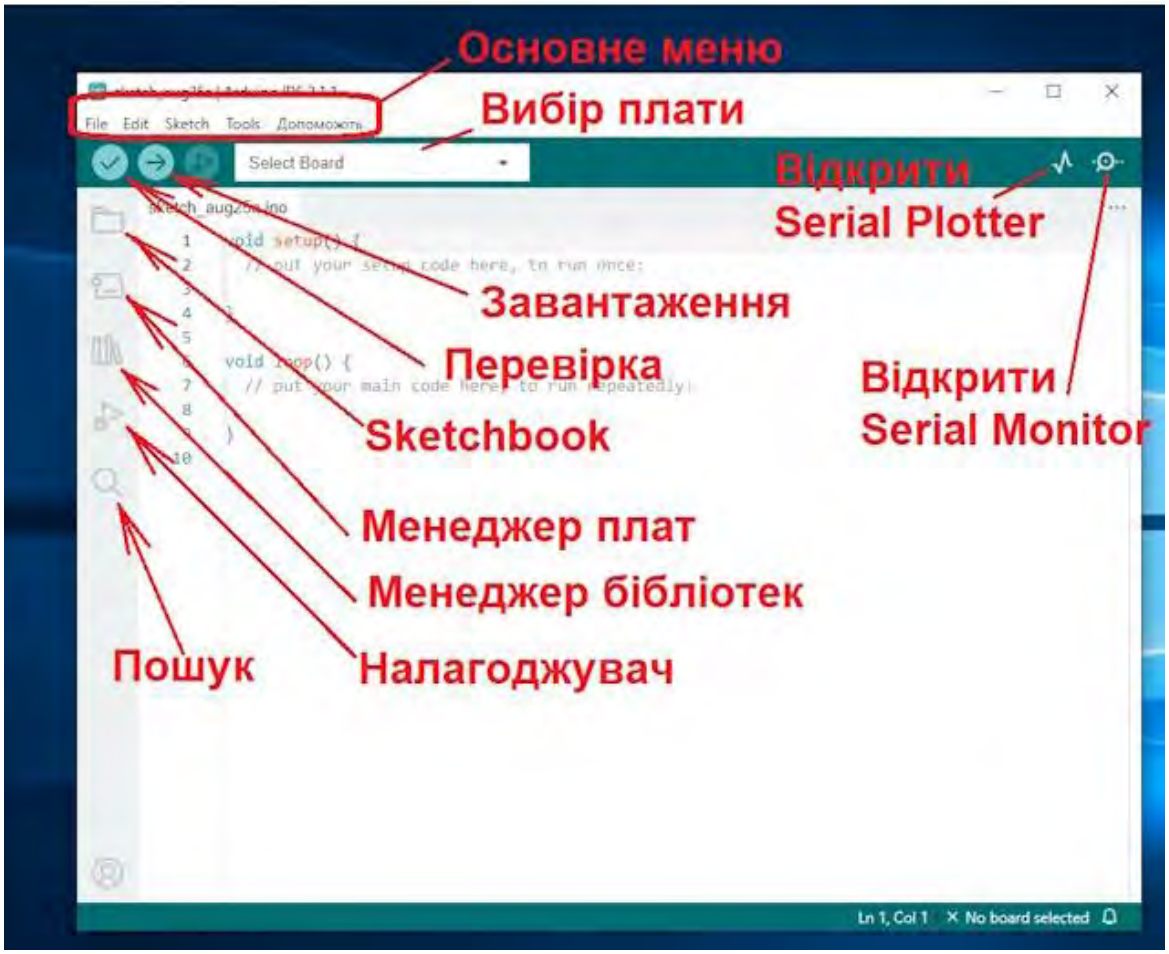

Рисунок 3.3 – Зовнішній вигляд головного вікна додатку Arduino IDE

Програмне середовище Arduino IDE складається з таких основних елементів:

- редактор для написання програмного коду;
- компілятор для перевірки та компіляції коду;
- інструмент для завантаження прошивки в мікроконтролер.

3.2.2 Підключення бібліотеки для роботи з GSM модулем

Щоб забезпечити функціонування GSM-модуля SIM800L у середовищі Arduino IDE, необхідно інтегрувати відповідну бібліотеку. Це здійснюється через меню «Tools», де слід обрати опцію «Manage Libraries». У відкритому вікні «Library Manager» у рядок пошуку «Type» вводиться запит «SIM800L». Після знаходження потрібної бібліотеки натискається кнопка «Install», що дозволяє додати її до середовища розробки. Приклад цього процесу наведено на рис. 3.4.

Рисунок 3.4 – Встановлення бібліотеки для роботи з модулем SIM800L

3.3 Реалізація програмного забезпечення системи охоронної сигналізації офісного приміщення

3.3.1 Код для опитування клавіатури

Для забезпечення взаємодії з клавіатурою на початковому етапі програми були задані константи, які відповідають функціям її кнопок (рис. 3.5).

```
const int Row[] = {11, 10, 9, 8}; // виводи рядків
const int Col[] = {7, 6, 5};      // виводи стовпців
const char k3x4 [3][4] = {        // символи на клавіатурі
  {'1', '2', '3',},
  {'4', '5', '6',},
  {'7', '8', '9',},
  {'*', '0', '#'}
};
```

Рисунок 3.5 – Лістинг коду з визначенням констант для роботи з клавіатурою

У функції setup() за допомогою циклу налаштовано режими роботи виводів мікроконтролера: пінів, підключених до рядків клавіатури, як цифрові виходи з подачею високого рівня напруги, а пінів, які відповідають за стовпці, як цифрові входи з підтягуванням до логічної одиниці (рис. 3.6).

Фрагмент коду надається за звернення до авторів

Рисунок 3.6 – Призначення режиму роботи виводів МК для клавіатури

У функції loop() з інтервалом у 50 мс на виходах рядків циклічно встановлюється низький рівень напруги. У вкладеному циклі здійснюється перевірка стану виводів стовпців. Якщо на якомусь зі стовпців фіксується логічний «0»,

це свідчить про з’єднання рядка i зі стовпцем j, а отже, була натиснута кнопка k3x4(i, j).

3.3.2 Код для виведення інформації на LCD дисплей

Перед початком роботи з LCD-дисплеєм необхідно імпортувати відповідну бібліотеку для його використання та вказати тип і розмір екранного модуля:

```
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x3F,16,2);
```

У функції setup() виконується первинне налаштування LCD-дисплея та виведення стартового повідомлення на його екран (див. рис. 3.7).

Фрагмент коду надається за звернення до авторів

Рисунок 3.7 – Лістинг коду для ініціалізації LCD дисплею

3.3.3 Код для обміну даними з GSM модулем

Оскільки для взаємодії з GSM-модулем застосовується UART-інтерфейс, у програмному коді використовується бібліотека SoftwareSerial.h (див. рис. 3.8).

Фрагмент коду надається за звернення до авторів

Рисунок 3.8 – Лістинг коду для ініціалізації UART інтерфейсу
для обміну даними між мікроконтролером і GSM модулем

У підпрограмі loop() реалізовано обмін даними за допомогою функцій available() та write(), які забезпечують передачу й отримання інформації (рис. 3.9).

Фрагмент коду надається за звернення до авторів

Рисунок 3.9 – Лістинг коду для надсилання та отримання даних по UART інтерфейсу

На рис. 3.10 представлено фрагмент коду, який реалізує функцію відправлення SMS-повідомлення за допомогою GSM-модуля.

Фрагмент коду надається за звернення до авторів

Рисунок 3.10 – Лістинг функції для надсилання sms повідомлення через GSM модуль

3.3.4 Команди DTMF

DTMF-команди використовуються для ініціалізації набору телефонного номера. Вони дозволяють створювати аналоговий сигнал, що складається з двох тонів різної частоти. Цей сигнал широко застосовується для автоматизованої телефонної комутації між пристроями. Зокрема, такі сигнали можуть забезпечувати управління з'єднаннями в аналогових системах, наприклад, між телефонними апаратами та автоматичними телефонними станціями (АТС).

Тональні сигнали також активно використовуються для ручного введення команд користувачами в різних системах, наприклад, у сервісах голосового меню. Їх часто застосовують на телебаченні та радіо для інтерактивної взаємодії з аудиторією. Технологія DTMF знайшла широке застосування і в сферах охоронних сигналізацій та систем "розумного будинку".

У створюваній системі DTMF-команди забезпечують дистанційне управління сигналізацією через модуль SIM800L. Якщо на SIM-карті збережені номери, то їх власники отримують право керувати сигналізацією, зокрема, активувати або деактивувати її. Номер, записаний під іменем ADMIN, наділяється

статусом адміністратора. Якщо в пам’яті SIM-карти немає такого номера, перший користувач, який здійснить дзвінок на нову SIM-карту, автоматично стане адміністратором. У цей момент його номер зберігається в телефонній книзі модуля.

