

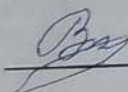
Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Розробка програмно-апаратного комплексу сигналізації з функціями віддаленого керування та оповіщення на основі платформи Arduino

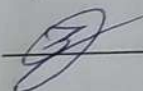
Виконав: студент 4 курсу, гр.2КІТС-216
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)



Ніколайчук О.В.

(прізвище та ініціали)

Керівник: к.т.н., доц., зав. каф. МБІС

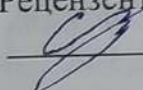


Карпінець В.В.

(прізвище та ініціали)

« 4 » *серпень* 2025 р.

Рецензент: к.т.н., професор кафедри ОТ



Захарченко С.М.

(прізвище та ініціали)

« 4 » *серпень* 2025 р.

Допущено до захисту

Голова секції УБ кафедри МБІС

д.т.н., проф. Яремчук Ю.Є.

« 4 » *серпень* 2025р.

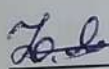
Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти I-й (бакалаврський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека

Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС



д.т.н., проф. Яремчук Ю.Є.

“ 20 ” березня 2025 р.

ЗАВДАННЯ

на бакалаврську кваліфікаційну роботу студенту

Ніколайчук Олександр Вікторович

(прізвище, ім'я, по-батькові)

1. Тема роботи Розробка програмно-апаратного комплексу сигналізації з функціями віддаленого керування та оповіщення на основі платформи Arduino
Керівник роботи Карпинець Василь Васильович, к.т.н., доц., зав. каф. МБІС
(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “20” березня 2025 року
№ 97

2. Термін подання студентом роботи 3 червня 2023р

3. Вихідні дані до роботи Електронні джерела, підручники та наукові статті по темі. Існуюче програмне забезпечення, яке стосується теми бакалаврської кваліфікаційної роботи.

4. Зміст текстової частини:

У ході виконання бакалаврської роботи було досліджено потреби у сфері охорон об'єктів, проаналізовано існуючі рішення, після чого розроблено програмно-апаратний комплекс сигналізації з можливістю віддаленого керування через Telegram-бота. Було реалізовано програмний модуль на мові C/C++ в середовищі Arduino IDE, який забезпечує обробку даних з датчиків, реагування на загрози, надсилання повідомлень і переведення системи в різні стани. Результати тестування підтвердили коректну роботу всіх функціональних блоків, стабільність підключення до мережі та зручність взаємодії з користувачем.

5. Перелік ілюстративного матеріалу:

Структурна схема системи охоронної сигналізації, Принципова електрична схема підключення компонентів, Схема алгоритму роботи, Фрагменти програмного коду, Схема з'єднання мікроконтролера.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ I	Карпинець В. В., к.т.н., доц., зав. каф. МБІС		
Розділ II	Карпинець В. В., к.т.н., доц., зав. каф. МБІС		
Розділ III	Карпинець В. В., к.т.н., доц., зав. каф. МБІС		

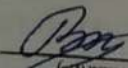
7. Дата видачі завдання 20 березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

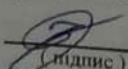
№	Назва та зміст етапу	Термін виконання		Примітка
		початок	закінчення	
1	Аналіз потреб у сфері охоронних систем	01.04.2025	07.04.2025	Виконано
2	Аналіз існуючих рішень та методів реалізації	08.04.2025	14.04.2025	Виконано
3	Постановка задачі та визначення технічних вимог	15.04.2025	17.04.2025	Виконано
4	Вибір архітектури системи та основних компонентів	18.04.2025	21.04.2025	Виконано
5	Розробка структурної та електричної схем	22.04.2025	26.04.2025	Виконано
6	Розробка алгоритму роботи охоронної сигналізації	27.04.2025	01.05.2025	Виконано
7	Реалізація програмного забезпечення для ESP8266 та Arduino	02.05.2025	10.05.2025	Виконано
8	Збірка апаратного забезпечення прототипу	11.05.2025	14.05.2025	Виконано
9	Тестування роботи системи на практиці	15.05.2025	20.05.2025	Виконано
10	Оформлення пояснювальної записки та підготовка до захисту	21.05.2025	25.05.2025	Виконано

Студент

Керівник роботи


(підпис)

Ніколайчук О.В.
(прізвище та ініціали)


(підпис)

Карпинець В.В.
(прізвище та ініціали)

АНОТАЦІЯ

У роботі представлено процес розробки програмно-апаратного комплексу охоронної сигналізації, що підтримує функції дистанційного керування та оповіщення користувача. Система реалізована на основі мікроконтролера Arduino із застосуванням недорогих апаратних компонентів та сучасних засобів комунікації, зокрема через Telegram-бота. Проведено аналіз існуючих рішень у сфері безпеки, досліджено принципи дії датчиків та обґрунтовано вибір технічних складових. У результаті спроектовано, зібрано й протестовано робочий прототип сигналізації, орієнтований на захист об'єктів від несанкціонованого доступу, призначеної для захисту приватних або малих комерційних об'єктів.

ABSTRACT

The paper presents the development process of a hardware-software security alarm system that supports remote control and user notification functions. The system is implemented based on an Arduino microcontroller using low-cost hardware components and modern communication tools, particularly a Telegram bot. An analysis of existing security solutions was conducted, the operating principles of sensors were examined, and the selection of technical components was justified. As a result, a working prototype of the alarm system was designed, assembled, and tested, aimed at protecting premises from unauthorized access, including private or small commercial properties.

ЗМІСТ

ВСТУП.....	8
1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ОБҐРУНТУВАННЯ ТЕМИ КВАЛІФІКАЦІЙНУ РОБОТИ.....	10
1.1 Аналіз сучасних апаратних рішень охоронних сигналізацій.....	10
1.2 Класифікація та принципи роботи охоронних систем.....	14
1.3 Порівняння основних типів охоронних сигналізацій	17
1.4 Огляд та принцип дії основних типів сенсорів	21
1.6 Висновки та постановка задач.....	28
2 ПРОЄКТУВАННЯ СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ З ВІДДАЛЕНИМ КЕРУВАННЯМ ТА ОПОВІЩЕННЯМ.....	30
2.1 Аналіз можливості вдосконалення системи сигналізації.....	30
2.2 Вибір компонентів для програмно-апаратного комплексу сигналізації.	32
2.3 Розробка алгоритму роботи програмно-апаратного комплексу сигналізації.....	38
2.4 Обґрунтування вибору мов програмування.....	42
Висновок до розділу 2	43
3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС СИГНАЛІЗАЦІЇ З ВІДДАЛЕНИМ КЕРУВАННЯМ ТА ОПОВІЩЕННЯМ.....	45
3.1 Реалізація програмного забезпечення програмно-апаратного комплексу сигналізації.....	45
3.2 Апаратна реалізація програмно-апаратного комплексу сигналізації ...	52
3.3 Тестування прототипа програмно-апаратного комплексу сигналізації	55
3.4 Висновок до розділу 3.....	59

ВИСНОВКИ	61
ПЕРЕЛІК ПОСИЛАНЬ.....	63
Додаток А. Технічне завдання.....	67
Додаток Б. Лістинг програмного коду.....	71
Додаток В. Ілюстраційний матеріал	75
Додаток Г. Протокол перевірки на антиплагіат	83

ВСТУП

Актуальність. У сучасних умовах стрімкого розвитку інформаційних технологій та зростання рівня загроз інформаційній безпеці особливої уваги потребує захист фізичних об'єктів, зокрема приватних помешкань, офісів, складів та інших приміщень. Несанкціонований доступ до таких об'єктів може призвести до матеріальних збитків, крадіжок, витоку конфіденційної інформації та інших серйозних наслідків.

У зв'язку з цим актуальним є створення ефективних, доступних і гнучких у налаштуванні охоронних систем, які поєднують апаратні засоби з інтелектуальними функціями програмного забезпечення. Особливої актуальності набуває використання мікроконтролерів, таких як Arduino, які дають змогу реалізувати масштабовані рішення із широким спектром функцій, включаючи дистанційне керування та оповіщення користувача про загрози в реальному часі.

Метою роботи є розробка програмно-апаратного комплексу охоронної сигналізації на базі Arduino, який має можливість дистанційного керування та оповіщення про інциденти. Це дозволяє створити універсальну, доступну та масштабовану систему для захисту приватних об'єктів від несанкціонованого доступу.

Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати існуючі типи охоронних сигналізацій, їх архітектуру, типи сенсорів та можливості;
- дослідити принципи побудови систем на базі мікроконтролера Arduino та засоби реалізації зв'язку з користувачем;
- розробити структуру апаратної частини системи: сенсори, контролер, виконавчі пристрої;
- реалізувати програмну логіку реагування на тривожні події, а також механізми дистанційного керування;
- протестувати функціональність розробленого комплексу в умовах, наближених до реального середовища.

Об'єктом дослідження є технічні засоби охоронної сигналізації, зокрема, сенсори для виявлення вторгнень, а також інші компоненти програмно-апаратної системи, що забезпечують охорону приміщень.

Предметом дослідження є методи та засоби реалізації недорогих охоронних систем з використанням Arduino, включаючи принципи роботи сенсорів, алгоритми оповіщення та функціональність дистанційного керування.

Новизна роботи полягає в інтеграції доступних апаратних засобів та сучасних методів розробки охоронних систем, які поєднують зручність віддаленого керування та оповіщення через мобільні додатки з високою ефективністю у захисті об'єктів. Крім того, новизна виявляється у простоті і доступності запропонованої системи, що дозволяє її широке застосування.

Практична цінність роботи полягає в тому, що розроблений комплекс може бути застосований для захисту приватних будинків, дач, гаражів, офісів та інших невеликих об'єктів. Результати роботи можуть стати основою для подальшої модернізації та інтеграції в інші системи "розумного дому", а також для розробки аналогічних охоронних систем.

1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ОБҐРУНТУВАННЯ ТЕМИ КВАЛІФІКАЦІЙНУ РОБОТИ

У цьому розділі проводиться аналіз існуючих рішень у сфері сигналізаційних систем, а також визначаються основні переваги та недоліки комерційних аналогів. Розглядаються сучасні технології, що використовуються для підвищення ефективності безпеки об'єктів.

1.1 Аналіз сучасних апаратних рішень охоронних сигналізацій

Людство стикається з проблемою крадіжок з найдавніших часів, і способи захисту майна постійно змінювалися. Замки, охоронці, собаки, механічні пастки усе це використовувалося для забезпечення безпеки. Однак із розвитком технічного прогресу акцент змістився на сучасні засоби захисту, зокрема охоронну сигналізацію [1].

Сьогодні охоронні системи, відеоспостереження та сигналізація стали невід'ємною частиною нашого життя. Вони забезпечують своєчасне виявлення несанкціонованого проникнення на охоронюваний об'єкт та оповіщення про надзвичайні ситуації, включаючи пошкодження, спричинені стихійними лихами, техногенними аваріями чи нещасними випадками.

Охоронна сигналізація (ОС) – це електронний пристрій, який дозволить Вам завжди бути упевненим в безпеці вашого будинку, офісу, квартири, складу, виробничого приміщення і т. д. Охоронна сигналізація розрахована на попередження несанкціонованого доступу в приміщення [7].

Найпоширенішими пристроями для забезпечення безпеки є різноманітні системи сигналізації. Вони можуть сповіщати про нештатні ситуації за допомогою звукових (дзвінки, сирени) та світлових сигналів (сигнальні лампи, світлодіоди), а також передавати тривожний сигнал на централізовані пульти охорони[2]. Передача сигналу може здійснюватися як дротовими каналами (через кабельні з'єднання), так і бездротовими (через GSM, Wi-Fi або радіоканали),

Зазвичай система сигналізації складається з охоронної панелі (централі, ППК), яка приймає та аналізує інформацію від датчиків безпеки, а також виконує заздалегідь запрограмовані дії у разі спрацювання датчиків. До її складу входить пульт управління, що відображає стан системи, дозволяє її програмувати, вмикати та вимикати охорону. Мінімальний набір обладнання також включає джерело безперебійного живлення (ДБЖ), кабельну мережу та охоронні датчики.

Ринок сигналізаційних систем пропонує широкий вибір пристроїв, які відрізняються конструкцією, комплектацією, функціональними можливостями, призначенням і ціною [4]. Замовник може обрати як готовий комплекс для повноцінного захисту, так і індивідуально підібраний набір обладнання, що відповідає певному типу сигналізації. Вибір оптимального обладнання залежить від конкретних умов і вимог до системи безпеки, зокрема від того, які датчики необхідно встановити [3].

Сучасна система Ajax - це універсальні пристрої, що дозволяють встановлювати їх в житлових будинках, квартирах і офісних приміщеннях. Основа даної охоронної системи сигналізації - це датчики, в основному бездротові, що функціонують на вбудованих акумуляторах (рис 1.1) [6].



Рисунок 1.1 – Ajax StarterKit White

Компанія «Аjax» виготовляє охоронні пристрої, сирени, центральні блоки керування для встановлення їх у житлових, офісних та інших приміщеннях. Компактність, ергономіка, сучасний мінімалістичний дизайн і висока якість є особливою рисою даних пристроїв [5].

Однак серед недоліків варто відзначити:

- високу вартість обладнання,
- обмежену можливість розширення системи за рахунок зовнішніх датчиків або інтеграції з іншими технологіями,
- відсутність вбудованої сирени,
- відсутність входів для шлейфів дротяних датчиків,
- вихід для підключення зовнішнього світодіода,
- система потребує стабільного інтернет-з'єднання для нормальної роботи і хмарне функціонування системи.

Таблиця 1.1 Основна характеристика Ajax StarterKit White [8]

Модель центрального блоку	Ajax Hub
Частота GSM мережі, МГц	850/900/1800/1900
Максимальна відстань між датчиками і центральним блоком, м	2000
Кількість бездротових/дротових зон:	100
Максимальна кількість пристроїв, що підключаються	100
Час автономної роботи, год:	до 12
Ємність вбудованого/зовнішнього акумулятора, мА	2000
Діяльність детектування руху, м:	12
Поріг спрацьовування датчик відкриття, см	2

Система охоронної сигналізації Tiras — це надійне рішення українського виробництва, яке призначене для захисту житлових, комерційних та промислових об'єктів. В основі функціонування систем Tiras лежать дротові та бездротові сповіщувачі, центральні прилади керування та модулі розширення, що забезпечують комплексний підхід до безпеки (рис. 1.2) [9].



Рисунок 1.2 – Orion NOVA X. Basic kit

Компанія «Tiras» розробляє та виготовляє високоякісне обладнання для пожежної та охоронної сигналізації, включаючи контрольні панелі, сирени, датчики руху, диму, витоку газу тощо. Системи Tiras активно впроваджуються в офісах, державних установах, навчальних закладах та житлових будинках. Особливістю продукції є надійність, відповідність європейським стандартам, а також можливість інтеграції з системами відеоспостереження та автоматизації [10].

Таблиця 1.2 – Характеристика Basic kit

Кількість бездротових датчиків,	64
Діапазон частот радіосигналу SRD, МГц	868.0-868.6
Потужність передавача SRD, мВт, не більше	25
Максимальна ширина смуги частот каналу, кГц, не більше	
Канали зв'язку з ПЦС та Tiras CLOUD II	2G (EGSM900/DCS1800), Wi-Fi (802.11 b/g/n)
Діапазон частот радіосигналу Wi-Fi, МГц	2400-2483.5
Час роботи, год.	24
Дальність виявлення руху, м	12
Поріг спрацьовування датчик відкриття, мм	10

До переваг систем Tiras можна віднести доступну ціну в порівнянні з іноземними аналогами, підтримку українською мовою, технічну підтримку в Україні та широкий асортимент продукції. Пристрої добре адаптовані до вітчизняних умов експлуатації, зокрема – електромереж та середовища.

Серед недоліків слід згадати:

- більш складне налаштування у порівнянні з сучасними бездротовими системами,
- віддалене керування через застосунок реалізовано лише в деяких моделях,
- високу вартість обладнання,
- обмежену можливість розширення системи за рахунок зовнішніх датчиків або інтеграції з іншими технологіями,
- відсутність вбудованої сирени,
- відсутність входів для шлейфів дротяних датчиків,

Самі датчики класифікуються за типом впливу, на який вони реагують. Найпоширенішими є об'ємні інфрачервоні (ІЧ-датчики), магнітоконтатні (геркони), акустичні, вібраційні, ультразвукові, променеві, ємнісні, а також датчики з направленою діаграмою виявлення.

Деякі пристрої мають просту конструкцію та легко встановлюються самостійно, тоді як інші потребують професійного монтажу. Врахування цього фактора є важливим етапом у процесі вибору охоронної системи, оскільки від правильності установки залежить її ефективність і надійність.

1.2 Класифікація та принципи роботи охоронних систем

Принцип роботи всіх охоронних сигналізаційних систем загалом однаковий і відрізняється лише типом та кількістю датчиків. Датчики сприймають певні зміни в навколишньому середовищі та передають сигнал на головну панель. Вона, своєю чергою, може активувати звукові та світлові оповісники, сповістити власника або передати сигнал на пульт охорони.

Варто розуміти, що стандартні системи сигналізації не зупиняють зловмисників, а лише попереджають власника, оточуючих або службу охорони про потенційну загрозу. Виняток становлять спеціалізовані охоронні системи, які використовуються в банках, фінансових установах, музеях та інших місцях збереження цінностей. Такі системи можуть автоматично блокувати вікна й двері, активувати захисні механізми, а в деяких випадках навіть створювати фізичні перешкоди, наприклад, опускати захисні ворота або змінювати умови в приміщенні.

Комплектація сигналізаційних систем може включати різні типи датчиків: відкриття дверей і вікон, розбиття скла, руху. Додатково система може бути оснащена датчиками пожежної безпеки (задимлення, температури), затоплення, витоку газу та тривожною кнопкою. Вибір конкретної конфігурації залежить від типу об'єкта, особливостей приміщення та вимог замовника.

Вибір конкретної системи залежить від характеристик об'єкта охорони та потреб власника — від багатофункціональних комплексів до вузькоспеціалізованих рішень. Крім того, сигналізації різняться за ступенем захисту як самого об'єкта, так і системи від можливих збоїв чи зловмисного втручання. Розглянемо основні класифікації охоронних сигналізацій [11].

Класифікація за видом об'єкта охорони:

- охоронна сигналізація для приватного будинку, дачі, офісу.
(включаючи прилеглі території);
- охоронна сигналізація для банківських установ;
- охоронна сигналізація для приміщень музеїв;
- охоронна сигналізація для військової інфраструктури;
- охоронна сигналізація для складських і промислових приміщень.

Таке розділення дозволяє створювати спеціалізовані рішення з урахуванням специфіки об'єкта охорони та рівня потенційних загроз. Це забезпечує ефективність захисту для кожного конкретного типу об'єкта.

Класифікація за тим, що розцінюється як загроза:

- сигналізація від злому і проникнення – оснащена датчиками, які реагують на рух в будинку (або квартирі) і прибудинкової території, розбиття вікон, відкривання дверей та інші дії пов'язані з проникненням зловмисників на територію володіння;
- протипожежна сигналізація – датчики системи повідомляють про задимлення приміщення, різкому підйомі температури, можуть повідомляти про місце загоряння і включати систему тривоги для евакуації;
- захист від чадного газу – датчики заміряють концентрацію небезпечних речовин в повітрі і повідомляють про витік власнику, система може бути частиною протипожежної сигналізації;
- захист від затоплення приміщення – датчики сигналізують про прориви труб, а також протечках пральних і посудомийних машин;
- комбінована система – включає в себе всі або частину датчиків для захисту від загроз злому, пожежі, витоку води або чадного газу. На даний момент, найпопулярніший вид системи.

Завдяки цій класифікації можна підібрати систему, що найбільш точно відповідає потребам користувача. Комбіновані рішення дозволяють досягти максимального рівня безпеки шляхом багатofакторного моніторингу загроз [11].

Класифікація за способом оповіщення власника:

- сигналізація, що функціонує без каналу зв'язку з власником, працює в автономному режимі та сповіщає про загрозу виключно локальними засобами оповіщення, такими як звукова сирена чи сигнальна лампа, сигналізація на телефон власника;
- сигналізація з GSM каналом зв'язу – зв'язується з власником через функцію автодозвону, та відправки СМС повідомлень;
- сигналізація з каналом зв'язку через Ethernet – тримає зв'язок з власником через інтернет-з'єднання.
- супутникова сигналізація – використовується в основному для

автомобілів разом з GPS-маячком і протиугінною системою, може також бути пов'язана з охороною компанією [11].

Спосіб оповіщення визначає, наскільки оперативно користувач дізнається про загрозу. У сучасних системах часто комбінуються кілька каналів зв'язку, що підвищує надійність та зручність використання.

1.3 Порівняння основних типів охоронних сигналізацій

Залежно від способів оповіщення існує три основні види охоронної сигналізації:

- автономна;
- пультова;
- GSM-сигналізація.

Автономна сигналізація

Автономна сигналізація працює на принципі відсутності зовнішнього підключення і активує звукове або світлове оповіщення у разі виникнення небезпечної ситуації. Це дає змогу привернути увагу людей, таких як поліція або сусіди. Переваги цієї системи включають її автономність, низьку вартість і можливість установки на віддалених об'єктах без необхідності підключення до зовнішніх мереж. Проте система має і свої недоліки: вона не дає гарантій безпеки, тому що залежить від реакції оточуючих, а також може бути легко відключена зловмисниками. У результаті, для ефективного використання автономної сигналізації важливо забезпечити певний рівень нагляду і реагування з боку власників або оточення. Автономність полягає в самостійному і незалежному контролі на об'єкті, що охороняється [12].

Переваги:

- Психологічний вплив на зловмисників: Завдяки звуковому або світловому оповіщенню, зловмисник може відчувати, що він перебуває під контролем, що підвищує ймовірність його відмови від злочину.
- Низька вартість експлуатації: Відсутність абонентської плати, де

сплачується лише вартість обладнання та встановлення, робить систему доступною для багатьох користувачів.

- Автономність: Можливість встановлення в місцях без доступу до зовнішніх мереж або зв'язку (дачі, котеджі), де інші типи сигналізацій можуть бути менш ефективними.

- Простота установки та експлуатації: Відсутність складних підключень і обслуговування дозволяє швидко налаштувати систему.

Недоліки:

- Довгий час спрацьовування: Після спрацьовування сигналізації потрібен час на реакцію людей, що може бути критичним для запобігання злочину.

- Легкість відключення: Зловмисники можуть відключити систему, наприклад, перекусивши дроти або зламавши її компоненти.

- Відсутність гарантії безпеки: Автономна сигналізація не гарантує цілісність майна, оскільки її спрацьовування залежить від реакції оточення, і не завжди є люди, які вчасно помітять сигнал або зможуть реагувати.

- Невизначеність реакції: Немає гарантії, що сигнал буде почутий або побачений, що може дозволити зловмисникам продовжити свою діяльність.

Пультова сигналізація

Пультова охорона є більш надійним і розповсюдженим типом сигналізації, порівняно з автономною. Вона передбачає підключення охоронного обладнання до центрального пульта, що здійснює постійний моніторинг. У разі спрацьовування датчиків, які фіксують злом, пожежу або інші небезпеки, сигнал негайно передається на пульт, і оперативна група виїжджає на місце події. Також власники об'єкта отримують сповіщення про тривогу. Це забезпечує швидке реагування, підвищує рівень безпеки та дає гарантію, що загроза буде нейтралізована в найкоротші терміни [13].

Переваги:

- Швидке реагування: Пультова охорона забезпечує миттєву передачу

сигналу про небезпеку на центральний пульт, що дозволяє оперативно реагувати на ситуацію.

- Надійність: Система постійно знаходиться під контролем, що зменшує ризик відключення чи несанкціонованого доступу до сигналізації.
- Професійне реагування: У разі тривоги виїжджає спеціалізована оперативна група, що дозволяє оперативно вжити заходів для нейтралізації загрози.
- Безпека майна: Оскільки пультава охорона забезпечує постійний моніторинг, ризик успішного злочину значно знижується.
- Інтеграція з іншими системами: Пультава охорона може бути інтегрована з іншими системами безпеки, такими як відеоспостереження чи контроль доступу.

Недоліки:

- Вартість: Пультава охорона є дорожчою за автономну сигналізацію через необхідність підключення до центрального пульта, що передбачає додаткові витрати на абонентську плату, установку та обслуговування.
- Залежність від зовнішнього пульта: Якщо виникнуть проблеми з комунікацією між об'єктом і пультом охорони, система може виявитися неефективною.
- Час реагування: Хоча система і забезпечує швидке реагування, все ж сам процес виїзду оперативної групи займає час, що дозволяє зловмисникам діяти до їхнього прибуття.
- Можливість шахрайства: Висококваліфіковані злочинці можуть спробувати перехопити сигнал або відключити систему перед її спрацюванням.
- Залежність від постачальника послуг: У разі проблем з пультом або технічного обслуговування об'єкта необхідно звертатися до постачальника послуг, що може призвести до певних затримок.

GSM-сигналізація

GSM-сигналізація набирає популярності завдяки своїй ефективності, простоті встановлення і доступній ціні. Це бездротова система, яка передає сигнал

тривоги через мобільний зв'язок. Основними складовими є центральний блок управління та датчики, які реагують на зміни в оточенні, наприклад, на проникнення. Її застосовують для охорони різноманітних об'єктів, таких як квартири, дачі, офіси або склади. Всі тривожні сигнали надходять на телефон власника або на пульт охорони через дзвінки або SMS-повідомлення. Це дозволяє оперативно відреагувати на ситуацію, навіть якщо об'єкт знаходиться далеко від користувача [14].

Переваги:

- Відсутність дротового підключення: Завдяки використанню мобільного зв'язку, система не потребує складного дротового монтажу, що спрощує установку та обслуговування.
- Мобільність: Її можна встановлювати в різноманітних місцях, зокрема на віддалених об'єктах, де немає можливості підключення до фіксованих ліній.
- Оперативне сповіщення: Сигнали про тривогу надходять на мобільний телефон або на пульт охорони через дзвінки або SMS, що дозволяє швидко реагувати на небезпеку.
- Доступна вартість: GSM-сигналізація має порівняно низьку вартість встановлення та обслуговування порівняно з іншими типами охоронних систем.
- Широкий діапазон застосування: Ідеально підходить для охорони квартир, дач, офісів, складів та інших об'єктів різного типу.

Недоліки:

- Залежність від мобільного зв'язку: У разі відсутності мобільного покриття або проблем з мережею сигналізація може не спрацювати, що є значним недоліком в ізольованих місцях.
- Можливість перехоплення сигналу: У разі використання старих мобільних технологій (2G, 3G) можлива спроба глушіння або перехоплення сигналу, хоча в нових системах використовується більш захищене з'єднання.
- Обмежена зона покриття: Якщо сигналізація налаштована на певну

зону або кілька мобільних операторів, збої в покритті або у виборі оператора можуть призвести до неефективності роботи системи.

– Не завжди точне сповіщення: SMS або дзвінки можуть бути не завжди миттєвими, що може затримати своєчасну реакцію на загрозу.

– Залежність від джерела живлення: Хоча GSM-сигналізація зазвичай має вбудований акумулятор для резервного живлення, у разі тривалого відключення електрики або несправності батареї сигналізація може бути неефективною [14].

У результаті аналізу існуючих рішень охоронних сигналізацій можна виокремити основні типи систем, що найчастіше застосовуються в різних умовах. Вони відрізняються за способом передачі сигналу, реакцією на загрозу та призначенням. Нижче наведено порівняльну таблицю, яка узагальнює ці характеристики (таблиця 1.3).

Таблиця 1.3 – Порівняння типів сигналізацій

Тип сигналізації	Канал зв'язку	Реакція	Призначення
Автономна	Відсутній	Сирена	Будинки
GSM	GSM, SMS	Оповіщення власника	Офіси, квартири
Пультова	Радіоканал або Інтернет	Виїзд охорони	Банки, великі об'єкти

Як видно з таблиці, кожен тип сигналізації має свої переваги та сфери доцільного застосування. Такий підхід до класифікації дозволяє обрати оптимальну систему відповідно до конкретних умов експлуатації та рівня необхідного захисту.

1.4 Огляд та принцип дії основних типів сенсорів

Сучасні охоронні системи використовують різноманітні датчики, які забезпечують виявлення загроз різного характеру — від вторгнення до пожежі чи пошкодження майна. Кожен тип датчика має власний принцип роботи, зону

покриття, чутливість та особливості застосування. Знання їх переваг і обмежень дозволяє ефективно проєктувати системи захисту відповідно до специфіки об'єкта.

Інфрачервоні (ІЧ) датчики руху, відомі також як об'ємні датчики, працюють на основі фіксації теплового випромінювання (рис. 1.3). Головним чутливим елементом такого пристрою є PIR-сенсор, який сприймає зміни температурного фону. Лінза Френеля допомагає розбити зону контролю на кілька секторів, і коли теплова пляма переміщується між ними, датчик фіксує рух і активує тривогу [15].

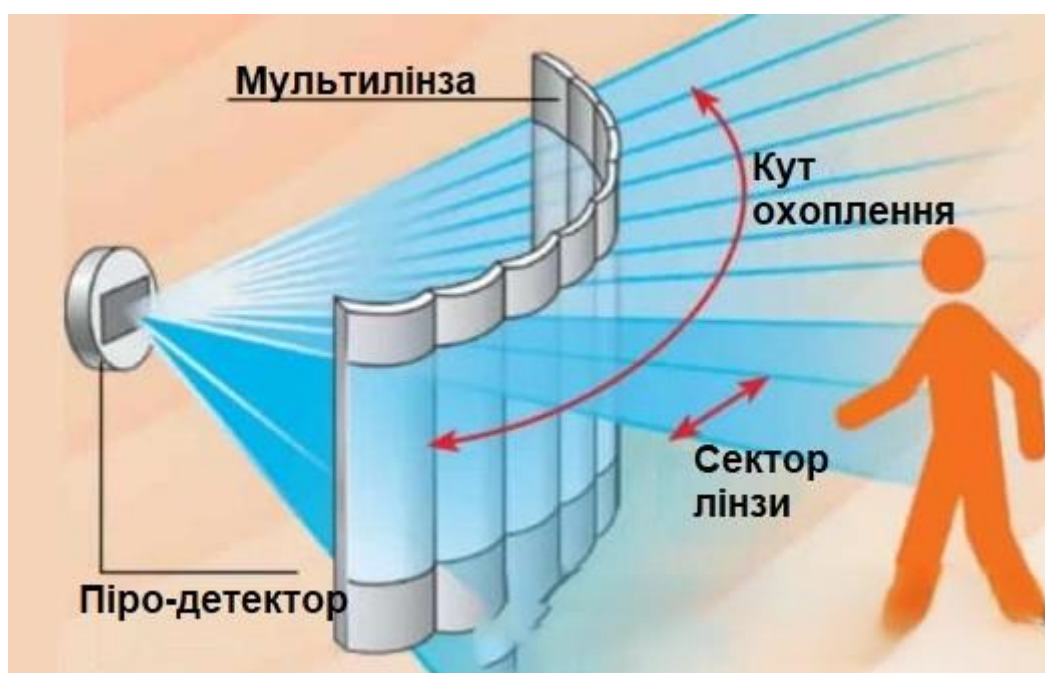


Рисунок 1.3 – Принцип роботи датчиків руху

Деякі моделі здатні відрізняти людину від домашніх тварин, аналізуючи розмір і характер теплового випромінювання. Завдяки доступній ціні та ефективності ці датчики широко використовуються в охоронних системах квартир і приватних будинків (рис. 1.4). Проте вони мають певні обмеження: зловмисник може використати теплоізоляційний матеріал або уникнути зони покриття датчика, щоб залишитися непоміченим. Тому в системах безпеки PIR-датчики часто комбінуються з іншими сенсорами, такими як магнітоконтактні або ультразвукові, що дозволяє підвищити надійність охоронної сигналізації.