Тільки адміністратор має право надсилати SMS і використовувати DTMF-команди для управління системою. У розроблюваній сигналізації передбачено набір команд, які відображені на рис. 3.11.

Фрагмент коду надається за звернення до авторів

Рисунок 3.11 – Список DTMF команд

GSM-модуль налаштований на автоматичне прийняття дзвінків лише з адміністративного номера, щоб забезпечити можливість використання DTMF-команд. Усі вхідні дзвінки з інших номерів будуть автоматично відхилятися. Передача команд DTMF доступна виключно адміністратору. У разі успішного прийняття команди система завершить виклик, після чого на вказану пошту буде надіслано звіт про виконання.

Для підтвердження завершення введення команди необхідно додатково натиснути будь-яку цифру, а потім символ #. На завершальному етапі модуль завершить телефонний виклик і перейде до виконання отриманої команди.

Висновки до третього розділу

В цьому розділі:

Проведено розробку алгоритмів роботи системи охоронної сигналізації для офісного приміщення.

Розроблено програмний код для керування мікроконтролером та основними структурними елементами системи.

РОЗДІЛ IV. РОЗРОБКА СТАРТАП ПРОЕКТУ
«Система охоронної сигналізації офісного приміщення»

4.1. Опис ідеї проєкту технології

У цьому розділі проведено аналіз стартап-проєкту, мета якого полягає в розробці системи охоронної сигналізації офісного приміщення з метою подальшого автоматизованого регулювання параметрів та цілодобової охорони офісних приміщень.

Для кращого розуміння вимог до реалізації проєкту, його цілей, завдань та орієнтовних термінів була створена інформаційна карта, представлена у вигляді таблиці 4.1 нижче.

Таблиця 4.1

Інформаційна карта

Назва блоку	**Характеристика**
1	**2**
Загальна характеристика стартап-проєкту	
Назва стартап-проєкту	Система охоронної сигналізації офісного приміщення.
Проблематика, яку вирішує стартап проєкт	Стартап «Система охоронної сигналізації офісного приміщення» вирішує проблему безпеки бізнес-приміщень, які часто залишаються без належного захисту від несанкціонованого доступу та крадіжок. У сучасних офісах зберігаються цінні дані та обладнання, які потребують надійного захисту. Відсутність оперативного реагування на загрози лише підвищує ризики для бізнесу. Інноваційна система з датчиками руху, контролем доступу і відеоспостереженням забезпечує автоматизований захист і швидке оповіщення, що мінімізує ризики та створює безпечне середовище для роботи компанії.
Головні цілі та завдання проєкту	1. Мета проєкту «Система охоронної сигналізації для офісного приміщення» – забезпечити автоматизований контроль безпеки для офісів, спрямований на оперативне виявлення загроз та захист майна. Проєкт передбачає створення комплексної системи моніторингу, що включає датчики руху, відеоспостереження та контроль доступу, аби забезпечити надійний захист приміщень та знизити ризики несанкціонованого проникнення, крадіжок і пошкодження майна. 2. Система охоронної сигналізації для офісного приміщення має забезпечити надійний і безперервний моніторинг безпеки офісу, виявляючи будь-які підозрілі дії або загрози. Вона передбачає швидке реагування на аномалії, такі як несанкціонований доступ чи рух у заборонених зонах, що може поставити під загрозу безпеку приміщення та майна.Запобігання аварійним ситуаціям: Система повинна мати можливість надсилати аварійні сигнали та повідомлення в разі виявлення відхилень від установлених нормативів мікроклімату. Це дозволить оперативно реагувати на потенційно небезпечні ситуації та запобігати негативним наслідкам.

	3. Система охоронної сигналізації для офісного приміщення повинна забезпечувати зручний і ефективний моніторинг безпеки через веб-інтерфейс. Це дозволить відповідальним особам оперативно відстежувати ситуацію в офісі, швидко реагувати на потенційні загрози та вносити необхідні корективи для підтримки безпеки приміщень. 4. Система повинна бути розроблена з можливістю простого розширення та оновлення, що дозволить додавати нові типи датчиків та покращувати функціонал веб-інтерфейсу. Така гнучкість дасть змогу адаптувати систему до зростаючих вимог безпеки та впроваджувати новітні технології у сфері охоронних рішень.
Головні цільові групи, на які спрямований проєкт	• Малий та середній бізнес • Великі компанії та корпоративні офіси • Коворкінги та офісні центри • Орендодавці офісних приміщень
Автори та команда стартап-проєкту	
Автори стартап- проєкту	Автори проєкту: Півень Назар, Богдан Галина Анатоліївна
Команда стартап- проєкту	Півень Назар, Богдан Галина Анатоліївна автори проєкту, Інвестори, керівники, працівники-дизайнери, інженери
Опис продукту стартап-проєкту	
Назва та коротка характеристика мінімального життєздатного продукту стартапу (MVP)	"OfficeGuard Secure" — це мінімально життєздатний продукт для забезпечення охорони офісних приміщень. Система оснащена базовим функціоналом для виявлення підозрілих дій, таких як рух чи несанкціонований доступ, та використовує інтегрований підхід для захисту офісного майна. "OfficeGuard Secure" забезпечує основні функції моніторингу безпеки з можливістю дистанційного керування та сповіщення через веб-інтерфейс, що робить її зручною та ефективною для користувачів.
Сфера застосування та функціональне призначення продукту	"OfficeGuard Secure" призначений для використання в офісних приміщеннях, де забезпечення надійного захисту та оперативний контроль доступу є ключовими для збереження майна, конфіденційної інформації та безперебійної роботи бізнес-процесів.
Опис унікальних властивостей продукту стартапу	Унікальні властивості "OfficeGuard Secure" включають його компактність і легкість інтеграції в офісний простір. Система не займає значного місця і не впливає на функціональність робочих зон, забезпечуючи ефективний моніторинг безпеки. Крім того, "OfficeGuard Secure" вирізняється простотою використання та швидким налаштуванням, що дозволяє легко впровадити її в існуючу офісну інфраструктуру без значних витрат і зусиль.
Стадія розробки продукту стартапу	Налагодження серійного виробництва, партнерство з українськими компаніями та потенційне масштабування на міжнародний ринок.
Технічні характеристики	"OfficeGuard Secure" — це компактний пристрій, призначений для встановлення в офісних приміщеннях. Він оснащений датчиками руху, відкриття дверей та шуму, що дозволяють виявляти підозрілу активність. Система базується на вбудованому мікроконтролері ESP32 та використовує датчики останнього покоління, а також модуль Wi-Fi для передачі даних на зовнішній сервер. "OfficeGuard Secure" забезпечує надійний моніторинг безпеки та ефективне управління системою охорони офісного приміщення.
Супровід продукту	У разі виникнення несправностей користувачі можуть скористатися безкоштовним обслуговуванням у технічних сервісах компанії. Додатково доступне планове технічне обслуговування системи охоронної

	сигналізації для перевірки її справності, яке рекомендується проводити кожні півроку.
Забезпечення стартап-проєкту	
Необхідні ресурси	На першому етапі необхідні датчики та плата для збірки модулів, та грошове забезпечення у вигляді 3650000 грн, на витрати виробництва, просування проєкту та маркетинг
Потреба в інвестиціях	На початкових етапах розвитку проєкту «OfficeGuard Secure» доцільно використовувати платформу Kickstarter для залучення фінансової підтримки та привернення уваги до інноваційної системи охоронної сигналізації. Паралельно варто активно працювати над пошуком інвесторів, які зацікавлені у впровадженні сучасних технологій для забезпечення безпеки офісних приміщень.
Інтелектуальна власність	Усі майнові авторські права на дизайн системи, її модулі, зображення, схеми, креслення, а також відео та аудіоматеріали, включаючи літературний і технічний опис, належать авторам стартапу «OfficeGuard Secure».
Результати стартап-проєкту	
Термін реалізації стартап-проєкту	Термін реалізації стартап-проєкту «OfficeGuard Secure» становить 18 місяців і включає розробку перших прототипів системи, тестування, налагодження виробництва та вихід на ринок.
Плановані кількісні показники стартап-проєкту	Плановані кількісні показники стартап-проєкту «OfficeGuard Secure» передбачають запуск серійного виробництва та вихід на ринок України протягом перших 12 місяців. У подальшому розвиток проєкту включає розширення на міжнародний ринок протягом наступних 24 місяців.
Якісні показники стартап-проєкту	Якісні показники стартап-проєкту «OfficeGuard Secure» включають у себе покращення безпеки та ефективності управління охороною в офісних приміщеннях. Цей продукт сприяє забезпеченню надійного захисту від несанкціонованого доступу та інших загроз, а також покращує загальну ефективність управління безпекою офісу. Система охоронної сигналізації своєчасно виявляє небезпеку, попереджає про потенційні ризики і дозволяє швидко реагувати на інциденти, що забезпечує стабільність роботи офісу.
Загальні очікувані результати	Загальні очікувані результати для стартап-проєкту «OfficeGuard Secure» включають виведення продукту на ринок та забезпечення його популярності серед власників офісних приміщень. Мета полягає в покращенні моніторингу та управління безпекою, забезпечуючи стабільний захист від несанкціонованого доступу та інших загроз. Проєкт прагне підвищити ефективність та безпеку в управлінні охороною офісних приміщень.