Рисунок 1.4 – PIR-датчики

Магнітоконтактні датчики, також відомі як геркони, встановлюються на дверях та вікнах і служать для фіксації їх відкриття або закриття (рис. 1.5).



Рисунок 1.4 – магнітоконтактні датчики

Принцип роботи заснований на взаємодії двох компонентів, магніта та геркона: магніт встановлюється на рухомій частині (наприклад, дверях або вікні), а геркон — на нерухомій. Коли магніт віддаляється від геркона, зникає контакт, датчик передає сигнал (рис. 1.5)[16].

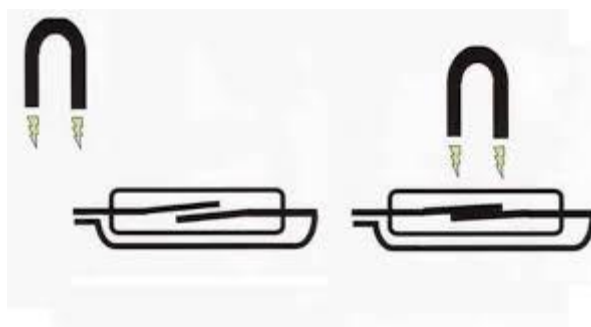


Рисунок 1.5 – Принцип роботи магнітоконтактного датчика

Ці датчики є доступними за ціною, надійними і мають мінімальне споживання електроенергії. Однак вони мають деякі обмеження, оскільки не здатні виявити проникнення через інші шляхи, такі як вентиляційні шахти або розбиття скла без відкриття рами. Для підвищення ефективності охоронної системи магнітоконтактні датчики часто комбінують з іншими типами сенсорів, наприклад, акустичними датчиками, що дозволяє забезпечити комплексний захист об'єкта.

Акустичні датчики спеціалізуються на виявленні різких звуків, таких як звук розбитого скла (рис. 1.6).



Рисунок 1.6 – Акустичний датчик

Вони оснащені мікропроцесором, який дозволяє точно аналізувати звукові хвилі, розрізняючи їх за характерними ознаками. Завдяки цьому, акустичні датчики можуть ефективно відрізняти розбиття скла від інших різких звуків, що значно знижує ймовірність помилкових спрацьовувань (рис. 1.7) [17].

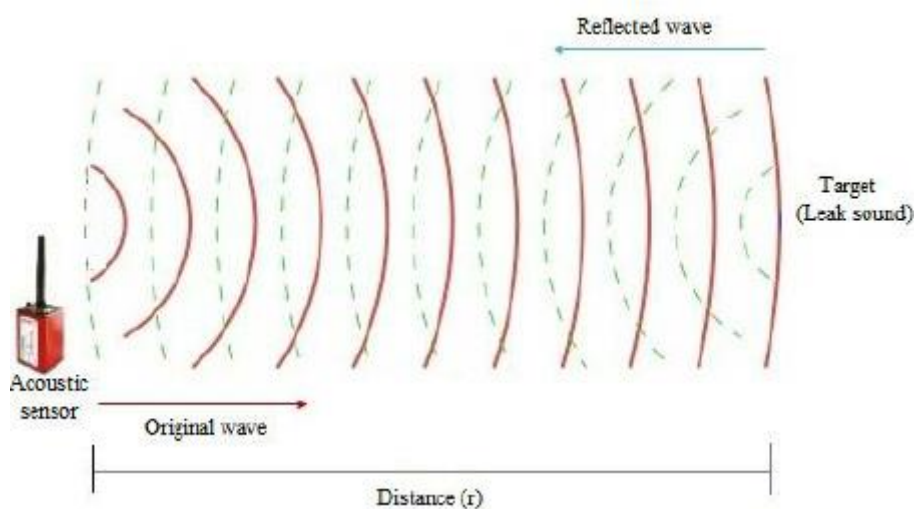


Рисунок 1.7 – принцип роботи акустичного датчика

Вони також зберігають звукові сигнатури різних типів скла, таких як звичайне, армоване або триплекс, що підвищує точність виявлення порушень.

Ультразвукові датчики функціонують на основі принципу локатора, випромінюючи ультразвукові хвилі, які відбиваються від рухомих об'єктів і повертаються до датчика (рис. 1.8).



Рисунок 1.8 – ультразвуковий датчик

Зміна частоти відбитих хвиль, що виникає через рух об'єкта, відповідно до закону Доплера, служить сигналом для активації датчика (рис 1.9).

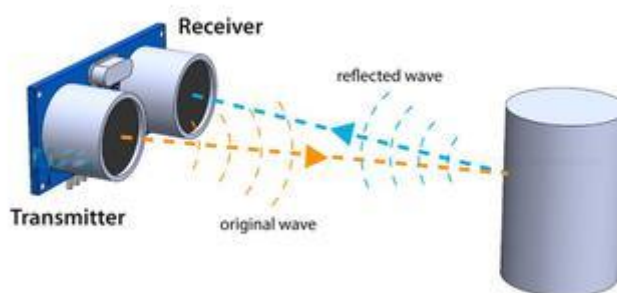


Рисунок 1.9 – принцип роботи ультразвукового датчика

Це дозволяє виявляти рух об'єктів навіть у складних умовах, таких як великі промислові приміщення або довгі коридори, де інші типи датчиків можуть бути менш ефективними. Ультразвукові датчики є надзвичайно корисними в таких середовищах, де необхідна точність і стабільність спостереження за великою площею [18].

Фотоелектричні (променеві) датчики складаються з передавача і приймача світла, які створюють невидимий промінь (рис. 1.10).



Рисунок 1.10 – Фотоелектричні дачики

Коли цей промінь переривається, наприклад, при проходженні людини або іншого об'єкта, датчик спрацьовує і передає сигнал [19] (рис. 1.11).

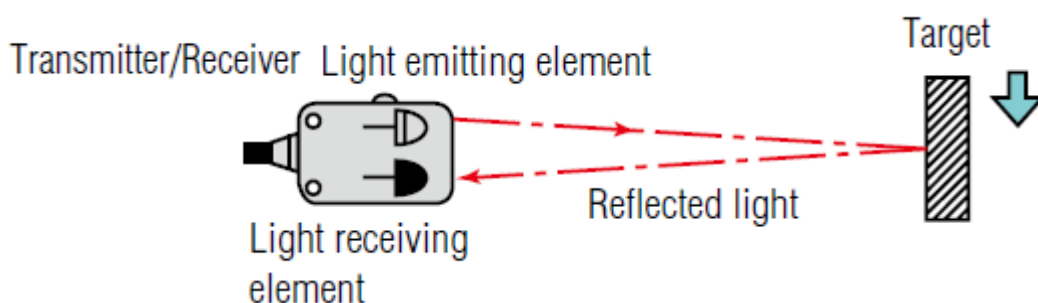


Рисунок 1.11 – принцип роботи фотоелектричного дачика

Це дозволяє ефективно охороняти великі простори, зазвичай по периметру об'єкта. Вони можуть працювати в будь-яких погодних умовах, але потребують точного налаштування для запобігання помилкових спрацьовувань.

Вібраційні датчики реагують на вібрації, що виникають при спробах проникнення через стіни, сейфи, вікна, підлоги та стелі (рис. 1.12).



Рисунок 1.12 - Вібраційний дачики

Вони чутливі до змін, що виникають при механічному впливі, і є надзвичайно корисними для захисту від фізичних пошкоджень об'єкта (рис. 1.13)[20].

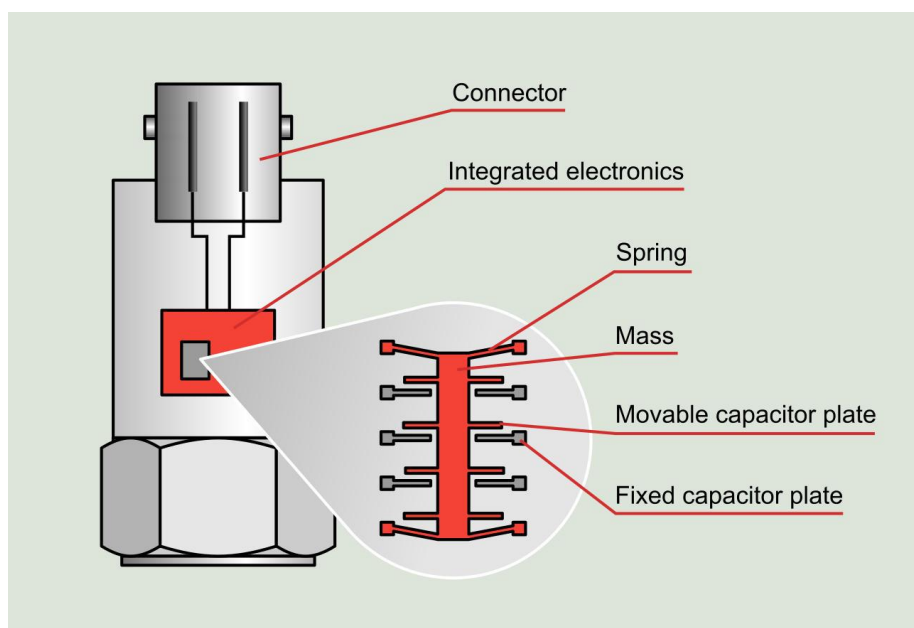


Рисунок 1.13 – принцип роботи вібраційного датчика

Однак налаштування таких датчиків може бути складним, і вони можуть давати помилки через вплив інших вібрацій, таких як рух транспорту. Тому ці датчики часто поєднують з іншими типами охоронних засобів для досягнення найкращого результату в системах безпеки.

Ємнісні датчики застосовуються для охорони особливо цінних предметів, таких як сейфи або витвори мистецтва (рис. 1.14).



Рисунок 1.14 - Датчик ємності

Вони працюють за принципом створення електричного поля навколо об'єкта, що охороняється. Коли в це поле потрапляє сторонній предмет, його електрична ємність змінюється, що викликає спрацювання сигналізації (рис. 1.15)[21].

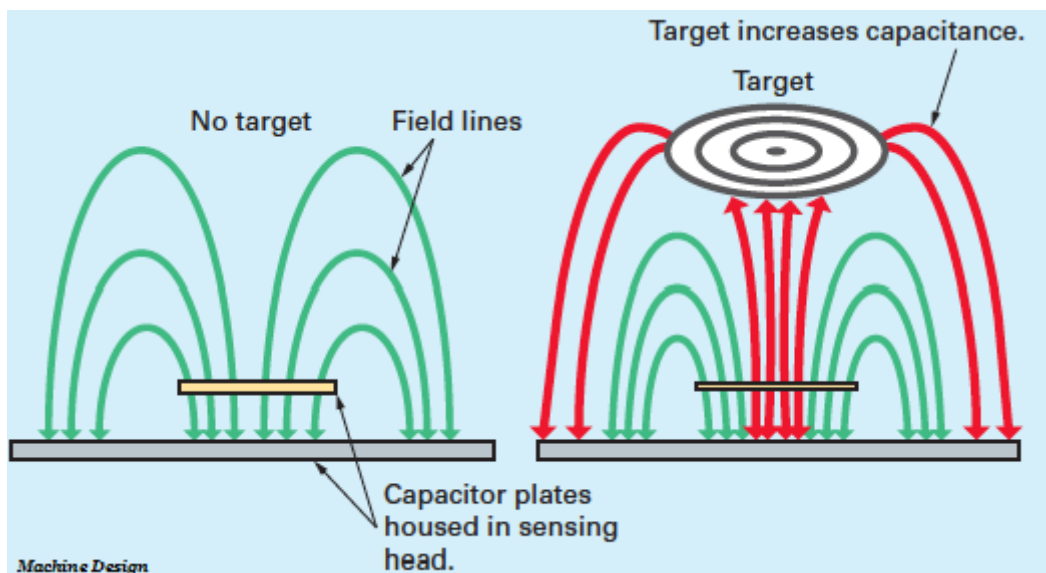


Рисунок 1.14 – принцип роботи датчика ємності

Однак ці датчики мають певні недоліки: вони складні в налаштуванні, мають великі габарити і високу вартість, тому застосовуються здебільшого для охорони найбільш коштовних об'єктів.

1.6 Висновки та постановка задач

У даному розділ було проаналізовано компоненти та методи програмно-апаратних комплексів сигналізації. Визначено що для ефективної роботи сигналізаційних систем важливим є правильний вибір надійних компонентів. Апаратна частина повинна бути гнучкою для інтеграції з різними типами датчиків і контролерів, забезпечуючи високу точність виявлення загроз. Існуючі методи передачі сигналів (автономні, пультові та GSM-сигналізації) мають свої переваги та недоліки, що дозволяє комбінувати їх для забезпечення швидкості реагування і надійності. Вибір відповідного методу передачі сигналу залежить від умов експлуатації і вимог до безпеки. Аналіз різних типів датчиків підтверджує, що їх різноманіття дозволяє створювати багатофункціональні та ефективні системи охорони.

Існуючі реалізації програмно-апаратних комплексів сигналізації з віддаленим керуванням, які використовують бездротові технології, показали високу ефективність у забезпеченні охорони та зручності використання. Сучасні

системи з можливістю віддаленого оповіщення значно підвищують рівень безпеки. Проте важливо забезпечити надійний захист від зовнішніх впливів і належне збереження даних.

Враховуючи проаналізовані варіанти, було обрано шлях створення програмно-апаратного комплексу охоронної сигналізації саме на основі платформи Arduino з модулем ESP, що дозволяє реалізувати віддалене керування та сповіщення через Telegram.

2 ПРОЄКТУВАННЯ СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ З ВІДДАЛЕНИМ КЕРУВАННЯМ ТА ОПОВІЩЕННЯМ

У цьому розділі розглядається проєктування програмно-апаратного комплексу охоронної сигналізації, призначеного для виявлення несанкціонованого проникнення та інформування користувача про події через віддалені канали зв'язку. Основу системи становить мікроконтролер Arduino з вбудованим Wi-Fi-модулем ESP, що забезпечує інтеграцію з месенджером Telegram для зручного керування.

Проєктування охоплює вибір компонентів системи, таких як датчики руху, геркони та звукові сигнальні пристрої, а також модулі для передавання повідомлень. Окрему увагу приділено аналізу сценаріїв роботи системи, алгоритмам взаємодії між складовими та обґрунтуванню вибору мов програмування. Також у розділі подано структурну та електричну схему майбутньої реалізації.

2.1 Аналіз можливості вдосконалення системи сигналізації

У сучасних умовах, коли безпека житла та офісних приміщень стає пріоритетом для багатьох громадян, особливу актуальність набувають прості, недорогі та надійні охоронні системи. Одним з найефективніших підходів до захисту є впровадження сигналізаційних пристроїв, які здатні швидко реагувати на спроби несанкціонованого доступу.

У межах цієї роботи було вирішено зосередитися саме на розробці сигналізації, а не, наприклад, відеоспостереженні чи лише на фізичних елементах захисту, такі як замки або ролетні системи. Основною перевагою сигналізаційної системи є її оперативна реакція на загрозу та можливість миттєвого інформування власника через мобільний інтерфейс. Зокрема, запропонована система відрізняється мобільністю, простотою налаштування, а головне — здатністю працювати автономно без необхідності постійного спостереження.