Із сформованої вище таблиці можна зробити висновок, що процес реалізації стартап-проєкту "OfficeGuard Secure" складатиме приблизно 18 місяців, враховуючи всі етапи від пошуку інвесторів до запуску виробництва та налаштування системи для досягнення оптимального функціонування.

Для формування більш ефективних ідей та прийняття доцільних рішень щодо конструювання модуля було вирішено використати метод формування «морфологічної карти». Саму карту представлено у таблиці 4.2 нижче.

Відповідно до морфологічної карти проєкту "OfficeGuard Secure", оптимальні рішення для безпосередньої розробки модулю визначаються наступним чином:

1. Кількість датчиків: 2 датчики.
2. Тип датчиків: Камери.
3. Механізм фіксації модулю: Зовнішнє кріплення до стелі серверної кімнати.

   Тип інтерфейсу: З'єднання з сервером через мережу Інтернет.

Таблиця 4.2

Морфологічна карта проєкту

Параметри	Проміжні рішення				
	1-ше	2-ше	3-ше	4-ше	5-ше
Кількість датчиків	1 датчик	2 датчики	3 і більше	Інше	Інше
Тип датчиків	Інфрачервоний руху	Камери	Розбиття скла	Інші датчики	Інші датчики
Розташування	Пожежні виходи та аварійні двері	Внутрішні приміщення	Стратегічні точки	Покрівля та підвал	Коридори та хол
Механізм фіксації модулю	Кріплення на стіну	Зовнішнє кріплення до стелі або стіни	Клейка основа на вікно	Поверхневий монтаж	Інші методи монтажу та фіксації
Тип інтерфейсу	Бездротовий (Wi-Fi)	Дротовий	Гібридний	З'єднання з сервером через мережу Інтернет	Інші способи комунікації та взаємодії

Таким чином оптимальним рішенням є використання декількох типів датчиків для підвищення безпеки та забезпечення комфортного розташування модулю. Модуль буде закріплений ззовні до стелі для оптимального контакту з оточуючим середовищем. Також, інтерфейс модулю буде забезпечено через підключення до серверу за допомогою мережі Інтернет.

Для більш ретельного розгортання концепції стартап-проєкту, ми визначилися зі створенням таблиці, в якій визначено сфери застосування та вигоди від використання модулю для кінцевого користувача (див. Таблицю 4.3).

Таблиця 4.3.

Опис ідеї стартап-проєкту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Автоматизований модуль контролю охоронної сигналізації в офісному приміщенні – «OfficeGuard Secure»	Автоматизований моніторинг та контроль охоронних параметрів, таких як доступ та вторгнення, у офісних приміщеннях.	Ефективний контроль та управління системою охоронної сигналізації в офісних приміщеннях.
	Інтеграція з системами вимірювання та аналізу даних безпеки в офісному приміщенні.	Запобігання несанкціонованому доступу та забезпечення стабільної роботи системи охоронної сигналізації в офісному приміщенні.
	Оптимізація процесів обробки даних для підвищення ефективності роботи системи охоронної сигналізації офісного приміщення.	Використання персонально-розробленого ПЗ без використання додаткових програм
	Віддалений моніторинг та керування системою охоронної сигналізації офісного приміщення через інтернет.	Оптимізація системи управління охоронною сигналізацією в офісному приміщенні за допомогою аналізу даних.

Відповідно до таблиці 4.3, система охоронної сигналізації «OfficeGuard Secure» є інноваційним модулем для автоматизованого контролю безпеки в офісних приміщеннях. Цей модуль інтегрований в офісні зони та призначений для автоматизованого моніторингу та управління параметрами охоронної сигналізації, такими як доступ та вторгнення. Його інтеграція з системами аналізу даних дозволяє ефективно управляти безпекою офісних приміщень. Модуль забезпечує оптимізацію процесів обробки даних, використовуючи спеціалізоване програмне забезпечення без необхідності встановлення додаткових програм. Крім того, віддалений моніторинг та керування системою охорони через Інтернет дозволяє оптимізувати управління безпекою за допомогою аналізу зібраних даних.

Розглянемо основних конкурентів, які представлені на ринку систем охоронної сигналізації для офісних приміщень:

1. **SafeGuard Solutions**
2. **SecureTech**

3. **ProtecSys**

Для більш детального аналізу техніко-економічних властивостей та переваг конкурентів було проведено порівняльний аналіз показників, що наведено в таблиці 4.4 нижче, де W позначають гірші значення, N – аналогічні або нейтральні значення, а S – кращі показники.

Із таблиці, що представлена вище, можна визначити сильні, слабкі та нейтральні характеристики системи охоронної сигналізації «OfficeGuard Secure» порівняно з конкурентами (SafeGuard Solutions, SecureTech, ProtecSys), зробити такі висновки:

1. **Швидкий зворотний зв'язок**: Усі компанії мають наявний швидкий зворотний зв'язок, що підкреслює стандартний рівень обслуговування.

2. **Інтеграція з іншими системами безпеки**: Проєкт «OfficeGuard Secure» вирізняється наявністю інтеграції з іншими системами безпеки, що дає йому перевагу перед конкурентами.

3. **Здатність до апгрейду**: «OfficeGuard Secure» та ProtecSys мають можливість апгрейду, що створює можливості для розширення функціоналу з часом.

4. **Вебсайт для моніторингу**: У «OfficeGuard Secure» є вебсайт для моніторингу, що робить його конкурентоспроможним, адже інші конкуренти не пропонують цю можливість.

5. **Легкість у використанні**: «OfficeGuard Secure» є зручним у використанні, що робить його привабливим для користувачів.

6. **Легкість монтажу**: «OfficeGuard Secure» має простий процес монтажу, що сприяє зручності впровадження.

7. **Наявність персонального кабінету**: «OfficeGuard Secure» та ProtecSys мають персональний кабінет, що забезпечує зручне управління системою.

8. **Ціна обслуговування та компонентів**: «OfficeGuard Secure» має конкурентну перевагу завдяки низькій ціні обслуговування та компонентів.

Таблиця 4.4.

Визначення сильних, слабких та нейтральних характеристик ідеї проєкту

№ п/п		(потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона	S (сильна сторона)
		Мій Проєкт	Конкурент1 **SafeGuard Solutions**	Конкурент2 **SecureTech**	Конкурент3 **ProtecSys**			
1.	Швидкий зворотній зв'язок	Наявний	Наявний	Наявний	Наявний	-	+	-
2.	Інтеграція з системами вимірювання та аналізу даних безпеки в офісному приміщенні.	Наявна	Відсутня	Відсутня	Відсутня	-	-	+
3.	Здатність до апргрейду	Наявна	Відсутня	Відсутня	Наявна	-	+	-
4	Вебсайт з моніторингом	Наявний	Відсутній	Відсутній	Відсутній		-	-
5	Легкість у використанні	Наявна	Наявна	Відсутня	Відсутня		-	+
6.	Легкий монтаж	Наявний	Відсутнє	Відсутнє	Відсутнє		-	-
7.	Наявність персонального кабінету	Наявне	Відсутнє	Відсутнє	Наявне		-	+
8	Ціна обслуговування і модулів	Низька	Висока	Висока	Висока		-	-

Із врахуванням вищезазначених факторів, можна стверджувати, що «OfficeGuard Secure» є конкурентоспроможним проєктом на ринку автоматизованих систем контролю мікроклімату.

Для того, щоб оцінити можливість реалізації проєкту, проведемо технологічний аудит сформованої ідеї (табл. 4.5).

Таблиця 4.5.

Технологічна здійсненність ідеї проєкту

№ п/п	Ідея проєкту	Технології її реалізації	Наявність технологій	Доступність технологій
1.	Автоматизований модуль контролю системи охоронної сигналізації в офісному приміщенні	Використання мікроконтролера ESP32 для програмування модуля	Наявні	У відкритому доступі

2.	Система вимірювання та аналізу даних безпеки в офісному приміщенні.	Інтеграція з датчиками руху та відкриття дверей, використання платформи Arduino для управління системою охоронної сигналізації в офісному приміщенні.	Наявні	Доступно
3.	Оптимізація обчислень	Використання персонально-розробленого програмного забезпечення без використання додаткових програм	Наявні	У відкритому достуі
4.	Віддалений моніторинг та керування системою охоронної сигналізації в офісному приміщенні.	Використання мережі Інтернет для віддаленого з'єднання та керування	Наявні	Доступно
5.	Інтеграція з існуючими системами	Сумісність з системами вимірювання та аналізу даних безпеки в офісному приміщенні.	Наявні	Доступно
6.	Зручне розташування модулю	Інтеграція модулю в систему «OfficeGuard Secure»	Наявні	Доступно
Обрана технологія реалізації ідеї проєкту: можлива для реалізації				

Виходячи з наведеної вище таблиці можна зробити висновок, що реалізація проєкту "OfficeGuard Secure" є технологічно здійсненною. Всі необхідні технології, використані для створення автоматизованої системи охоронної сигналізації в офісних приміщеннях, є доступними для використання. Мікроконтролери ESP32, як основний елемент проєкту, доступні для закупівлі за доступними цінами, а програмне забезпечення, розроблене на платформі Arduino IDE, є відкритим для користувачів, що забезпечує доступність для широкого кола розробників.

4.2. Аналіз ринкових можливостей запуску стартап-проєкту

Оцінимо основні перспективи впровадження нашого проєкту на ринок, а також визначимо потенційні загрози, які можуть виникнути під час його реалізації. Цей аналіз спрямований на успішний запуск проєкту на українському ринку з подальшою можливістю розширення на міжнародний рівень. Розпочнемо з детального вивчення попиту на нашу продукцію, оцінюючи його обсяг, динаміку розвитку та загальну доступність.

Для початку проведемо аналіз попиту на цю продукцію, зокрема це: наявність попиту, обсяг та динаміка розвитку ринку (табл. 4.6).

Таблиця 4.6

Попередня характеристика потенційного ринку стартап-проєкту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	3
2	Загальний обсяг продаж, грн/ум.од	5 000 000
3	Динаміка ринку (якісна оцінка)	Стабільний ріст
4	Наявність обмежень для входу (вказати характер обмежень)	Висока конкуренція, інтелектуальна власність
5	Специфічні вимоги до стандартизації та сертифікації	Необхідна сертифікація відповідно до стандартів безпеки та ефективності
6	Середня норма рентабельності в галузі (або по ринку), %	12,8 %

Відповідно до попередньої характеристики, зокрема до середньої норми рентабельності в галузі, яка становить 12.8%, можна визначити, що ринок систем охоронної сигналізації для офісних приміщень є перспективним. Основна перевага полягає в тому, що основні постачальники охоронних систем в Україні часто є іноземними виробниками, що створює можливість для вітчизняних стартапів у цій галузі. Запуск власного проєкту з розробки та впровадження систем охоронної сигналізації, спрямованого на підвищення безпеки офісних приміщень, може бути перспективним в першу чергу в Україні, а подальша експансія на міжнародні ринки стане доцільною.

Для подальшого вивчення ринку та оцінки можливостей впровадження стартап-проєкту, необхідно провести аналіз потенційних сегментів клієнтів, їх характеристик і сформулювати приблизний перелік вимог до нашого продукту (див. Таблицю 4.7).

Таблиця 4.7.

Характеристика потенційних клієнтів стартап-проєкту

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару

Автоматизований контроль системи охоронної сигналізації в офісних приміщеннях.	IT-компанії, дата-центри, бізнес-центри,	Різниця у масштабі та особливостях технічного обладнання	Ефективність контролю параметрів безпеки та доступу в офісних приміщеннях.

Враховуючи представлену таблицю, можна зробити висновок, що на ринку існує попит на системи охоронної сигналізації для офісних приміщень, оскільки подібні технології ще не були широко представлені споживачам. Основною цільовою аудиторією є офісні будівлі, бізнес-центри та організації, які потребують ефективного контролю безпеки та доступу. Різниця в розмірі та функціональних потребах приміщень визначає різні вимоги споживачів до ефективності та надійності охоронних систем.

При впровадженні технології, яка подібна за принципом дії до запропонованої, можна визначити ряд потенційних викликів, які відображені у таблиці 4.8 нижче. Ці фактори можуть вплинути на можливості успішної реалізації та утримання конкурентоспроможності проєкту на ринку.

Таблиця 4.8.

Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1.	Неоптимальна інтеграція з існуючими системами	Можливість недостатньої сумісності з іншими системами безпеки та контролю доступу в офісних приміщеннях.	Проведення тестів та оптимізація інтеграційного процесу, врахування особливостей роботи існуючих систем.
2.	Високі вартості обслуговування та підтримки	Можливість збільшення витрат на обслуговування та технічну підтримку клієнтів.	Оптимізація процесів обслуговування, надання ефективної технічної підтримки, розробка програм для самостійного рішення невеликих проблем.
3.	Низька готовність ринку до інновацій у даній сфері	Можливість відмови ринку від інновацій у сфері охоронних систем для офісних приміщень.	Інформаційна кампанія про переваги та необхідність використання інновацій, співпраця з ключовими гравцями ринку для збільшення інтересу.
4.	Обмежений фінансовий бюджет потенційних клієнтів	Недостатній бюджет у клієнтів для впровадження нових технологій.	Недостатній бюджет у клієнтів для впровадження нових технологій.

Відповідно до сформованих загроз для нашого стартап-проєкту в сфері систем охоронної сигналізації, серед основних ризиків варто виділити потенційну неоптимальну інтеграцію з уже існуючими системами безпеки та контролю доступу в офісних приміщеннях. Можлива загроза полягає в недостатній сумісності нашого рішення з існуючими системами, що може виникнути через технічні чи програмні розбіжності. Для уникнення цієї загрози ми плануємо провести тестування та оптимізацію інтеграційного процесу, враховуючи особливості роботи інших систем.

Ще однією значущою загрозою є можливе збільшення витрат на обслуговування та технічну підтримку клієнтів. Це може статися через незадоволеність клієнтів якістю обслуговування або високими витратами на підтримку. Наш план передбачає оптимізацію процесів обслуговування, надання ефективної технічної підтримки, а також розробку програм для самостійного вирішення невеликих проблем.

Щодо низької готовності ринку до інновацій у сфері охоронних систем, основною загрозою може бути відмова від нових технологій у сфері безпеки офісних приміщень. Наша стратегія передбачає проведення інформаційної кампанії для підвищення обізнаності ринку про переваги та необхідність використання інновацій. Крім того, ми плануємо співпрацювати з ключовими гравцями ринку для збільшення інтересу до нашого рішення.

Окремою загрозою може стати обмежений фінансовий бюджет потенційних клієнтів, що може призвести до недостатнього фінансування для впровадження нових технологій. У цьому випадку ми прагнемо пропонувати ефективні та економічно вигідні рішення, які відповідають потребам наших клієнтів.

Окрім зазначених загроз, є також ряд можливостей для реалізації цього проєкту. На основі розглянутих можливостей можна зазначити перспективність впровадження та розвитку проєкту як на ринку України, так і за її межами. Ключовими перевагами є відсутність аналогічних технологій на широкому ринку та простота конструкції, що сприятиме ефективному впровадженню та

масштабуванню виробництва. Це відкриває можливість зайняти лідерську позицію у галузі охорони офісних приміщень та стати ключовим гравцем у цьому сегменті промисловості.

Таблиця 4.9.

Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Ефективність вартості	Проведений аналіз наявних компонентів для технологічної складової проєкту дозволяє обрати оптимальні за якістю і ціною компоненти.	Розгляд можливості використання більш точних, хоча трошки дорожчих компонентів для поліпшення якості модулю
2	Непереверешена технологія	На сучасному українському та міжнародному ринках відсутня широко доступна технологія систем охоронної сигналізації для офісних приміщень.	Запуск виробництва на українському ринку дозволить зайняти лідерську позицію в даній ніші.
3	Простота конструкції	Простота реалізації модулю забезпечить відносну доступність складових частин, що дозволить швидко запустити та масштабувати виробництво.	Швидке налагодження та розширення масштабів виробництва.
4	Постійна технологічна підтримка	Постійний контроль за якістю роботи модулю та його впливі на контроль мікроклімату в серверних кімнатах.	Компанія здійснює постійну технологічну підтримку, консультації щодо використання модулю та проведення опитувань щодо його подальших вдосконалень.
5	Розвиток технології	Можливість покращення конструкції та програмної складової модулю.	Компанія активно досліджує ринок для пошуку варіантів покращення модулю та реалізації нових рішень для його вдосконалення.

Для отримання більш докладного уявлення про конкурентне середовище та його вплив на функціонування підприємства, був проведений детальний аналіз особливостей конкурентного оточення, результати якого наведено у таблиці 4.10 нижче.

Відповідно до проведеного аналізу конкуренції на ринку систем охоронної сигналізації для офісних приміщень, виявлено певні бар'єри для виходу на український та міжнародний ринки. Зокрема, спостерігається олігопольна структура, де невелика кількість іноземних компаній через посередників домінує на українському ринку.

Таблиця 4.10.