Система базується на мікроконтролері Arduino з вбудованим ESP-модулем, що дає змогу реалізувати функцію віддаленого керування та оповіщення через Telegram-бота.

В основі її дії — реагування на рух об'єкта в зоні спостереження (за допомогою інфрачервоного датчика HC-SR501) та відкриття дверей або вікон (виявлення за допомогою геркона). У разі спрацювання одного з датчиків — система активує звукову сигналізацію та надсилає повідомлення власнику через Telegram.

Обраний принцип дії має кілька переваг:

- ІЧ-датчик HC-SR501 дозволяє точно виявляти рух на відстані до 3–5 метрів у секторі до 120°, що є оптимальним для більшості приміщень.
- Герконовий датчик забезпечує простий та надійний спосіб контролю відкриття дверей або вікон, що особливо важливо для виявлення вторгнень.
- Telegram-бот не потребує створення окремого мобільного застосунку, несе мінімальні витрати на реалізацію та є зручним у використанні.

У порівнянні з альтернативними методами сигналізації — такими як лазерні бар'єри чи системи з відеоаналітикою — обране рішення вигідно вирізняється простотою монтажу, невеликою вартістю, гнучкістю налаштувань і можливістю розширення функціоналу. Наприклад, на відміну від систем з камерами, запропонована конструкція не потребує складного зберігання відеоданих або постійного інтернет-з'єднання високої пропускної здатності.

Крім того, ця система є повністю кастомізованою, а отже, користувач може легко додавати нові функції, змінювати логіку сповіщення або тип датчиків відповідно до потреб конкретного об'єкта.

Таким чином, вибір принципу дії, технологій і компонентів був зумовлений поєднанням таких факторів, як надійність, простота реалізації, доступність, енергоефективність і зручність використання. Запропонований пристрій стане гарною альтернативою комерційним охоронним системам у випадках, коли потрібне недороге, але ефективне рішення.

Програмно-апаратний комплекс сигналізації з можливістю віддаленого керування особливо актуальна в умовах зростання кількості квартирних крадіжок, несанкціонованого проникнення до офісів, дачних будинків, складів тощо. У багатьох випадках власники не мають можливості перебувати на об'єкті цілодобово, а тому потребують надійного засобу оповіщення про загрозу в реальному часі.

Розроблена система дозволяє:

- оперативно отримувати сповіщення про вторгнення через Telegram, незалежно від місця знаходження користувача;
- здійснювати активацію чи деактивацію програмно-апаратного комплексу сигналізації дистанційно;
- отримувати ідентифікацію джерела спрацювання

Таким чином, запропоноване рішення може значно підвищити рівень безпеки об'єкта, дозволяючи своєчасно реагувати на загрози, не вдаючись до дорогих комерційних систем.

2.2 Вибір компонентів для програмно-апаратного комплексу сигналізації

На етапі проектування програмно-апаратного комплексу сигналізації важливо ретельно підібрати апаратні та програмні компоненти, які забезпечать надійну та стабільну роботу пристрою в реальних умовах.

Основними завданнями, які повинні виконувати обрані компоненти, є:

- виявлення вторгнення до охоронюваного приміщення (наприклад, відчинення дверей або виявлення руху),
- генерація звукового сигналу тривоги,
- передавання сповіщення власнику через інтернет-з'єднання,
- забезпечення можливості віддаленого керування системою через Telegram-бота.

Для досягнення цих цілей у системі використовуються такі ключові складові:

В якості основної плати на якій буде проектуватися програмно-апаратний комплекс сигналізації буде плата UNO+Wifi R3 ATmega328P+ESP8266 8Mb flash, USB-TTL CH340G, Micro-USB [22] (рис. 2.1).



Рисунок 2.1 – UNO+Wifi R3

Основною перевагою цієї платформи є наявність на одній платі одночасно мікроконтролера ATmega328P та модуля ESP8266, які вже розпаяні та з'єднані між собою. Це дозволяє уникнути додаткових труднощів, пов'язаних із ручним підключенням одного модуля до іншого, забезпечуючи готове й стабільне з'єднання.

У випадку, якщо використовувати окрему плату Arduino та окремий модуль ESP, можуть виникнути труднощі як на апаратному, так і на програмному рівні. Зокрема, на апаратному рівні можливі проблеми через різну логічну напругу: Arduino працює з рівнем 5 В, тоді як ESP — з 3.3 В, що потребує використання додаткових перетворювачів рівнів. На програмному рівні можливі ускладнення через різні швидкості передавання даних, що може призвести до помилок у

взаєморозумінні між модулями. Якщо швидкості передачі не будуть узгоджені, пристрої не зможуть коректно обмінюватися інформацією.

Табличка 2.1 – Характеристики плати [23]

Параметр	Значення
Мікроконтролер	ATmega328P
USB-UART перетворювач	CH340G
Wi-Fi контролер	ESP8266
Флеш-пам'ять ESP8266	8 Мбіт
Робоча напруга	5 В
Вхідна напруга	7 – 12 В
Рекомендована вхідна напруга	7 – 9 В
Цифрові входи/виходи	14 (з них 6 підтримують PWM)
Аналогові входи	6
Максимальний постійний струм на пін	40 мА
Максимальний струм на виході 3.3 В	50 мА
Постійна пам'ять (Flash)	32 КБ
Оперативна пам'ять (SRAM)	2 КБ
Пам'ять для збереження даних (EEPROM)	1 КБ
Тактова частота	16 МГц

Одним із ключових елементів системи виявлення вторгнень є інфрачервоний датчик руху HC-SR501 (рис. 2.2). Цей модуль використовується для детекції присутності або руху людей у контрольованій зоні.



Рисунок 2.2 – HC-SR501

Інфрачервоний датчик руху HC-SR501, також званий PIR-сенсором, є пристрій, що реагує на рух людей в навколишньому просторі. Датчик працює за принципом вимірювання рівня інфрачервоного випромінювання, що випромінюється живими істотами. Також HC-SR501 може реагувати на інші об'єкти, що випромінюють тепло, особливо якщо їх температура змінюється. Сенсор HC-SR501 легко впроваджується у схеми на базі Arduino, AVR, PIC, ARM та інших мікроконтролерів [24].

PIR-датчик — це надійне рішення для контролю внутрішніх приміщень (наприклад, кімнат, коридорів), де не очікується руху без присутності людини.

Табличка 2.2 – Характеристика PIR-сенсора

Параметр	Значення
Модель	HC-SR501
Напруга живлення	4.5 – 20 В
Вихідний сигнал	TTL рівень: High (3.3 В) / Low (0 В)
Час затримки (затримка вимкнення)	5 – 200 с (налаштовується потенціометром)
Чутливість (відстань виявлення)	4 – 7 м (регулюється потенціометром)
Ефективний кут виявлення	<120°

У ролі датчика, що реагує на відкриття або закриття дверей, у системі буде використовуватись герконовий датчик (геркон) (рис 2.3).



Рисунок 2.3 – герконовий датчик

Такий тип датчика обрано завдяки його простій конструкції, високій надійності та перевіреним часом ефективності. На відміну від механічних перемикачів, геркони мають тривалий термін служби та не мають рухомих частин, що підвищує надійність [25].

Табличка 2.3 – Характеристики дачика

Параметр	Значення
Спосіб активації	Магнітне поле
Максимальний комутаційний струм	~100 мА
Максимальна комутаційна напруга	100 В постійного або змінного струму
Опір у замкнутому стані	~0.1 Ом
Відстань спрацювання	10 – 25 мм
Монтаж	Накладний або вбудований

Для виявлення звуків (шуму) в приміщенні у складі охоронної системи використовується звуковий датчик КУ-037 (рис. 2.4).

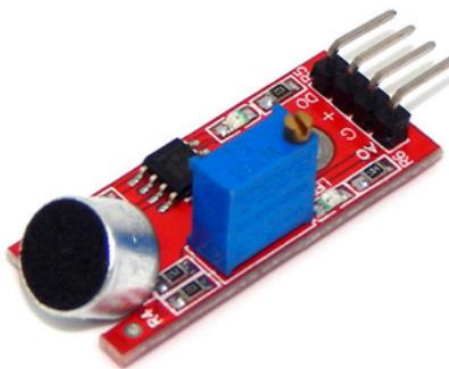


Рисунок 2.4 – КУ-037

Цей модуль дозволяє фіксувати підвищення рівня шуму, наприклад: гучні розмови, удари, кроки або звук розбитого скла. Завдяки високочутливому мікрофону та простоті інтеграції з мікроконтролерами (наприклад, Arduino), модуль є ефективним рішенням для аудіомоніторингу у приміщенні. У програмно-апаратному комплексі сигналізації його доцільно застосовувати як додатковий

рівень захисту, що може спрацювати у випадках, коли інші сенсори залишаються неактивними.

Таблиця 2.4 – Характеристики КУ-037 [26]

Параметр	Значення
Живлення	3.3 – 5 В
Тип мікрофона	Електретний мікрофон
Вихідні сигнали	Цифровий (D0) та аналоговий (A0)
Регулювання чутливості	Підлаштовується змінним резистором (потенціометром)

Модуль складається з чутливого датчика звуку, коли мембрана датчика коливається від звукової хвилі, змінюється його ємність, що призводить до зміни напруги на виході датчика звуку. Мікросхема компаратора використовується для визначення моменту перевищення порога гучності звуку.

2.3 Розробка алгоритму роботи програмно-апаратного комплексу сигналізації

Проектована програмно-апаратний комплекс сигналізації є автономним засобом технічного захисту, що базується на виявленні руху та несанкціонованого проникнення (рис 2.5). У своїй основі система використовує прості, але надійні компоненти — інфрачервоний датчик HC-SR501, герконовий датчик, звуковий датчик КУ-037, мікроконтролер Arduino Uno з вбудованим модулем ESP8266 та Telegram-бот для дистанційного керування і сповіщення.

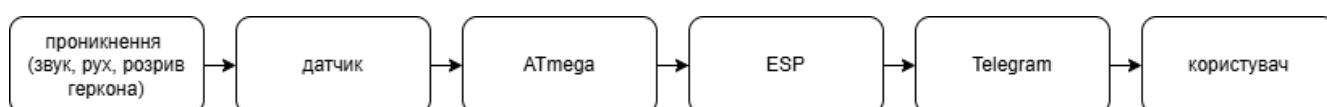


Рисунок 2.5 – проста блок-схема реагування на проникнення

Детальний покроковий розбір схеми алгоритму реагування на проникнення:

1. Крок – Виявлення загрози. Один із датчиків (руху, відкриття дверей або звуку) фіксує підозрілу активність у зоні, що охороняється.
2. Крок – Перевірка режиму охорони. Контролер перевіряє, чи система перебуває в активному режимі охорони (моніторинг увімкнено). Якщо сигналізація вимкнена — подальші дії не виконуються.
3. Крок – Активація тривоги. У разі активного режиму сигналізація переходить у тривожний стан:
4. Крок – Надсилення сповіщення. Через ESP-модуль надсилаються сповіщення до Telegram-бота:
 - Перше повідомлення – загальна інформація про тривогу;
 - Друге повідомлення – тип спрацювавшого датчика.
5. Крок – Перехід у режим утримання. Після фіксації та сигналу тривоги система переходить у режим утримання: на інші датчики до подальшої команди.
6. Крок – Очікування команди користувача. Система очікує нову команду від користувача через Telegram (наприклад, /on для повторного включення охорони). Без втручання користувача сигналізація залишається в режимі утримання.

Принцип дії програмно-апаратного комплексу сигналізації полягає у безперервному моніторингу середовища за допомогою датчиків. У разі фіксації загрози (наприклад, виявлення руху, відкриття дверей або звуку), система активує сирену та надсилає сповіщення користувачеві через Telegram про проникнення.

Сценарії активації та деактивації системи

Користувач має змогу дистанційно вмикати та вимикати охоронну систему через Telegram-бота. Для цього достатньо надіслати одну з передбачених команд:

- /on – увімкнути охоронний режим;
- /off – вимкнути охоронний режим;

У активному стані Arduino постійно аналізує сигнали з підключених датчиків. При виникненні події, яка розцінюється як загроза, система негайно активує звукову сирену та ініціює надсилення сповіщення в Telegram.

У неактивному режимі сигнали з датчиків ігноруються, і система перебуває в режимі очікування команд (рис 2.6).

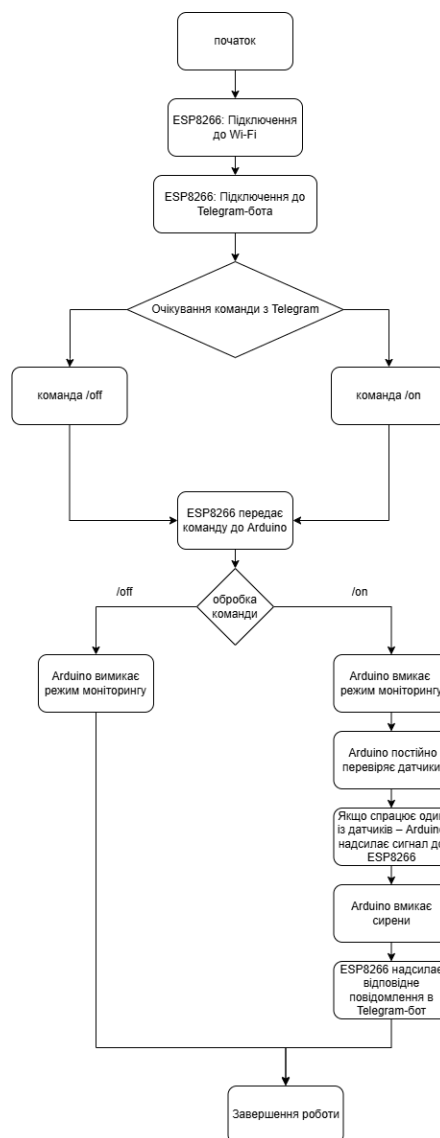


Рисунок 2.6 – блок-схема програмно-апаратного комплексу сигналізації

Детальний покроковий розбір блок-схема алгоритму охорони системи:

1. Крок – Початок роботи системи. Система запускається: Arduino та ESP8266 переходять у робочий режим.
2. Крок – Підключення ESP8266 до Wi-Fi. ESP-модуль встановлює з'єднання з локальною мережею для забезпечення доступу до Telegram.
3. Крок – Підключення до Telegram-бота. Після підключення до Інтернету ESP8266 ініціалізує з'єднання з Telegram-ботом, через якого буде здійснюватись керування.

4. Крок – Очікування команди з Telegram. Система очікує отримання керуючих команд від користувача. Доступні команди: /on – увімкнення моніторингу, /off – вимкнення.

5.1 Крок – Передача команди до Arduino. ESP8266 передає повідомлення Arduino про вимкнення моніторингу.

5.2 Крок – Arduino вимикає режим моніторингу. У цьому стані всі датчики ігноруються, тривоги не фіксуються.

6.1 Крок – Передача команди до Arduino. ESP8266 надсилає команду на Arduino про ввімкнення моніторингу.

6.2 Крок – Arduino активує режим моніторингу. Увімкнення режиму постійного аналізу показників з усіх підключених датчиків

7 Крок – Постійна перевірка датчиків. Arduino регулярно опитує всі датчики для виявлення змін, що можуть свідчити про проникнення.

8 Крок – Виявлення вторгнення. Якщо один із датчиків подає сигнал (тобто спрацював): Arduino розпізнає джерело події, формує відповідь для ESP8266.

9 Крок – Активація сирени. Arduino активує звукову сигналізацію (бузер), яка служить для локального попередження про проникнення.

10 Крок – Надсилання повідомлень у Telegram. ESP8266, отримавши дані від Arduino, надсилає: Повідомлення про тривогу , Повідомлення з типом спрацювавшого датчика.

11 Крок – Завершення роботи. Після обробки події система або: переходить у режим утримання, очікуючи подальшу команду, або продовжує моніторинг (залежно від реалізованої логіки коду).

Взаємодія компонентів системи

- Охоронна система складається з таких основних елементів:
- HC-SR501 датчик, який фіксує рух . При спрацюванні генерує високий логічний сигнал.
- Геркон магнітний контакт, який визначає відкриття дверей або вікон.
- ATmega + ESP8266 — обробляє сигнали з датчиків, виконує логіку керування

системою та надсилає сповіщення через Wi-Fi.

- П'єзосирена — забезпечує звукову сигналізацію при тривозі.
- Telegram-бот — дозволяє користувачу керувати програмно-апаратним комплексом сигналізації та отримувати повідомлення про події.

Усі компоненти взаємодіють за допомогою програмної логіки Arduino. ESP-модуль підключається до мережі Wi-Fi та зв'язується з Telegram API, забезпечуючи миттєву передачу інформації.

Алгоритм роботи Telegram-бота

Telegram-бот реалізує функції керування програмно-апаратним комплексом сигналізації та зворотного зв'язку. Його логіка роботи включає такі етапи:

- Користувач надсилає команду в Telegram-бот.
- ESP8266 отримує команду і передає її мікроконтролеру Arduino.
- Arduino оновлює стан системи (вмикає/вимикає охорону).
- У разі спрацювання датчика Arduino активує сирену та надсилає сигнал через ESP для повідомлення користувачу.
- Telegram-бот надсилає повідомлення про подію у чат користувача.

Завдяки Telegram-інтерфейсу не потрібна установка окремого застосунку, користувач взаємодіє із системою в зручному форматі, доступному з будь-якого пристрою з Інтернетом.

2.4 Обґрунтування вибору мов програмування

Для реалізації програмної частини програмно-апаратного комплексу сигналізації в даному проєкті було обрано мову програмування C/C++ у поєднанні із середовищем розробки Arduino IDE. Такий вибір зумовлений не лише технічними характеристиками обраної апаратної платформи Arduino Uno WiFi R3, а й загальними вимогами до надійності, швидкодії та ефективного використання обмежених ресурсів вбудованих систем.

Arduino — це апаратно-програмна платформа з відкритим вихідним кодом, що базується на мікроконтролерах, зокрема на популярному ATmega328P. Основна

мова програмування Arduino — це C++, яка дозволяє отримати прямий доступ до апаратних ресурсів, таких як порти введення/виведення, таймери, ПД (PWM), аналогові та цифрові входи/виходи. Це критично важливо для управління компонентами охоронної системи, зокрема датчиками [27] .

C++ забезпечує ефективне використання обмежених ресурсів мікроконтролера. Arduino Uno має сильно обмежений об'єм оперативної пам'яті та флеш-пам'яті, тож важливо писати код з урахуванням цих обмежень. C++ дозволяє оптимізувати об'єм програми та забезпечити високу швидкодію навіть на обмеженому обладнанні [28].

C++ також підтримує об'єктно-орієнтоване програмування, що дозволяє створювати модульну архітектуру коду. Це важливо для гнучкого масштабування системи, наприклад, при додаванні нових сенсорів або функцій, без необхідності переписувати всю систему з нуля [29].

Окрім технічних переваг, варто враховувати й підтримку з боку спільноти. Arduino IDE та мова C++ є надзвичайно поширеними в середовищі розробників вбудованих систем, а це означає наявність великої кількості бібліотек, документації. Наприклад, існують бібліотеки для роботи з ESP8266. Це значно пришвидшує розробку, дозволяє уникнути типових помилок та сфокусуватися на логіці системи.

Використання Arduino IDE як середовища розробки також є обґрунтованим: воно підтримує автоматичну компіляцію, завантаження прошивки на плату, має інтеграцію з великою кількістю плат і модулів, а також простий інтерфейс, що робить його зручним [30].

Таким чином, вибір C++ у поєднанні з Arduino IDE є оптимальним для розробки ефективного, розширюваного та надійної програмно-апаратного комплексу сигналізації.

Висновок до розділу 2

У даному розділі було здійснено всебічне проєктування системи сигналізації з віддаленим керуванням та оповіщенням, що ґрунтується на мікроконтролерній

платформі Arduino. Визначено обґрунтування доцільності розробки саме такої системи, враховуючи потребу у доступному, мобільному та кастомізованому рішенні для забезпечення базового рівня безпеки приміщень.

Проведено детальний вибір апаратних компонентів системи, зокрема було проаналізовано можливості мікроконтролера Arduino Uno WiFi R3, інфрачервоного датчика руху HC-SR501, геркона, звукового датчика KY-037. Обґрунтовано вибір саме цих компонентів на основі їхньої надійності, простоти інтеграції та відповідності вимогам до функціональності системи.

Окреслено логіку роботи сигналізації: від сценаріїв активації та деактивації до обміну даними між компонентами та взаємодії з Telegram-ботом. Також було аргументовано використання мови програмування C/C++ та середовища Arduino IDE, які забезпечують високий рівень контролю над апаратними ресурсами та зручність розробки.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС СИГНАЛІЗАЦІЇ З ВІДДАЛЕНИМ КЕРУВАННЯМ ТА ОПОВІЩЕННЯМ

У цьому розділі наведено процес реалізації програмно-апаратного комплексу сигналізації з функціями віддаленого керування та оповіщення. Представлено розроблений програмний код, описано особливості підключення та взаємодії компонентів системи, а також продемонстровано фізичну реалізацію прототипу.

Окрему увагу приділено тестуванню системи: описано методику перевірки, зафіксовано результати тестів та проаналізовано ефективність роботи пристрою в реальних умовах. Реалізація проєкту підтверджує життєздатність обраної концепції та її придатність для практичного використання в умовах побутової або офісної безпеки.

3.1 Реалізація програмного забезпечення програмно-апаратного комплексу сигналізації

Програмне забезпечення системи програмно-апаратний комплекс сигналізації реалізується за допомогою двох взаємопов'язаних програмних модулів: одного для мікроконтролера ESP8266, що відповідає за зв'язок із Telegram-ботом, і другого для мікроконтролера ATmega328P, який безпосередньо керує сенсорами та виконавчими пристроями. Комунікація між модулями здійснюється через послідовний інтерфейс UART.

Код для ESP8266

Імпорт бібліотек та оголошення констант

```
#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>
const char* ssid = "UnoWiFi";
const char* password = "basiscum";
#define BOT_TOKEN "YOUR_BOT_TOKEN"
#define CHAT_ID "YOUR_CHAT_ID"
```

Цей блок коду підключає потрібні бібліотеки для роботи Wi-Fi та Telegram API, а також оголошує константи для налаштування мережі та зв'язку з ботом.

- ESP8266WiFi.h — бібліотека для підключення ESP до Wi-Fi.
- WiFiClientSecure.h — бібліотека для HTTPS-з'єднань (обов'язкова для Telegram).
- UniversalTelegramBot.h — бібліотека для взаємодії з Telegram API.
- ssid, password — назва та пароль Wi-Fi мережі, до якої підключається ESP8266.
- BOT_TOKEN — токен Telegram-бота, отриманий у BotFather.
- CHAT_ID — ID користувача чи групи, куди надсилатимуться повідомлення.

Підключення до Wi-Fi

```
WiFi.begin(ssid, password);
while (WiFi.status() != WL_CONNECTED) {
    delay(500);
}
```

Цей блок відповідає за з'єднання ESP8266 з Wi-Fi мережею. Мікроконтролер очікує встановлення з'єднання перед продовженням виконання коду.

- WiFi.begin(ssid, password) — ініціює підключення до мережі Wi-Fi.
- WiFi.status() — перевіряє статус підключення.
- delay(500) — коротка пауза між перевітками.

Надсилання стартового повідомлення

```
bot.sendMessage(CHAT_ID, "Бот запущено! Введи /on або /off", "");
```

Після успішного підключення до мережі бот надсилає стартове повідомлення користувачу Telegram, інформуючи про готовність до роботи.

- bot.sendMessage(...) — функція надсилає повідомлення у чат Telegram.
- "Бот запущено!..." — текст повідомлення для користувача.

Обробка команд з Telegram

```
int numNewMessages = bot.getUpdates(bot.last_message_received + 1);
for (int i = 0; i < numNewMessages; i++) {
    String text = bot.messages[i].text;
    String chat_id = bot.messages[i].chat_id;
```

Цей блок перевіряє наявність нових повідомлень від користувача та зберігає їхній вміст.

- `bot.getUpdates(...)` — отримує нові повідомлення.
- `bot.messages[i].text` — текст повідомлення від користувача.
- `bot.messages[i].chat_id` — ідентифікатор чату, з якого надійшло повідомлення.

Реакція на команди `/on` та `/off`

```
if (text == "/on") {
  Serial.write('1');
  notificationsEnabled = true;
  bot.sendMessage(CHAT_ID, "Система моніторингу активована!", "");
}
if (text == "/off") {
  Serial.write('0');
  notificationsEnabled = false;
  bot.sendMessage(CHAT_ID, "Система моніторингу вимкнена.", "");
}
```

Блок реагує на команди керування сигналізацією. При `/on` вмикається система моніторингу, при `/off` — вимикається.

- `Serial.write('1')` — надсилає символ '1' на Arduino (включення системи).
- `Serial.write('0')` — надсилає символ '0' на Arduino (вимкнення системи).
- `notificationsEnabled` — логічна змінна, що дозволяє надсилання повідомлень про тривоги.

Прийом подій з Arduino

```
if (Serial.available()) {
  char signal = Serial.read();
  if (notificationsEnabled) {
    if (signal == 'A') bot.sendMessage(CHAT_ID, "🚨 ТРИВОГА!", "");
    else if (signal == 'R') bot.sendMessage(CHAT_ID, "👤 Рух виявлено", "");
    else if (signal == 'G') bot.sendMessage(CHAT_ID, "🔪 Геркон розімкнутий", "");
    else if (signal == 'S') bot.sendMessage(CHAT_ID, "🔊 Гучний звук виявлено", "");
    else if (signal == 'H') bot.sendMessage(CHAT_ID, "🛑 Режим утримання", "");
  }
}
```

ESP8266 постійно перевіряє, чи не надійшов сигнал з Arduino. Якщо надходить, то бот відповідно реагує, надсилаючи повідомлення в Telegram.

- `Serial.available()` — перевірка наявності вхідних даних.
- `Serial.read()` — зчитує один символ з UART.

- `signal == 'A'` — загальна тривога.
- `signal == 'R'` — рух виявлено (PIR).
- `signal == 'G'` — геркон розімкнутий.
- `signal == 'S'` — гучний звук.
- `signal == 'H'` — перехід у режим утримання.

Код для ATmega328P (Arduino Uno)

Оголошення пінів та змінних

```
#define PIR_PIN 2
#define REED_PIN 3
#define SOUND_PIN 4

#define LED_ON 5
#define LED_OFF 6
#define BUZZER 7
#define LED_HOLD 13

bool alertEnabled = false;
bool inHold = false;
bool holdMessageSent = false;
unsigned long holdStartTime = 0;

unsigned long monitoringStartTime = 0;
unsigned long ignoreTriggersUntil = 0;
const unsigned long IGNORE_DURATION = 3000;
```

Цей фрагмент оголошує пінові константи, булеві прапори стану та часові змінні для керування режимами програмно-апаратного комплексу сигналізацій.

- `PIR_PIN` — пін для ІЧ-датчика руху.
- `REED_PIN` — пін для геркона (контактний датчик відкриття).
- `SOUND_PIN` — пін для звукового датчика.
- `LED_ON`, `LED_OFF`, `LED_HOLD` — піни для світлодіодів: зелений, червоний та жовтий.
- `BUZZER` — пін зумера (звукове сповіщення).
- `alertEnabled` — прапор активності системи моніторингу.
- `inHold` — прапор, що вказує, чи активний режим утримання.
- `holdMessageSent` — запобігає повторному надсиланню повідомлення про утримання.

- `holdStartTime` — час початку режиму утримання.
- `monitoringStartTime` — час активації моніторингу.
- `ignoreTriggersUntil` — час, до якого ігноруються датчики після активації.
- `IGNORE_DURATION` — період ігнорування датчиків після активації (3 с).

Ініціалізація у `setup()`

```
void setup() {
    pinMode(PIR_PIN, INPUT);
    pinMode(REED_PIN, INPUT_PULLUP);
    pinMode(SOUND_PIN, INPUT);
    pinMode(LED_ON, OUTPUT);
    pinMode(LED_OFF, OUTPUT);
    pinMode(BUZZER, OUTPUT);
    pinMode(LED_HOLD, OUTPUT);
    Serial.begin(9600);
    Serial.println("Система моніторингу запущена...");
}
```

Цей блок виконується один раз під час запуску і конфігурує пінові режими роботи.

- `INPUT` — для підключення датчиків руху та звуку.
- `INPUT_PULLUP` — для геркона (зовнішній контакт з підтягувачем до VCC).
- `OUTPUT` — для керування світлодіодами та зумером.
- `Serial.begin(9600)` — встановлення серійного з'єднання з ESP8266.
- `Serial.println(...)` — виводить повідомлення у серійний монітор.

Зчитування стану датчиків

```
int pirState = digitalRead(PIR_PIN);
int reedState = digitalRead(REED_PIN);
int soundState = digitalRead(SOUND_PIN);
```

У кожному циклі `loop()` програма зчитує стани всіх трьох датчиків.

- `pirState` — стан ІЧ-датчика.
- `reedState` — стан геркона.
- `soundState` — стан звукового сенсора.

Умови активації тривоги

```
if (alertEnabled && !inHold && millis() > ignoreTriggersUntil) {
    if (pirState == HIGH || reedState == HIGH || soundState == HIGH) {
```

```

Serial.println("ТРИВОГА! Помічено порушення!");
Serial.write('A');
if (pirState == HIGH) {
    Serial.write('R');
} else if (reedState == HIGH) {
    Serial.write('G');
} else if (soundState == HIGH) {
    Serial.write('S');
}
digitalWrite(LED_ON, HIGH);
digitalWrite(LED_OFF, HIGH);
digitalWrite(BUZZER, HIGH);
holdStartTime = millis();
inHold = true;
holdMessageSent = false;
}
}

```

Цей блок запускає тривогу, якщо система активна, не в режимі утримання і завершено період ігнорування.

- Serial.write('A') — сигнал про тривогу.
- 'R', 'G', 'S' — тип датчика: PIR (рух), геркон, звук.
- Вмикається зелений і червоний LED + зумер.
- holdStartTime зберігає час початку утримання.
- inHold = true — система переходить у режим утримання.
- holdMessageSent = false — дозвіл на одне повідомлення про HOLD.

Утримання після тривоги

```

if (inHold && millis() - holdStartTime >= 5000) {
    if (!holdMessageSent) {
        Serial.write('H');
        holdMessageSent = true;
    }
    alertEnabled = false;
    digitalWrite(BUZZER, LOW);
    digitalWrite(LED_ON, LOW);
    digitalWrite(LED_OFF, LOW);
    digitalWrite(LED_HOLD, HIGH);
}

```

Через 5 секунд після тривоги:

- Serial.write('H') — повідомлення про вхід у режим утримання.
- Вмикається зумер і LED ON/OFF.
- Вмикається LED_HOLD (жовтий індикатор).

- `alertEnabled = false` — система виходить з моніторингу.