Ступеневий аналіз конкуренції на ринку

№	Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1	Тип конкуренції: олігополія	Невелика кількість компаній-постачальників, які домінують через посередників на українському ринку систем охоронної сигналізації для офісних приміщень.	Розвиток власного українського виробництва, щоб здобути значну частку ринку.
2	Рівень конкурентної боротьби: національний	Присутність бар'єрів для нових учасників ринку.	Розгляд можливостей співпраці з великими виробництвами та підняття стандартів якості.
3	Галузева ознака: внутрішньогалузева	Конкуренція між компаніями, що працюють у галузі систем охоронної сигналізації для офісних приміщень.	Сприяє поліпшенню якості продукції та вдосконаленню технологічних процесів.
4	Конкуренція за видами товарів: товарно-видова	Змагання з іншими компаніями, які пропонують аналогічні рішення для систем охоронної сигналізації в офісних приміщеннях.	Збільшення витрат на маркетинг та рекламу продукту для підвищення його впізнаваємості.
5	Характер конкурентних переваг: неціонова	Зосередженість на якості, функціоналі та простоті реалізації конструкції.	Збільшення попиту на продукцію завдяки високій якості та точності роботи.
6	Інтенсивність конкуренції: марочна	Присутність багатьох відомих компаній у галузі систем охоронної сигналізації для офісних приміщень.	Ускладнення можливостей виходу на ринок, потреба в створенні унікальної пропозиції.

Однак налагодження повністю українського виробництва в галузі систем охоронної сигналізації для офісних приміщень дозволить ефективно зайняти ключову нішу, особливо враховуючи, що основні конкуренти є міжнародними компаніями, які працюють через посередників. Такий крок відкриває можливість для підприємства зайняти значну частку ринку, пропонуючи власні рішення та конкуруючи з іноземними брендами.

Після аналізу конкуренції проведемо більш детальний аналіз умов конкуренції в галузі за Портером. Отриманий аналіз показано у таблиці 4.11.

Таблиця 4.11.

Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
Складові аналізу	SafeGuard Solutions	SecureTech, ProtecSys	Виробники електронних компонентів.	IT-компанії, дата-центри, бізнес-центри,	Датчики для дистанційного контролю параметрів охоронної сигналізації.
Висновки:	Низька інтенсивність конкуренції обумовлена наявністю аналогічної продукції на ринку, яка відрізняється масштабами та за функціоналом і ціною.	Існують можливості для виходу на ринок через відсутність аналогічного модулю від потенційних конкурентів	Постачальники не диктують особливих умов, але маємо певний рівень залежності від них, зокрема від виробників електронних компонентів та баз даних.	Клієнти представлені IT-компаніями, дата-центрами, бізнес-центрами, можуть впливати на умови контрактів та співпраці.	Наявні товари-замінники мають схожий функціонал для контролю навколишнього середовища, проте не призначені для контролю в офісних приміщеннях з охоронною сигналізацією.

З проведеного аналізу видно, що ринок систем охоронної сигналізації в офісних приміщеннях, зокрема для серверних кімнат, насичений продуктами, які мають подібний функціонал контролю клімату. Однак вони відрізняються масштабами, технологічним оснащенням та ціною. Враховуючи це, виробництво спеціалізованих модулів для дистанційного контролю в таких приміщеннях є перспективним напрямком, оскільки наразі відсутні прямі конкуренти, які б спеціалізувалися на цьому сегменті ринку. Можливість виходу на ринок стає реальною завдяки відсутності аналогічних рішень у конкурентів та невисокій конкуренції, обумовленій тим, що існуючі продукти не фокусуються на охоронній сигналізації в серверних приміщеннях.

Залежність від постачальників виникає через співпрацю з виробниками електронних компонентів, що може впливати на умови контрактів і співпраці. Клієнтська база включає IT-компанії, дата-центри, бізнес-центри та майнінг ферми, що вимагає особливої уваги до умов контрактів та індивідуальних потреб кожного замовника.

Товари-замінники, наприклад, датчики для дистанційного контролю погодних умов, мають схожий функціонал, проте вони не призначені для використання в серверних кімнатах, що робить нашу розробку унікальною на ринку.

Після проведених аналізів буде сформований повний перелік факторів, які впливають на конкурентоспроможність проєкту в цьому сегменті ринку (табл. 4.12).

Таблиця 4.12.

Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проєктів значущим)
1	Точність і надійність вимірювань	Висока точність і надійність датчиків є ключовими чинниками, які впливають на ефективність роботи системи охоронної сигналізації в офісному приміщенні, забезпечуючи своєчасне виявлення аномалій та запобігання несправностей.
2	Масштабованість системи	Можливість масштабування системи від невеликих серверних кімнат до великих дата-центрів забезпечує універсальність та пристосованість до потреб клієнтів різних масштабів.
3	Енергоефективність	Зменшення витрат електроенергії сприяє економії коштів для клієнтів і впливає на стабільність експлуатації системи.
4	Гнучкість інтеграції з існуючими системами	Здатність системи охоронної сигналізації легко інтегруватися з наявними системами управління мікрокліматом та серверами дозволяє зберегти вже зроблені інвестиції клієнтів і спрощує процес впровадження нових технологій без значних додаткових витрат.
5.	Регулярні оновлення програмного забезпечення	Постійні оновлення ПЗ забезпечують підтримку нових функцій, безпеку та оптимізацію роботи системи протягом тривалого періоду користування.

Після аналізу факторів конкурентоспроможності проведемо порівняльний аналіз слабких та сильних сторін (табл. 4.13).

Таблиця 4.13.

Порівняльний аналіз сильних та слабких сторін «DUST_METER»

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з SafeGuard Solutions						
			–3	–2	–1	0	+1	+2	+3
1	Точність і надійність вимірювань	18							+
2	Масштабованість системи	16						+	

3	Енергоефективність	12				+			
4	Гнучкість інтеграції з існуючими системами	17						+	
5.	Регулярні оновлення програмного забезпечення	14					+		

З проведеного порівняльного аналізу видно, що система охоронної сигналізації "OfficeGuard Secure" має значні конкурентні переваги. Її висока точність і надійність датчиків, масштабованість, енергоефективність, гнучкість інтеграції з іншими системами безпеки та регулярні оновлення програмного забезпечення роблять її привабливою для користувачів. Рейтинг конкурентів підтверджує вищий статус "OfficeGuard Secure" на ринку охоронних систем для офісних приміщень порівняно із суперниками.

Ці фактори сприятимуть успішній реалізації проєкту та забезпечать його конкурентоспроможність у сфері систем охоронної сигналізації.

Для узагальнення результатів аналізу буде сформовано SWOT-аналіз, що підкреслить сильні та слабкі сторони, а також можливі загрози й можливості для розвитку проекту "OfficeGuard Secure".

Загалом, проведений аналіз показує, що "OfficeGuard Secure" володіє значними перевагами, які роблять його перспективним для успішного впровадження на ринку охоронних систем для офісних приміщень. Виявлені слабкі сторони та загрози не є критичними і можуть бути усунені за допомогою стратегічних кроків та заходів.

Переваги проєкту "OfficeGuard Secure" включають високу точність та надійність вимірювань, масштабованість системи, енергоефективність, гнучкість інтеграції з існуючими системами, а також систематичні оновлення програмного забезпечення. Ці фактори сприятимуть успішній реалізації та популяризації продукту на ринку.

Таблиця 4.14.

SWOT-аналіз для проєкту "OfficeGuard Secure"

Сильні сторони:	Слабкі сторони:

1. Висока точність і надійність вимірювань.. 2. Масштабованість системи. 3. Енергоефективність. 4. Гнучкість інтеграції з існуючими системами. 5. Регулярні оновлення програмного забезпечення.	1 Висока конкуренція на ринку охоронних систем для офісних приміщень. 2Можливість недовіри покупців до нових продуктів. 3.Залежність від стабільності поставок електронних компонентів і стабільності баз даних.
Можливості: 1. Підвищення точності вимірювань за рахунок нових технологій.. 2. Запуск великого виробництва для задоволення попиту. 3. Покращення якості системи через постійну технічну підтримку.	Загрози: 1. Можлива недостатня точність системи 2. Підвищення чутливості покупців до цін обслуговування і підтримки системи і модулів 3 Втрата конкурентних переваг через рост конкуренції. 4. Тиск з боку сильних конкурентів на ринку систем охоронної сигналізації для офісних приміщень.

Хоча існують конкурентні виклики та певні труднощі, але з належним підходом та врахуванням виявлених факторів, є можливість ефективно уникнути або подолати ці обмеження. Такий SWOT-аналіз дає підстави вважати "OfficeGuard Secure" перспективним та конкурентоспроможним продуктом в обраному сегменті ринку.

На основі проведеного SWOT-аналізу сформуємо стратегію альтернативного впровадження стартап-проєкту.

Ця таблиця відображає альтернативні стратегії для покращення ринкового впровадження проєкту "OfficeGuard Secure". Кожна альтернатива має свої переваги та можливості для реалізації.

На основі проведеного SWOT-аналізу сформульована стратегія альтернативного впровадження стартап-проєкту "OfficeGuard Secure". Запропоновані альтернативи для ринкового впровадження наведені в таблиці 4.15, і кожна з них орієнтована на підвищення конкурентоспроможності та ефективніше впровадження продукту на ринку систем охоронної сигналізації для офісних приміщень.