Обробка команд з ESP (UART)

```
if (Serial.available()) {
    String command = Serial.readString();
    command.trim();

    if (command == "1") {
        alertEnabled = true;
        inHold = false;
        holdMessageSent = false;
        monitoringStartTime = millis();
        ignoreTriggersUntil = monitoringStartTime + IGNORE_DURATION;
        digitalWrite(LED_ON, HIGH);
        digitalWrite(LED_OFF, LOW);
        digitalWrite(LED_HOLD, LOW);
        Serial.println("Система моніторингу активована!");
    } else if (command == "0") {
        alertEnabled = false;
        inHold = false;
        holdMessageSent = false;
        monitoringStartTime = millis();
        ignoreTriggersUntil = monitoringStartTime + IGNORE_DURATION;
        digitalWrite(LED_ON, LOW);
        digitalWrite(LED_OFF, HIGH);
        digitalWrite(BUZZER, LOW);
        digitalWrite(LED_HOLD, LOW);
        Serial.println("Система моніторингу вимкнена.");
    }
}
```

Цей блок обробляє вхідні команди з ESP8266:

- "1" — активація системи:
 - `alertEnabled = true` — дозволено моніторинг.
 - Підсвічується червоний світлодіод.
 - Починається період ігнорування (3 секунди).
- "0" — вимкнення:
 - Скидаються всі прапори.
 - Вмикається лише зелений світлодіод.
 - Зумер вимикається.

У підсумку, реалізація програмної логіки на мікроконтролері ATmega328P забезпечує надійну взаємодію з датчиками програмно-апаратного комплексу сигналізації, дозволяє ефективно реагувати на потенційні загрози та передавати

сигнали тривоги до модуля зв'язку ESP8266. Завдяки чітко визначеним станам системи (активація, тривога, режим утримання) та використанню серійного інтерфейсу, забезпечується узгоджена робота всієї системи сигналізації. Такий підхід дозволяє створити гнучкий та зручний механізм керування безпекою приміщення з можливістю подальшої модернізації та розширення функціоналу.

3.2 Апаратна реалізація програмно-апаратного комплексу сигналізації

Реалізація апаратної частини системи програмно-апаратного комплексу сигналізації потребує правильного підключення всіх компонентів, які взаємодіють між собою через мікроконтролер Arduino Uno WiFi R3, що має вбудований модуль ESP8266. На основі проектування, розглянутого в попередньому розділі, було зібрано функціональний макет системи (рис. 3.1).

До складу пристрою входять наступні основні елементи:

- Arduino Uno WiFi R3 (ATmega328P + ESP8266) — Реалізація апаратної частини системи сигналізації потребує правильного підключення всіх компонентів, які взаємодіють між собою через мікроконтролер Arduino Uno WiFi R3, що має вбудований модуль ESP8266. На основі проектування, розглянутого в попередньому розділі, було зібрано функціональний макет системи.

- PIR-датчик руху HC-SR501 — Реалізація апаратної частини системи сигналізації потребує правильного підключення всіх компонентів, які взаємодіють між собою через мікроконтролер Arduino Uno WiFi R3, що має вбудований модуль ESP8266. На основі проектування, розглянутого в попередньому розділі, було зібрано функціональний макет системи.

- Герконовий датчик (магнітний контакт) — складається з двох частин: магніту і контактної групи. При наближенні магніту контакти замикаються, сигналізуючи, що двері або вікно зачинені. При розмиканні сигнал надходить до контролера, що інтерпретується як вторгнення.

- Зумер — забезпечує гучний звуковий сигнал у разі виявлення небезпеки.

У системі використовується активний зумер, який генерує звук самостійно при подачі живлення.

- Світлодіоди:
 - Червоний – світиться при активації сигналізації.
 - Зелений – вмикається у момент виявлення вторгнення.
 - Жовтий – вказує на перехід системи в режим утримання.
- Резистори – використовуються для обмеження струму, що протікає через світлодіоди (типово 220 Ом).

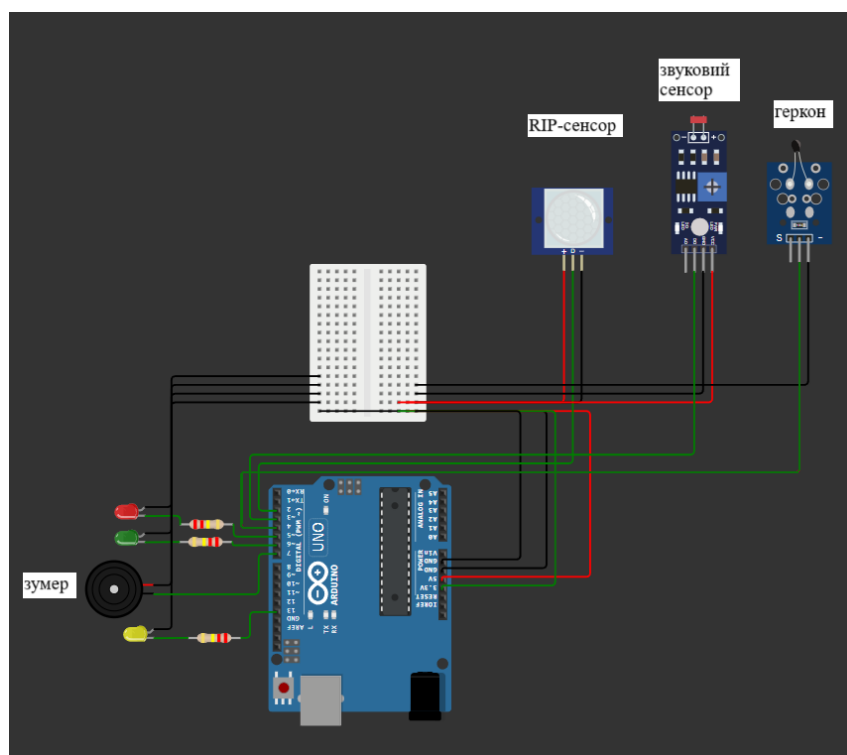


Рисунок 3.1 – схематичне зображення пристрою

Підключення компонентів:

Компоненти підключаються до Arduino за схемою(рис. 3.1):

HC-SR501:

- VCC → 5V
- GND → GND
- OUT → D2

Герконовий датчик:

- Один контакт → GND
- Інший контакт → D3

KY-037:

- VCC → 3.3V
- GND → GND
- D0 → D4

Зумер:

- "+" → D7
- "-" → GND

Світлодіоди:

- Червоний
 - Анод через резистор в D5
 - Катод → GND
- Зелений
 - Анод через резистор в D6
 - Катод → GND
- Жовтий
 - Анод через резистор в D13
 - Катод → GND

Комунікація між ATmega328P та ESP8266

Використовується програмна послідовна передача даних через SoftwareSerial. Для цього ESP8266 підключено до вільних цифрових пінів ATmega які вже прокладені в нашій платі.

Особливості живлення:

Arduino живиться від USB (5V), однак для автономної роботи доцільно використовувати зовнішнє живлення (адаптер 9V або акумулятор 7.4V – 12V). Оскільки модуль ESP8266 вшитий в нашу плату слід враховувати його підвищене

енергоспоживання, особливо під час передавання даних у Wi-Fi мережі. У зв'язку з цим, важливо забезпечити стабільне джерело живлення з мінімальними шумами.

3.3 Тестування прототипа програмно-апаратного комплексу сигналізації

Після завершення етапу розробки програмної та апаратної частини, зібрану на макетній платі систему було переведено у прототип, готовий до реального тестування. На рисунку нижче представлено фотографію готового зібраного пристрою з усіма підключеними елементами (рис.3.2).

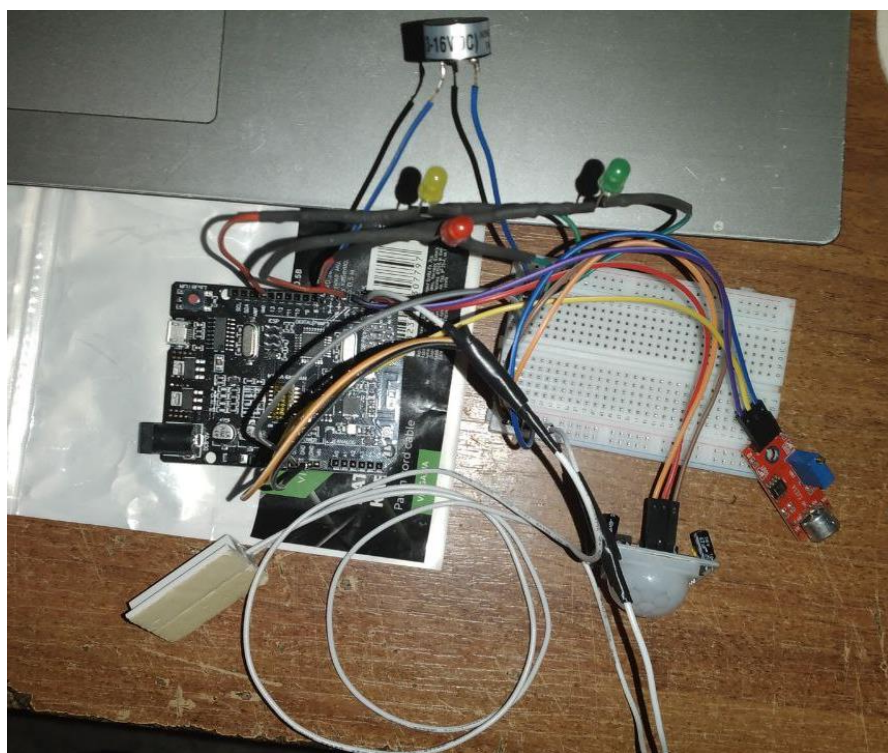


Рисунок 3.2 – Прототип програмно-апаратного комплексу сигналізації

Для перевірки працездатності системи були виконані серії тестів, які включали основні сценарії взаємодії користувача з пристроєм, а також реакції на спрацювання різних типів датчиків. Спостереження за результатами проводилося як через фізичну індикацію на пристрої (світлодіоди та зумер), так і через Telegram-бота, який фіксував усі події та дозволяв віддалене керування.

Вмикання системи сигналізації. Користувач надсилає команду `/on` через Telegram. Система переходить у режим активного моніторингу: вмикається червоний світлодіод. У Telegram надходить повідомлення про успішне включення (рис 3.3).

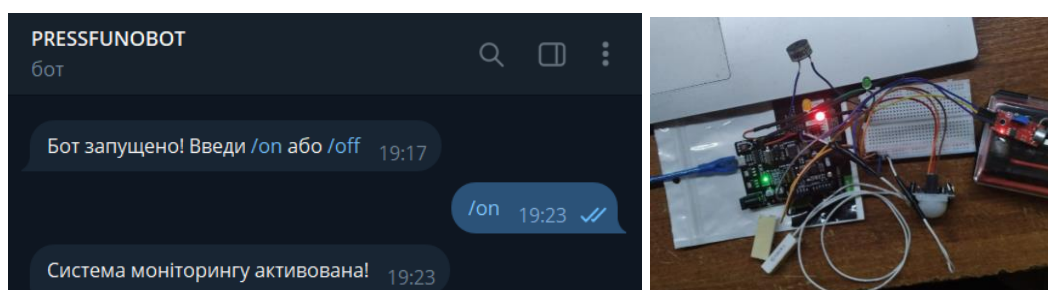


Рисунок 3.3 – Активація сигналізації у Telegram

Вимкнення системи сигналізації. Команда `/off` деактивує систему. Всі датчики стають неактивними, сигналізація не реагує на події. У чат надсилається відповідне повідомлення, світлодіоди вимикаються окрім зеленого (система вимкнена) (рис 3.4).



Рисунок 3.4 – Деактивація сигналізації у Telegram

Спрацювання PIR-сенсора. Після активації сигналізації система реагує на рух, виявлений інфрачервоним сенсором. Вмикається зумер, горять червоний і зелений світлодіоди. Telegram-бот надсилає два повідомлення: "ТРИВОГА!" та "Рух виявлено (PIR)". Через 5 секунд система переходить у режим утримання (рис 3.5).

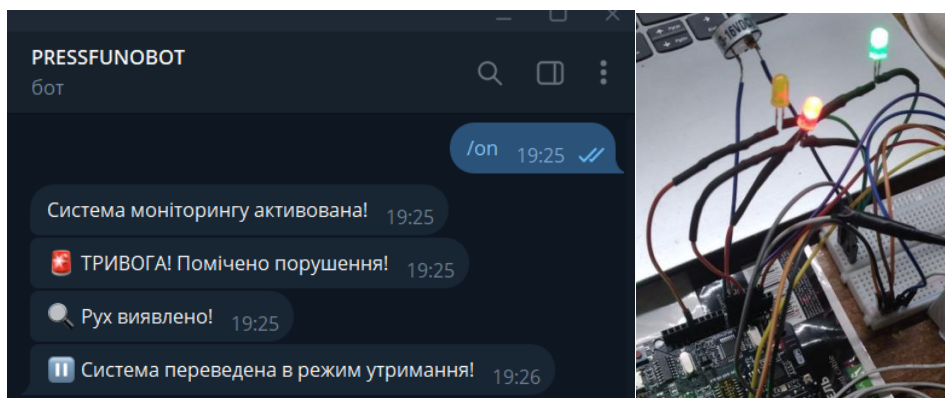


Рисунок 3.5 – Спрацювання PIR-сенсора у Telegram

Спрацювання звукового сенсора. Аналогічно до PIR-сенсора, при виявленні звуку активується сигналізація. Зумер і світлодіоди сигналізують про тривогу, надсилається повідомлення про спрацювання звукового сенсора. Через 5 секунд система переходить у режим утримання (рис 3.6).

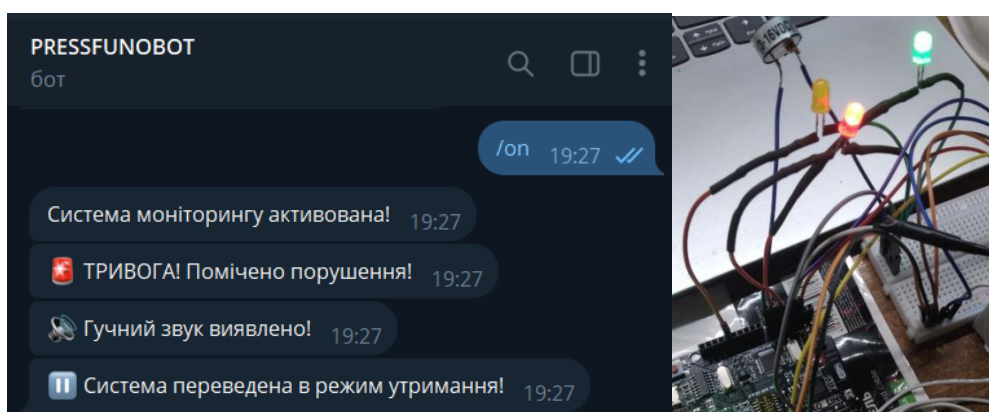


Рисунок 3.6 – Спрацювання звукового сенсора у Telegram

Спрацювання геркона. Коли розмикається контакт геркона (наприклад, відкриваються двері), система ідентифікує це як вторгнення. Вмикається тривожна сигналізація, Telegram-бот повідомляє про подію. Через 5 секунд система переходить у режим утримання (рис 3.7).