Таблиця 4.15.

Альтернативи ринкового впровадження стартап-проєкту "OfficeGuard Secure"

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації

1	Покращення точності та надійності системи охоронної сигналізації офісного приміщення.	Ресурси доступні та використовуються для підвищення ефективності модулю	3 місяці
2	Розширення функціоналу та можливостей системи	Забезпечить конкурентні переваги та високий рівень використання продукту	4-5 місяці
3	Інтенсивна рекламна кампанія та розвиток партнерських відносин	Сприятиме підвищенню усвідомленості та популярності продукту	2 місяці

Зважаючи на розглянуті альтернативи, важливо обрати оптимальний напрямок розвитку, який враховує поточний стан ринку та переваги проєкту "OfficeGuard Secure". Такий підхід дозволить максимізувати конкурентоспроможність та забезпечити успішне впровадження на ринку систем охоронної сигналізації.

4.3. Розроблення ринкової стратегії проєкту

Для ефективної розробки ринкової стратегії необхідно спочатку визначити стратегію охоплення ринку, зокрема, описати основні цільові групи потенційних споживачів (табл. 4.16). Основною аудиторією в цьому сегменті є підприємства та організації, які використовують системи охоронної сигналізації. Вибір конкретного сегменту серед них не є критичним, оскільки всі вони мають спільну потребу в надійному захисті та контролі безпеки приміщень.

Таким чином, проєкт "OfficeGuard Secure" орієнтований на широкий спектр клієнтів, і вибір конкретної цільової групи не є визначальним для стратегії виходу на ринок. Ключовим є забезпечення універсальності системи, що дозволить її адаптацію для різних типів офісних приміщень та об'єктів моніторингу.

Таблиця 4.16.

Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент

1	ІТ-компанії та дата-центри	Споживачі готові до впровадження інноваційних технологічних рішень, оскільки стабільність умов в офісних приміщеннях є критично важливою для їхнього нормального функціонування.	Високий попит в межах сегменту, оскільки для них критично важливо підтримувати оптимальні умови	Висока	Сервіс "OfficeGuard Secure" має високий технічний ступінь інтеграції та низьку ціну, що створює складні умови для конкурентів
2	Технічні підприємства	Зацікавлені в оптимізації умов експлуатації обладнання та підтриманні стабільності технічних систем	Середній попит в межах сегменту, оскільки вони можуть використовувати різні системи моніторингу	Середня	Можливість вибору між різними рішеннями створює середні умови для конкуренції
3	Бізнес-центри та офісні приміщення	Важливо для створення безпечного робочого середовища для співробітників	Високий попит в межах сегменту, оскільки забезпечення безпечних умов є ключовим для здоров'я та безпеки співробітників та обладнання	Середня	Доступність різних рішень у сегменті
4	Освітні установи Споживачі	Споживачі, які віддають перевагу безпеці навчального середовища	Середній попит в межах сегменту, оскільки освітні установи можуть мати обмежений бюджет	Середня	Доступність різних рішень у сегменті
Обрано цільові групи: інформаційні технології, технічні підприємства, бізнес-центри та офісні приміщення, освітні установи.					

Для ефективної роботи з обраними цільовими групами необхідно розробити базову стратегію розвитку, яка допоможе визначити основні напрямки та підходи до взаємодії з клієнтами (табл. 4.17).

Таблиця 4.17.

Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проєкту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку*
	Розширення функціоналу та можливостей системи, інтенсивна рекламна кампанія та розвиток партнерських відносин	Стратегія концентрованого зростання	Висока точність та безпека приміщення, енергоефективність, гнучкість інтеграції, регулярні оновлення ПЗ.	Стратегія диференціації за спеціалізованістю та інноваціями

У процесі аналізу стратегії розвитку для проєкту "OfficeGuard Secure" можна виокремити ключові напрямки, що сприятимуть досягненню успіху на ринку. Обрані стратегії дозволяють позиціонувати проєкт як інноваційне та конкурентоспроможне рішення на ринку охоронних систем для офісних приміщень, що сприятиме залученню нових клієнтів та підвищенню попиту серед цільових груп.

Наступним кроком буде вибір стратегії конкурентної поведінки. Обрану стратегії показано у таблиці 4.18 нижче.

Таблиця 4.18.

Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проєкт «першопроходьцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1	Так	Буде і шукати нових споживачів і частково забирати існуючих конкурентів	Не буде, основою проєкту є розробка альтернативних та інноваційних рішень	Стратегія зайняття конкурентної ніші

Обрана стратегія конкурентної поведінки передбачає активний пошук нових споживачів та часткове відтягування клієнтів від конкурентів, при цьому компанія не буде копіювати основні характеристики конкурентних рішень. Основною метою є розробка альтернативних та інноваційних рішень, що дозволить зайняти конкурентну нішу на ринку систем охоронної сигналізації для офісних приміщень.

На основі проведеного аналізу обраного сегменту ринку, а також враховуючи вибрану стратегію розвитку та конкурентної поведінки, слід розробити стратегію позиціонування (табл. 4.19).

Обрана стратегія позиціонування фокусується на високій точності вимірювань, ефективності та надійності системи охоронної сигналізації, масштабованості та простоті інтеграції. Ключові асоціації для формування комплексної позиції проекту: точність, надійність та ефективність.

Таблиця 4.19.

Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
	Наявність надійного та точного моніторингу безпеки офісного приміщення.	Стратегія лідерства по витратах	Низька ціна, висока точність моніторингу, ефективність та надійність, масштабованість та простота інтеграції	Ціна. Точність. Надійність. Ефективність.

4.4. Розроблення маркетингової програми стартап-проєкту

Для розробки ефективної та якісної маркетингової програми необхідно сформулювати маркетингову концепцію товару, яку отримає споживач та яка принесе йому вигоду. Для цього було узагальнено результати аналізу конкурентоспроможності товару у вигляді таблиці 4.20 нижче.

Аналізуючи ключові переваги концепції системи охоронної сигналізації "OfficeGuard Secure", можна відзначити, що проєкт має унікальні характеристики, такі як точне вимірювання параметрів безпеки, швидка реакція на зміни та здатність до інтеграції з існуючими системами охорони. Ці переваги роблять проєкт конкурентоспроможним на ринку охоронних рішень для офісних приміщень.

Таблиця 4.20.

Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
	Точність виявлення небезпек.	Забезпечення точності моніторингу.	Висока точність розпізнання загроз порівняно з існуючими системами.
	Швидкість реагування на загрозу.	Забезпечення оперативності подання сигналу про небезпеку	Ефективна система моніторингу, яка дозволяє швидко реагувати на присутні загрози.
	Інтеграція з існуючими системами моніторингу.	Можливість використання разом з іншими системами..	Сумісність із вже впровадженими засобами моніторингу та автоматизації.

Сформуємо основні характеристики і властивості нашого проєкту у вигляді трьохрівневої моделі товару. Сформований опис представлено у вигляді таблиці 4.21 нижче.

Таблиця 4.21.

Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
I. Товар за задумом	Автоматизований модуль моніторингу мікроклімату для серверних кімнат "OfficeGuard Secure"		
II. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	1. Забезпечення безпеки приміщення. 2. Ефективна цінова політика. 3. Легка інтеграція з існуючими системами. 4. Постійні оновлення програмного забезпечення. 5. Зручне програмне забезпечення для користувачів.	Нм М Нм М Нм	Тх Е Вр Тх Е
	Якість: висока точність, зручне і надійне програмне забезпечення		
	Пакування: сам модуль для охоронної сигналізації офісного приміщення поставляється в коробці з документацією. Окрім цього, передбачено наявність адміністративного сайту, на якому можна буде додавати користувачів для моніторингу системи та призначати їм відповідні ролі в межах підприємства.		
	Марка: OfficeGuard Secure		
III. Товар із підкріпленням	Після, як і до продажу супроводжується постійною технічною підтримкою з налаштування. Проводиться демонстрація використання сайту і всі основні особливості і можливості сайту.		

З наведеного аналізу видно, що на першому рівні представлено основну концепцію проєкту — автоматизовану систему охоронної сигналізації "OfficeGuard Secure". На другому рівні розкриваються важливі характеристики та переваги продукту, такі як висока точність сигналізації, ефективна цінова політика, легкість інтеграції, регулярні оновлення програмного забезпечення та зручність використання для кінцевих користувачів. Всі ці характеристики

роблять продукт перспективним і конкурентоспроможним на ринку охоронних систем для офісних приміщень.

Після детального аналізу властивостей та характеристик продукту необхідно визначити цінові межі для встановлення вартості товару. Ці межі формуються на основі цін конкурентів та доходів цільових споживачів. Отримані цінові межі наведені в таблиці 4.22.

Таблиця 4.22.

Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	Від 5000 до 40000 грн	Немає аналогів в широкому доступі, ціна невідома	Від 15000 грн і вище	Від 10000 до 60000 грн

Отримані межі встановлення ціни на "OfficeGuard Secure" враховують аналіз ринку товарів-замінників, відсутність аналогів у широкому доступі та дохід цільової групи споживачів. Рекомендовані верхня та нижня межі встановлення ціни на "OfficeGuard Secure" становлять від 10000 до 60000 гривень. Ці ціни враховують специфіку ринку та доступність для цільової аудиторії.

Після проведеного аналізу ціни на систему охоронної сигналізації "OfficeGuard Secure" для офісних приміщень, необхідно розробити стратегію збуту товару. Результати цієї стратегії наведені в таблиці 4.23 нижче.

Отже, Отримана система збуту "OfficeGuard Secure" враховує особливості цільових клієнтів, функції постачальника товару та ринкові умови. Продажі плануються через веб-сайт та прямі поставки, орієнтуючись на IT-компанії, дата-центри та адміністраторів серверних кімнат на ринку України.

Таблиця 4.23.

Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	IT-компанії, дата-центри, адміністратори серверних кімнат	Технічна підтримка, налаштування, навчання користувачів	Ринок України	Продажі через веб-сайт та прямі поставки

Останнім етапом буде формування концепції комунікацій для маркетингу, що ґрунтуються на основі попереднього аналізу проєкту. Отриману концепцію буде представлено у вигляді таблиці 4.24 нижче.

Таблиця 4.24.

Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
	Пошук системи охоронної сигналізації, яка відповідає вимогам щодо цінової доступності, зручності управління та можливості дистанційного моніторингу.	Спеціалізовані веб-сайти, конференції, презентації	Автоматизована система охоронної сигналізації "OfficeGuard Secure".	Пояснення переваг та ефективності управління безпекою та охороною офісних приміщень.	Підкреслення технологічності та унікальності системи охоронної сигналізації "OfficeGuard Secure".

В результаті формування концепції маркетингових комунікацій визначено, що в основі поведінки цільових клієнтів лежить пошук продукту з високою точністю мікроклімату та можливістю дистанційного контролю. Основними каналами комунікацій є спеціалізовані веб-сайти, конференції та презентації. Для привертання уваги цільових споживачів слід акцентувати увагу на сильних сторонах проєкту та на відсутності подібного товару у широкому доступі на ринку мікрокліматичних систем для серверних кімнат.

4.5. Організація реалізації стартап-проєкту

В результаті формування концепції маркетингових комунікацій для системи охоронної сигналізації "OfficeGuard Secure" було визначено, що ключовим фактором для цільових клієнтів є пошук рішення з високою точністю контролю безпеки та можливістю дистанційного моніторингу. Основними каналами комунікації стануть спеціалізовані веб-сайти, конференції та презентації. Для

привертання уваги споживачів варто акцентувати увагу на сильних перевагах системи, таких як її надійність, інноваційність та унікальність на ринку охоронних систем для офісних приміщень.

Таблиця 4.25.

Команда стартап-проєкту

Учасник команди	Посада	Завдання, що необхідно виконати
Інженер-розробник	Керівник розробки	Розробити прототип системи охоронної сигналізації для офісного приміщення та забезпечити її повну функціональність.
Архітектор програмного забезпечення	Головний програміст	Розробити високоефективне програмне забезпечення для OfficeGuard Secure
Менеджер проекту	Керівник проекту	Координувати роботу команди, визначити критичні точки та вирішувати організаційні питання
Спеціаліст з інтеграції систем	Інженер з інтеграції	Забезпечити сумісність OfficeGuard Secure з існуючими системами управління
Експерт з маркетингу	Спеціаліст з аналізу ринку	Провести ретельний аналіз сегменту ринку та розробити стратегію маркетингу

Після створення команди важливо розробити графік для моніторингу завдань та приблизного визначення термінів їх виконання. Створений графік подано у таблиці 4.26 нижче.

На основі розробленого календарного плану, вартість повного процесу від розробки системи охоронної сигналізації до її запуску оцінюється приблизно в 880 тис. грн. Ця сума знаходиться в межах визначеного цінового діапазону, вказаного в таблиці 4.22. Процес реалізації проєкту включає розробку надійного модуля для системи охоронної сигналізації, розробку конструкції та супутньої документації для монтажу, створення програмного забезпечення для управління системою та тестування отриманого продукту, а також залучення інвестицій та запуск виробництва і продажу.

Таблиця 4.26.

Календарний план реалізації проєкту

№ п/п	Зміст етапу	1	2	3	4	5	6	7	8	9	10	11	12	Собівартість реалізації
1	Аналіз ринку та визначення вимог													0
2	Розробка концепції ідеї проєкту													500$
3	Створення технічного завдання та конструкції													800$
4	Розробка електричних та принципових схем, виготовлення прототипу													1200$
5	Розробка та вдосконалення програмного забезпечення													1500$
6	Тестування та виправлення недоліків													300$
7	Пошук і залучення інвестицій													1000$
8	Запуск виробництва													15000$
9	Проведення масштабних рекламних кампаній та старт продаж													3000$
													Сума	22300$

Для залучення інвесторів рекомендується використовувати можливості спеціалізованих виставок охоронних технологій, де можна продемонструвати основні переваги системи. Крім того, платформи для запуску нових стартапів, такі як Kickstarter, можуть стати ефективним інструментом для залучення фінансування. Таким чином, впровадження та виробництво автоматизованої системи охоронної сигналізації для офісних приміщень, згідно з розробленими етапами, дозволяє реалізувати проєкт у визначеному ціновому діапазоні та залучити необхідні інвестиції.

Після створення календарного плану, необхідно розробити таблицю вихідних витрат на компоненти та обладнання, необхідні для виготовлення модулю. Розрахунки за цією ініціативою наведено у таблиці 4.27.

Таблиця 4.27.

Витрати на виробництво

№ п/п	Витрати	Тип	Терміни постачання/виконання	Вартість, $
1	Мікроконтролер ESP32	----	3 днів	10
2	Модуль для Wi-Fi	----	3 днів	3
3	Датчик руху	----	4 днів	5
4	Макетна платформа	----	2 днів	4
5	Паяльна станція	---	2 дні	60
6	Припій	---	3 днів	5
7	Флюс	---	5 днів	4
8	Розхідні матеріали	----	5 днів	50
			Сума	141

Отже, для старту виробництва одного модулю на початковому етапі потрібно 141 долар. На першій фазі наявні 20 000 доларів для втілення проєкту, а в подальшому можливо залучити інвесторів за допомогою платформи Kickstarter.

Висновки до IV розділу

У цьому розділі детально розглянуто перспективи впровадження модулю для автоматизованої системи охоронної сигналізації офісних приміщень. Підкреслено, що реалізація такого проєкту є надзвичайно важливою в контексті зростаючих вимог до безпеки та ефективності охоронних систем у сучасних офісах.

Автоматизована система охоронної сигналізації "OfficeGuard Secure" має стратегічне значення для забезпечення надійного захисту офісних приміщень. Вона передбачає інтеграцію з існуючими системами безпеки та покращення контролю за доступом, відеоспостереженням і іншими критичними параметрами. Розроблений календарний план показує, що загальні витрати на реалізацію проєкту оцінюються на рівні приблизно 22,300 доларів.

Процес реалізації включає створення надійної та високоточної системи охоронної сигналізації, а також розробку концепції, створення конструкції, супровідної документації, розробку програмного забезпечення, тестування, залучення інвестицій, запуск виробництва та впровадження на ринок.

Загальний висновок підкреслює важливість впровадження автоматизованих систем охоронної сигналізації в офісних приміщеннях. Цей інноваційний підхід сприяє підвищенню надійності та ефективності систем безпеки, відкриваючи нові можливості для розвитку безпечного і ефективного робочого середовища. Тому впровадження "OfficeGuard Secure" стане важливим кроком до стабільної роботи офісних приміщень, що є ключовим фактором у забезпеченні безпеки в сучасному діловому середовищі.

ЗАГАЛЬНІ ВИСНОВКИ

Під час виконання магістерської дисертації було розроблено автоматизовану системи охорони для офісного приміщення. Система дозволяє відстежувати стан офісного приміщення та за рахунок бездротового з’єднання здатна посилати сигнал сповіщення на пульт охорони.

В роботі було виконано:

1. Аналіз існуючих рішень: Проведений аналіз складових охороної системи, проведено огляд існуючих технічних рішень. Наведені їх переваги та недоліки.
2. Вибір елементної бази обгрунтований розповсюдженням та ціною елементів.
3. Розроблено структурну та електричну принципову схеми системи охорони офісного приміщення.
4. Наведено алгоритми роботи системи та програмні коди для керування блоками системи.

СПИСОК ЛІТЕРАТУРИ

1. Михальчук Д. О., Яворська О. М. Аналіз ринку систем охоронної сигналізації. Матеріали 75-ї науково-технічної конференції професорсько-викладацького складу, науковців, аспірантів та студентів. 2020. С. 49-50.

2. Ahmad M. B., Abdullahi A. A., Muhammad A. S., Saleh Y. B., Usman U. B. The Various Types of sensors used in the Security Alarm system. International Journal of New Computer Architectures and their Applications (IJNCAA). 2019. 9(2). P. 50-59.

3. Погребенник В. Д., Політило Р. В. Ультразвукові сенсори системи охоронної сигналізації. Вісник НТУУ “КПІ”. Серія «Приладобудування». 2008. Вип. 36. С. 68-76.

4. Кугір А. В. Автоматизована система охоронної сигналізації для промислового підприємства. 2021. С. 75-76.

5. Çavaş M., Ahmad M. B. A review advancement of security alarm system using internet of things (IoT). International Journal of New Computer Architectures and their Applications (IJNCAA). 9 (2). 2019.P. 38-49.

6. Кучеров Д. П., Березкін А. Л. Радіоканал LORA в системі охоронної сигналізації. Наукоємні технології. 2019. № 3(43). С. 357-363.

7. Комплект бездротової сигналізації MAKS PRO Black. URL: https://securitylab.com.ua/ua/maks-pro-black/ (дата звернення: 16.09.2024).

8. Комплект бездротової сигналізації ATIS Kit GSM 100. URL: https://securitylab.com.ua/ua/atis-kit-gsm-100/ (дата звернення: 17.09.2024).

9. StarterKit – стартовий комплект системи безпеки Ajax. URL: https://ajax.systems/ua/products/starterkit/ (дата звернення: 18.09.2024).

10. Бездротова кімнатна сирена Ajax HomeSiren. URL: https://ajax.systems/ua/products/homesiren/ (дата звернення: 18.09.2024).

11. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп’ютеризованих вимірювальних систем і комплексів. Навчальний посібник. Тернопіль: ТНТУ. 2019. 150 с.

12. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. [навчальний посібник] Львів: «Магнолія 2006». 2013. 256 с.

13. Лупенко С.А., Тиш Є.В. Прикладна теорія цифрових автоматів. Навчальний посібник. Тернопіль: ТНТУ ім. І. Пулюя. 2011. 247 с.

14. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп'ютеризованих вимірювальних систем і комплексів. Навчальний посібник. Тернопіль: ТНТУ. 2019. 150 с.

15. Osukhivska H., Tysh I., Lobur T., Shylinska I., Lupenko S. Method for Estimating the Convergence Parameters of Dynamic Routing Protocols in Computer Networks. In 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT). 2021. Vol. 1. P. 228-231.

16. Тиш Є., Зима О. Вибір критеріїв ефективності безпровідних телеметричних мереж. Матеріали VII науково-технічної конференції "Інформаційні моделі, системи та технології". Тернопіль : ТНТУ. 2019. С. 139.

17. Тиш Є.В., Зима О.В. Методи та засоби підвищення ефективності безпровідних телеметричних мереж. Збірник тез доповідей VIII Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». 2019. С. 101.

18. Оконський М. В., Лупенко С. А., Паламар А. М. Комп'ютерна система для моніторингу метеорологічних параметрів на основі IoT. Збірник тез доповідей X Міжнародної науково-практичної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». 2021. С. 109.

19. Vasylkivskyi I., Ishchenko V., Pohrebennyk V., Palamar M., Palamar A. System of water objects pollution monitoring. International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management (SGEM 2017), Vienna, Austria. 2017. Vol. 17, No. 33. P. 355-362.

20. Palamar A. Intelligent control and monitoring module for uninterruptible power supply system. II International Scientific and Practical Conference

«Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs» (MC&FPGA-2020), Kharkiv, Ukraine. 2020. P. 12-13.

21. Arduino Uno R3 https://www.mini-tech.com.ua/ua/arduino-uno (дата звернення: 30.09.2024).

22. Arduino UNO - популярна плата розробки https://itmaster.biz.ua/directory/kits-nabory/arduino-uno.html (дата звернення: 30.09.2024).

23. Датчик руху (PIR Motion sensor) HC-SR501 https://radiostore.ua/products/datchik-dvizheniya-pir-motion-sensor-hc-sr501-2 (дата звернення: 30.09.2024).

24. Магнітно-контактний герконовий датчик відкриття дверей, вікна MC-38 https://diyshop.com.ua/ua/magnitno-kontaktnyj-gerkonovyj-datchik-otkrytiya-dveri-okna-mc-38?srsltid=AfmBOooG3F4ibjlPJFICt49cr9h68cJ69AHE1HIxb7VuTsG1LHIKj6F2 (дата звернення: 30.09.2024).

25. Модуль мікрофон Arduino із високою чутливістю KY-037 (датчик звуку) https://mrrobot.com.ua/product/modul-mikrofon-arduino-iz-vysokoyu-chutlyvistyu-ky-037-datchyk-zvuku/?srsltid=AfmBOoq6FiV4Uv--PHZS2g2fN5dCHTsN7Cwj_PYLmKA-NX6mJSaL0KmG (дата звернення: 30.09.2024).

26. GSM модуль на SIM800L https://arduino.ua/prod1665-gsm-modyl-na-sim800l (дата звернення: 30.09.2024).

27. Зарядний модуль TP4056 Type-C з функцією захисту акумулятора https://arduino.ua/prod4517-zaryadnii-modyl-tp4056-type-c-s-fynkciei-zashhiti-akkymylyatora (дата звернення: 30.09.2024).

28. Модуль п'єзодинаміка https://uamper.com/Buzzer-%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C-%D0%B4%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8%D0%BA%D0%BE%D0%BC-%D0%BF%D1%8C%D0%B5%D0%B7%D0%BE-

%D0%BF%D0%B8%D1%89%D0%B0%D0%BB%D0%BA%D0%B0 (дата звернення: 30.09.2024).

29. LCD дисплей 1602 (HD44780) із зеленим підсвічуванням https://ardushop.in.ua/arduino/lcd-display-1602-hd44780-with-green-backlight (дата звернення: 30.09.2024).

30. I2C модуль розширення виводів Arduino для підключення LCD дисплея на PCF 8574T https://arduino.ua/prod1790-iici2cinterfeis-lcd1602-2004 (дата звернення: 30.09.2024).

31. Чорнобай, Д. «Розробка охоронної системи «розумного будинку» на основі Arduino : кваліфікаційна робота : 126 Інформаційні системи та технології/ Чорнобай Дмитро. – Київ, 2024. – 71 с.

32. Богдан Г.А., Глущенко М.О., Протасов А. Г Система моніторингу якості повітря на промислових підприємствах. XXII Міжнародна науково-технічна конференція "Приладобудування: стан і перспективи", 16-17 травня 2023р., м. Київ, Україна : збірник тез доповідей. – Київ : КПІ ім. Ігоря Сікорського, 2023. – С. 283–285

33. Богдан Г.А., Глущенко М.О. Оптичний датчик чадного газу. X Міжнародна науково-технічна конференція «ДАТЧИКИ, ПРИЛАДИ ТА СИСТЕМИ – 2023», присвячена пам‘яті професора Шарапова В.М., 12 - 14 вересня 2023 року, м. Черкаси, Україна : збірник праць. – Черкаси, 2023. – С. 52–53

34. Богдан Г.А., Глущенко М.О. Система попередження пожеж. XXII Міжнародна науково-технічна конференція "Приладобудування: стан і перспективи", 16-17 травня 2023р., м. Київ, Україна : збірник тез доповідей. – Київ : КПІ ім. Ігоря Сікорського, 2023. – С. 234–236.

35. Антонюк В.С. Методологія наукових досліджень: [Текст] : навч. посіб./ В.С. Антонюк, Л.Г. Полонський, В.І. Аверченков, Ю.А. Малахов. – К.: НТУУ «КПІ», 2015. – 276 с.

36. Богдан Г.А., Глущенко М.О. Загальні тенденції побудови

автоматизованих систем моніторингу якості повітря на промислових підприємствах Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2023. – Том. 34 (73), №4. – С. 12-17.

37. Муравйов О. В. Сучасний стан та перспективи розвитку адитивних технологій / О. В. Муравйов, Ю. М. Нижник, В. Ф. Петрик, А. Г. Протасов, К. М. Сєрий // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. – 2021. – Том 32 (71), №5. – С. 114-119.

38. Куц, Ю. В. Спеціальні розділи математики. Курс лекцій: навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Комп'ютерно-інтегровані системи та технології в приладобудуванні» спеціальності 151 Автоматизація та комп’ютерно–інтегровані технології / Ю. В. Куц, Ю. Ю. Лисенко ; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2022. – 180 с.

39. Баженов В.Г. Електроніка. Лабораторний практикум: навчальний посібник / В. Г. Баженов, Є. Ф. Суслов, Ю. Ю. Лисенко, А.С. Момот; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2022. – 70 с.