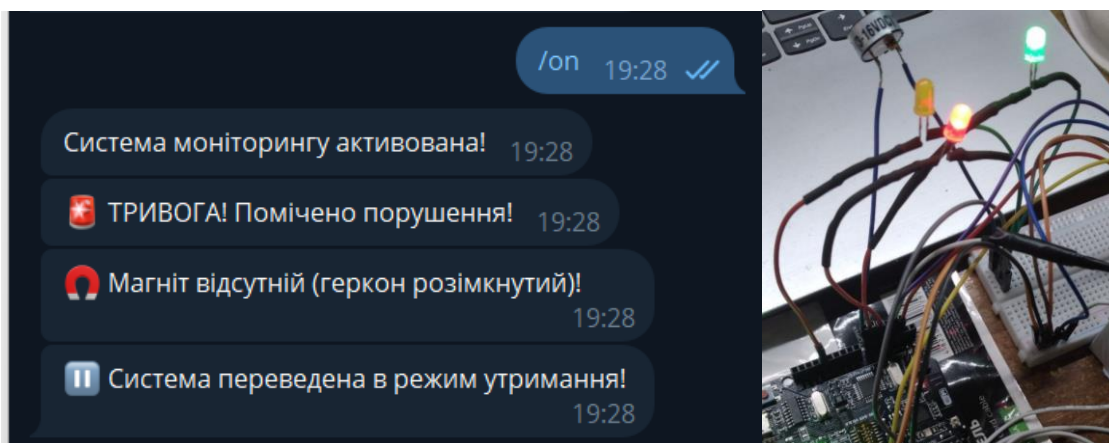


Рисунок 3.7 – Спрацювання геркона у Telegram

Переведення системи в режим утримання. Після будь-якого спрацювання система автоматично переходить у режим утримання: сигналізація вимикається, активується жовтий світлодіод, Telegram-бот надсилає повідомлення "Система переведена в режим утримання". У цьому режимі система не реагує на події (рис 3.8).

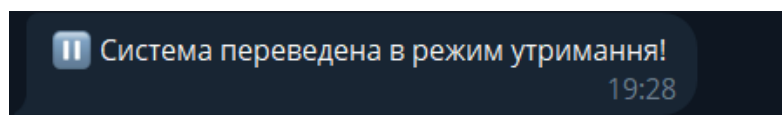
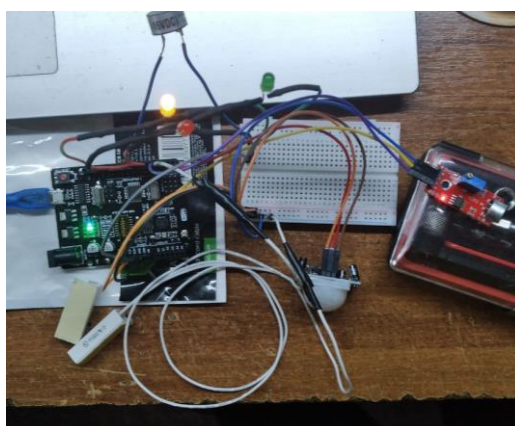


Рисунок 3.8 – Повідомлення про режим утримання у Telegram

Вихід з режиму утримання командою /on. Користувач може знову активувати систему командою /on. Telegram підтверджує це, світлодіоди змінюють індикацію. Система повертається до активного моніторингу (рис 3.9).

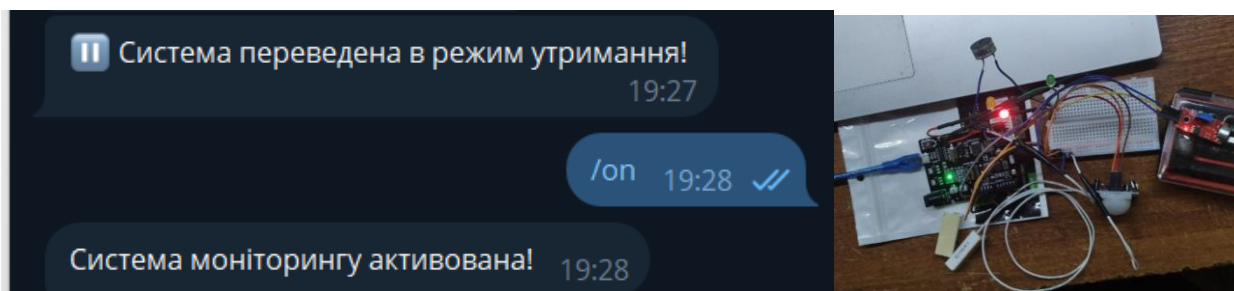


Рисунок 3.9 – Вихід з утримання командою /on

Вихід з режиму утримання командою /off. Команда /off у режимі утримання вимикає систему повністю. Включається зелений індикатор, система стає неактивною до наступної активації (рис 3.10).

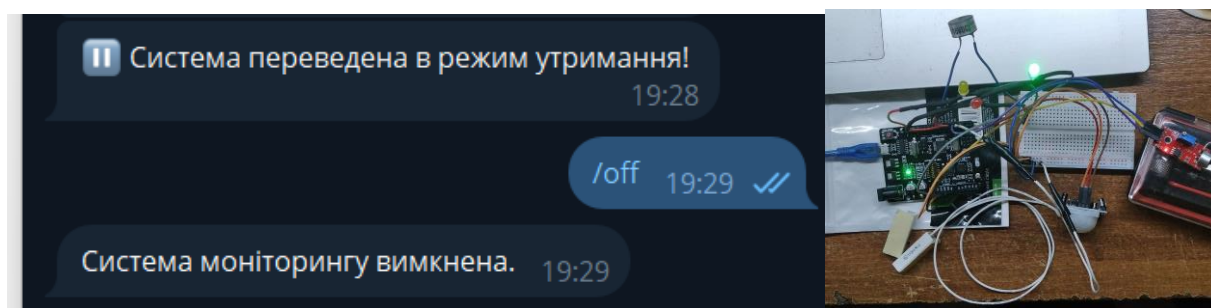


Рисунок 3.10 – Вихід з утримання командою /off

У результаті тестування було підтверджено працездатність усіх компонентів: система стабільно з'єднується з мережею, коректно реагує на команди та події, надає миттєве інформування користувача через Telegram. Всі датчики та індикаційні елементи працюють узгоджено відповідно до заданого алгоритму.

3.4 Висновок до розділу 3

У даному розділі було реалізовано повний цикл створення прототипу програмно-апаратного комплексу сигналізації з віддаленим керуванням та оповіщенням на базі мікроконтролера Arduino Uno WiFi R3, який об'єднує в собі модулі ATmega328P та ESP8266. Було детально розглянуто програмну реалізацію системи — з поділом логіки між мікроконтролерами, обробкою сигналів від сенсорів та організацією взаємодії з Telegram-ботом.

У ході роботи було реалізовано підтримку трьох типів сенсорів: інфрачервоного (PIR), звукового та магнітного (геркон), що дозволило створити багатофункціональну систему виявлення вторгнень. Окрему увагу приділено алгоритмам активації, деактивації, обробки тривоги та переходу в режим утримання, що забезпечують надійну та передбачувану поведінку пристрою.

Під час тестування прототипу було перевірено всі основні сценарії роботи системи, включаючи коректну обробку команд користувача (/on, /off), спрацювання кожного з датчиків, а також реакцію системи у режимі утримання. Система показала стабільну роботу: чітко фіксувала події, миттєво надсилала повідомлення до Telegram, а також забезпечувала звукову та візуальну індикацію тривоги.

Таким чином, у результаті реалізації та тестування було доведено, що спроектована система є функціональною, надійною та придатною до подальшого використання або масштабування — з можливістю інтеграції додаткових сенсорів.

ВИСНОВКИ

У ході виконання було проведено аналіз сучасних охоронних систем, виявлено їхні ключові особливості, переваги та недоліки, а також визначено актуальні вимоги до безпекових рішень з віддаленим керуванням. На основі цього аналізу сформовано вимоги до майбутнього проєкту.

Після вивчення доступних апаратних та програмних рішень було обґрунтовано вибір мікроконтролера Arduino Uno WiFi R3 з вбудованим ESP8266 як основи для побудови сигналізації. Також було підібрано оптимальні типи сенсорів — інфрачервоний датчик руху, герконовий датчик відкриття дверей і звуковий сенсор — для забезпечення контролю над фізичними загрозами.

Для програмної реалізації системи було обрано мову C/C++ та середовище Arduino IDE, що забезпечують прямий доступ до апаратних ресурсів і дозволяють ефективно працювати в умовах обмежених обчислювальних потужностей мікроконтролера. Система розроблена з використанням Telegram-бота для дистанційного керування, сповіщення про тривоги та зміни режимів.

Було реалізовано повноцінний прототип системи програмно-апаратного комплексу сигналізації, що виконує активацію та деактивацію режимів охорони, виявляє рух, звук або відкриття дверей, генерує тривожні сигнали, надсилає повідомлення користувачу та переходить у режим утримання після спрацювання тривоги. Завдяки використанню інтеграції з Telegram, система дозволяє здійснювати дистанційний контроль у режимі реального часу.

Проведене тестування підтвердило стабільну та надійну роботу всіх елементів системи: підключення до інтернету, обмін повідомленнями з ботом, коректне реагування на команди /on, /off, спрацювання всіх сенсорів, звукову сигналізацію та функцію режиму утримання. Прототип успішно пройшов перевірку в умовах, наближених до реального використання.

Таким чином, поставлена мета роботи була досягнута. Розроблена система є ефективною, доступною та гнучкою у застосуванні, а її функціонал може бути розширений у майбутньому для більш складних сценаріїв охорони.

ПЕРЕЛІК ПОСИЛАНЬ

1. Smart Home and Security Systems: An IoT-Based Approach Utilizing ESP 32 and Multi-sensor Integration / S. S. Prakash та ін. E3S Web of Conferences. 2025. Т. 616. С. 02004. URL: <https://doi.org/10.1051/e3sconf/202561602004> (дата звернення: 05.05.2025).

2. Development and Implementation of an IoT-Based Smart Home Security System in Mogadishu, Somalia / A. Y. Nageye та ін. International Journal of Electrical and Electronics Engineering. 2024. Т. 11, № 9. С. 326–332. URL: <https://doi.org/10.14445/23488379/ijeee-v11i9p129> (дата звернення: 05.05.2025).

3. Narsaiah Domala et al. Iot Based Home Security System Using Arduino. Proceeding International Conference on Science and Engineering. 2023. Т. 11, № 1. С. 1608–1614. URL: <https://doi.org/10.52783/cienceng.v11i1.312> (дата звернення: 06.05.2025).

4. Design and implementation of an intelligent building security system using Arduino GIGA R1 Wi-Fi / M. Bounabi та ін. *STUDIES IN ENGINEERING AND EXACT SCIENCES*. 2024. Т. 5, № 2. С. e7917. URL: <https://doi.org/10.54021/seesv5n2-217> (дата звернення: 05.05.2025).

5. Перспективи впровадження доступних охоронних систем на основі сучасних технологій і відкритих платформ URL: <https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2025/paper/view/24169/20022> (дата звернення: 05.05.2023)

6. Прилади охорони та моніторингу. UNICOM. URL: https://el-sys.com.ua/solution_5 (дата звернення: 05.05.2023).

7. Охоронна система Ajax URL: <https://ajax.systems/ua/> (дата звернення: 16.05.2023).

8. Комплект GSM сигналізації Ajax StarterKit White. Hotline. URL: <https://hotline.ua/ua/dom-komplekty-signalizacij/ajax-starterkit-white/?tab=about> (дата звернення: 06.05.2023).

9. TIRAS Technologies. URL: <https://tiras.technology/> (дата звернення: 16.05.2023).

10. Orion NOVA X. Basic kit. URL: <https://tiras.technology/documentation/orion-nova-x-basic-kit/> (дата звернення: 07.05.2023).

11. Види охоронної сигналізації. legion-security. URL: <https://legion-security.com.ua/ua/vidi-ohoronno%D1%97-signalizaczi%D1%97/> (дата звернення: 07.05.2023).

12. Які є види сигналізацій та їх принцип роботи. gaziknet. URL: <https://www.gazik.com.ua/yaki-ye-vydy-sygnalizacij-ta-yih-prynczyp-roboty.html> (дата звернення: 08.05.2023).

13. Види охоронної сигналізації. SECURITY. URL: <https://sg-ukraine.com.ua/news/vidy-ohrannoj-signalizacii/> (date of access: 17.05.2023).

14. Охоронна сигналізація – які бувають та в чому різниця. URL: <https://tech.gas.ua/blog/25?srsId=AfmBOopyusV6jLsAQmkOz0A9CB3rfDvpE19565Z5bd85YYYWMhswidlY> (дата звернення: 10.05.2023).

15. Види датчиків руху Безпека та відеоспостереження. URL: <https://oxorona.com/motion-sensor-types/> (дата звернення: 11.05.2023).

16. Як працює датчик відкриття дверей: що таке геркон та який принцип його роботи. Ohrana.ua. URL: <https://ohrana.ua/uk/stati-i-obzory/kak-rabotaet-datchik-otkrytiya-dveri-cto-takoe-gerkon-i-princip-ego-raboty.html> (дата звернення: 18.05.2023).

17. Датчик розбиття скла: детальна характеристика та принцип роботи. OIBS. URL: <https://oib.com.ua/datchik-razbitiya-stekla-kharakteristika/> (дата звернення: 13.05.2023).

18. Принцип роботи ультразвукового датчика. URL: <https://ua.piezodisc.com/info/ultrasonic-transducer-working-principle-59601848.html> (дата звернення: 14.05.2023).

19. ФОТОЕЛЕКТРИЧНІ ДАТЧИКИ Загальний опис. ред. О. А. Яланський ; пер. з Англ. О. А. Яланський. М.Дніпропетровськ : ДВНЗ «НГУ». (дата звернення: 15.05.2023).

20. Вібраційні вилкові датчики рівня Fine Tek SC28. СВ АЛТЕРА. URL: <https://svaltera.lviv.ua/2020/06/10/fine-tek-sc28-datchyk-rivnya/> (дата звернення: 15.05.2023).

21. Ємнісний датчик. URL: <https://ayvaz.com.ua/ua/news/67-yomkostnyy-datchik> (дата звернення: 18.05.2023).

22. RobotDyn PINOUT DIAGRAM. URL: https://openhacks.com/uploads/productos/pinout__0g-00005215__uno_wifi-r3-at328-esp8266-ch340g.pdf (дата звернення: 18.05.2023).

23. RobotDyn UNO R3 ATmega328P + Wi-Fi ESP8266, 8Mbit. MiniBoard. URL: <https://miniboard.com.ua/mikrokontroleri/604-robotdyn-uno-r3-atmega328p-wi-fi-esp8266-8mbit.html> (дата звернення: 19.05.2023).

24. Датчик руху інфрачервоний (PIR Sensor) HC-SR501 URL: <https://www.minitech.com.ua/ua/datchik-dvizheniya-infrakrasniy-pir-sensor-hc-sr501> (дата звернення: 19.05.2023).

25. Геркон PRC ACMK-1 URL: <https://rombi.com.ua/ua/p2003304347-gerkon-prc-asmk.html> (дата звернення: 20.05.2023).

26. Звуковий модуль мікрофона KY-037 для Ардуїно URL: <https://arduinoakit.com.ua/ua/p1592083834-zvukovoj-modul-mikrofona.html?srsId=AfmBOoq-DZDltWrliQZV3GcSPjmRqGx-lpMWmkdouAMKyaA39eprS90b> (дата звернення: 20.05.2023).

27. Мікроконтролер Arduino URL: <https://bitkit.com.ua/shho-take-arduino?srsId=AfmBOorT9jLp66wK8Y1Je91zI-aQwWi0MexU4f88kYq83H9CKRV R8jAZ> (дата звернення: 20.05.2023).

28. Get Started! Get a Compiler URL: <https://isocpp.org/get-started> (дата звернення: 21.05.2023).

29. News, Status & Discussion about Standard C++: <https://isocpp.org/> (дата звернення: 21.05.2023).

30. Arduino IDE URL: <https://itmaster.biz.ua/electronics/arduino/arduino-ide.html> (дата звернення: 22.05.2023).

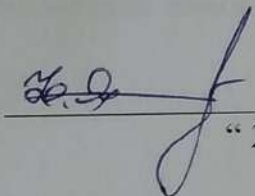
ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції “Управління інформаційною
безпекою” кафедри МБІС
д.т.н., професор

 Юрій ЯРЕМЧУК
“ 20 ” березня 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до бакалаврської кваліфікаційної роботи на тему:

Розробка програмно-апаратного комплексу сигналізації з функціями віддаленого
керування та оповіщення на основі платформи Arduino

08-72.БДР.012.00.065 ТЗ

Керівник бакалаврської кваліфікаційної роботи

к.т.н., доц., зав. каф. МБІС

 Карпінець В. В.
“20” березня 2023 р

Вінниця – 2025 р.

1. Найменування та область застосування

Програмно-апаратного комплексу сигналізації з функціями віддаленого керування та оповіщення на основі платформи Arduino. Область застосування: захист програмного забезпечення від несанкціонованих дій.

2. Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ № 97 від 20.03.2025 р.

3. Мета та призначення розробки

3.1 Мета розробки: розробка програмно-апаратного комплексу сигналізації з функціями віддаленого керування та оповіщення на основі платформи Arduino.

3.2 Призначення: розроблений програмний модуль виконує повідомлення та про несанкціоноване проникнення.

4. Джерела розробки

4.1 RobotDyn PINOUT DIAGRAM. URL:

https://openhacks.com/uploads/productos/pinout__0g-00005215__uno_wifi-r3-at328-esp8266-ch340g.pdf

4.2 RobotDyn UNO R3 ATmega328P + Wi-Fi ESP8266, 8Mbit. MiniBoard. URL:

<https://miniboard.com.ua/mikrokontroleri/604-robotdyn-uno-r3-atmega328p-wi-fi-esp8266-8mbit.html>

4.3 Arduino IDE URL: <https://itmaster.biz.ua/electronics/arduino/arduino-ide.html>

4.4 Прилади охорони та моніторингу. UNICOM. URL: https://elsys.com.ua/solution_5

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація програмно-апаратної системи не повина містити дорогих компонентів;

5.1.3 Програмний засіб повинен виконувати процес автентифікації

користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмно-апаратний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.3 Програмно-апаратний засіб повинен виконувати свої функції.

6. Вимоги до програмної документації

6.1 Обов'язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.3

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмно-апаратного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу до керування сигналізацією.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу

9. Стадії та етапи розробки

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Початок	Закінчення
1.	Визначення напрямку бакалаврської роботи, формулювання теми	10.03.2025	15.03.2025
2.	Аналіз предметної області обраної теми	20.03.2025	19.04.2025
3.	Розробка алгоритму роботи	11.05.2025	20.05.2025
4.	Написання бакалаврської роботи на основі розробленої теми	21.05.2025	25.05.2025
5.	Передзахист бакалаврської кваліфікаційної роботи	27.05.2025	28.05.2025
6.	Виправлення, уточнення, корегування бакалаврської кваліфікаційної роботи	29.05.2025	06.06.2025
7.	Захист бакалаврської кваліфікаційної роботи	10.06.2025	11.06.2025

10. Порядок контролю та прийому

70

10.1 До приймання бакалаврської кваліфікаційної роботи надається:

- ПЗ до бакалаврської кваліфікаційної роботи надається;
- демонстрація результату бакалаврської кваліфікаційної роботи;
- презентація;
- відзив керівника роботи;
- відзив рецензента

Технічне завдання до виконання прийняв  Ніколайчук О.В.

Додаток Б. Лістинг програмного коду

```
#include <ESP8266WiFi.h>
#include <WiFiClientSecure.h>
#include <UniversalTelegramBot.h>

const char* ssid = "UnoWiFi";
const char* password = "basiscum";
#define BOT_TOKEN "7731379464:AAHnknABQQjyJQDnciXedSnjaekC5_kl4Fk"
#define CHAT_ID "494305229"

WiFiClientSecure client;
UniversalTelegramBot bot(BOT_TOKEN, client);
unsigned long lastTimeBotRan = 0;

bool notificationsEnabled = false;

void setup() {
  Serial.begin(9600);
  WiFi.begin(ssid, password);
  client.setInsecure();

  Serial.print("Підключення до Wi-Fi...");
  while (WiFi.status() != WL_CONNECTED) {
    Serial.print(".");
    delay(500);
  }
  Serial.println(" Підключено!");
  bot.sendMessage(CHAT_ID, "Бот запущено! Введи /on або /off", "");
}

void loop() {
  // Telegram команди
  if (millis() - lastTimeBotRan > 2000) {
    int numNewMessages = bot.getUpdates(bot.last_message_received + 1);
    while (numNewMessages) {
      for (int i = 0; i < numNewMessages; i++) {
        String text = bot.messages[i].text;

        if (text == "/on") {
          Serial.write('1');
          notificationsEnabled = true;
          bot.sendMessage(CHAT_ID, "Система моніторингу активована!", "");
        }
        else if (text == "/off") {
          Serial.write('0');
          notificationsEnabled = false;
          bot.sendMessage(CHAT_ID, "Система моніторингу вимкнена.", "");
        }
      }
      numNewMessages = bot.getUpdates(bot.last_message_received + 1);
    }
    lastTimeBotRan = millis();
  }

  // Отримання подій з Arduino
  if (Serial.available()) {
```

```

char signal = Serial.read();

if (signal == 'A' && notificationsEnabled) {
  bot.sendMessage(CHAT_ID, " 🚨 ТРИВОГА! Помічено порушення!", "");
}
else if (signal == 'R' && notificationsEnabled) {
  bot.sendMessage(CHAT_ID, " 🕵️ Рух виявлено!", "");
}
else if (signal == 'G' && notificationsEnabled) {
  bot.sendMessage(CHAT_ID, " 🧲 Магніт відсутній (геркон розімкнутий)!", "");
}
else if (signal == 'S' && notificationsEnabled) {
  bot.sendMessage(CHAT_ID, " 🔊 Гучний звук виявлено!", "");
}
else if (signal == 'H' && notificationsEnabled) {
  bot.sendMessage(CHAT_ID, " 🛑 Система переведена в режим утримання!", "");
}
}
}

// Піни підключення датчиків
#define PIR_PIN 2
#define REED_PIN 3
#define SOUND_PIN 4

// Світлодіоди та зумер
#define LED_ON 5
#define LED_OFF 6
#define BUZZER 7
#define LED_HOLD 13

bool alertEnabled = false;
bool inHold = false;
bool holdMessageSent = false;
unsigned long holdStartTime = 0;

// Змінні для уникнення ложних спрацювань
unsigned long monitoringStartTime = 0;
unsigned long ignoreTriggersUntil = 0;
const unsigned long IGNORE_DURATION = 3000; // 3 секунди

void setup() {
  pinMode(PIR_PIN, INPUT);
  pinMode(REED_PIN, INPUT_PULLUP);
  pinMode(SOUND_PIN, INPUT);

  pinMode(LED_ON, OUTPUT);
  pinMode(LED_OFF, OUTPUT);
  pinMode(BUZZER, OUTPUT);
  pinMode(LED_HOLD, OUTPUT);

  Serial.begin(9600);
  Serial.println("Система моніторингу запущена...");
}

void loop() {
  int pirState = digitalRead(PIR_PIN);
  int reedState = digitalRead(REED_PIN);
  int soundState = digitalRead(SOUND_PIN);

```

```

if (alertEnabled && inHold && millis() > ignoreTriggersUntil) {
  if (pirState == HIGH || reedState == HIGH || soundState == HIGH) {
    Serial.println("ТРИВОГА! Помічено порушення!");
    Serial.write('A');

    if (pirState == HIGH) {
      Serial.write('R');
    } else if (reedState == HIGH) {
      Serial.write('G');
    } else if (soundState == HIGH) {
      Serial.write('S');
    }
  }

  digitalWrite(LED_ON, HIGH);
  digitalWrite(LED_OFF, HIGH);
  digitalWrite(BUZZER, HIGH);

  holdStartTime = millis();
  inHold = true;
  holdMessageSent = false;
}
}

if (inHold && millis() - holdStartTime >= 5000) {
  if (!holdMessageSent) {
    Serial.write('H'); // Надсилаємо лише один раз
    holdMessageSent = true;
  }

  alertEnabled = false;
  digitalWrite(BUZZER, LOW);
  digitalWrite(LED_ON, LOW);
  digitalWrite(LED_OFF, LOW);
  digitalWrite(LED_HOLD, HIGH);
}

if (Serial.available()) {
  String command = Serial.readString();
  command.trim();

  if (command == "1") {
    alertEnabled = true;
    inHold = false;
    holdMessageSent = false;
    monitoringStartTime = millis();
    ignoreTriggersUntil = monitoringStartTime + IGNORE_DURATION;

    digitalWrite(LED_ON, HIGH);
    digitalWrite(LED_OFF, LOW);
    digitalWrite(LED_HOLD, LOW);
    Serial.println("Система моніторингу активована!");
  } else if (command == "0") {
    alertEnabled = false;
    inHold = false;
    holdMessageSent = false;
    monitoringStartTime = millis();
    ignoreTriggersUntil = monitoringStartTime + IGNORE_DURATION;
  }
}

```

```
    digitalWrite(LED_ON, LOW);  
    digitalWrite(LED_OFF, HIGH);  
    digitalWrite(BUZZER, LOW);  
    digitalWrite(LED_HOLD, LOW);  
    Serial.println("Система моніторингу вимкнена.");  
  }  
}  
  
delay(200);  
}
```

Додаток В. Ілюстраційний матеріал

Вінницький Національний Технічний Університет | 2025

Сторінка

01

РОЗРОБКА ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ СИГНАЛІЗАЦІЇ З ФУНКЦІЯМИ ВІДДАЛЕНОГО КЕРУВАННЯ ТА ОПОВІЩЕННЯ НА ОСНОВІ ПЛАТФОРМИ ARDUINO

Виконав: студент групи 2KITC-216 Ніколайчук О.В.

Науковий керівник: к.т.н., доц., зав. каф. МБІС Карпинець В.В.

Вінницький Національний Технічний Університет | 2025

Сторінка

02

АКТУАЛЬНІСТЬ ТЕМИ

У сучасних реаліях питання безпеки житла та офісів стає дедалі важливішим. Традиційні системи захисту часто є дорогими, громіздкими або вимагають професійного обслуговування. Саме тому зростає потреба у недорогих, простих в установці та надійних системах охорони, які можна контролювати дистанційно. Платформа Arduino з ESP-модулем дозволяє реалізувати таку систему швидко, ефективно та з використанням сучасних каналів зв'язку, зокрема Telegram.

МЕТА РОБОТИ

Головною метою розробки є створення недорогої, доступної та легкої у конфігурації системи сигналізації на базі Arduino, яка здатна реагувати на загрози та негайно оповіщати користувача. Система повинна підтримувати Telegram-команди та працювати з різними типами датчиків.

ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Об'єкт дослідження

Об'єкт дослідження складається із охоронних систем з можливостями дистанційного керування.

Предмет дослідження

Предмет дослідження є принципи і методи застосування мікроконтролерів та датчиків у системах безпеки.

АНАЛІЗ АНАЛОГІВ

Розроблений пристрій на базі Arduino та ESP є доступним за ціною, підтримує декілька типів датчиків, а також керування через Telegram-бота.

Його переваги — відкритість, кастомізація, низька собівартість. Водночас, система поступається комерційним аналогам у дизайні, захисті від саботажу.

Ajax

Комерційна система сигналізації з розвиненим функціоналом. Її основні недоліки — висока вартість, закритий код та обмеженість у зміні налаштувань користувачем.

Teras

Бюджетна система охорони з базовими можливостями та підтримкою GSM-зв'язку. Вона проста у встановленні, але обмежена у гнучкості, не має інтернет-керування та не інтегрується з сучасними платформами.

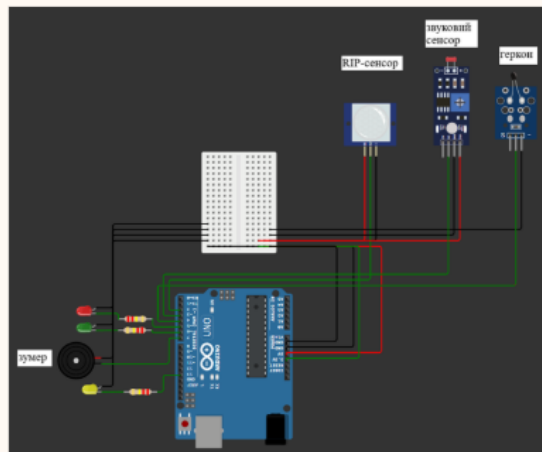
ВИКОРИСТАНІ ТЕХНОЛОГІЇ



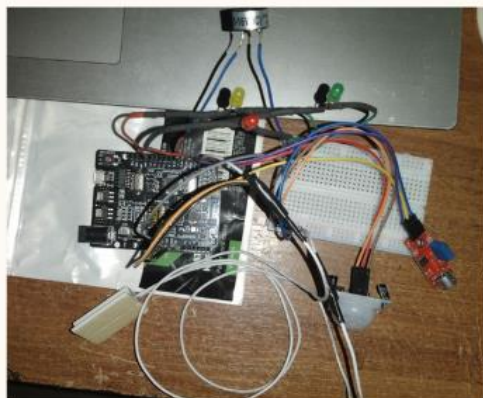
У реалізації використано мову програмування C/C++, середовище Arduino IDE та Telegram Bot API для обміну повідомленнями. Усі компоненти інтегруються через послідовне з'єднання. Завдяки використанню ESP8266 система підключається до Wi-Fi, а Telegram-бот забезпечує гнучкий канал зворотного зв'язку, який є надійним, простим у налаштуванні та не потребує додаткових серверів.

АЛГОРИТМ РОБОТИ ПРИЛАДА

Система працює в режимі моніторингу: при активації вона сканує датчики на предмет руху, відкривання дверей або підозрілих звуків. У разі спрацювання хоча б одного сенсора, система вмикає сигналізацію та надсилає повідомлення в Telegram. Після цього вона автоматично переходить у "режим утримання", очікуючи команду повторного запуску, або вимкнення від користувача.



КОМПОНЕНТИ СИСТЕМИ



До складу системи входить мікроконтролер Arduino Uno R3 з ESP8266, а також набір сенсорів: ІЧ-датчик, герконовий датчик (магнітний), мікрофонний модуль для виявлення звуків. В якості виконавчих елементів використовуються світлодіоди та зумер. Через ESP-модуль відбувається зв'язок з Telegram, що дозволяє надсилати тривожні повідомлення користувачу.



ФОТО ПРОТОТИПА ПРИБОРУ

На зображенні показано готовий пристрій в пластиковому корпусі з підключеним PIR-сенсором, світлодіодами, антеною Wi-Fi та герконовим датчиком. Це демонструє завершену конструкцію програмно-апаратного комплексу сигналізації, придатну до експлуатації.

ТЕСТУВАННЯ СИСТЕМИ: СЦЕНАРІЙ ТРИВОГИ



В прилада загорається 2 світлодіода і лунає сирена, відбувається надсилання повідомлень в чат з уточненням який датчик спрацював

PIR-датчик фіксує рух

ТРИВОГА! Помічено порушення! 0:13
Рух виявлено! 0:13

Звуковий сенсор фіксує шум

ТРИВОГА! Помічено порушення! 19:25
Гучний звук виявлено! 19:25

Геркон реагує на розмикання магніту

ТРИВОГА! Помічено порушення! 19:24
Магніт відсутній (геркон розімкнений)! 19:24

ТЕСТУВАННЯ СИСТЕМИ: РЕЖИМ УТРИМАННЯ

Після фіксації загрози, система автоматично переходить у режим утримання. Цей режим оптимізує сповіщення й запобігає повторному спрацювані тривоги.

II Система переведена в режим утримання! 19:24



ФОТО: ПРИСТРІЙ У СТАНІ АКТИВНОГО МОНІТОРИНГУ

На фото зображено готовий пристрій. Світлодіодний індикатор червоного кольору світить про те, що пристрій переведений у режим охорони.

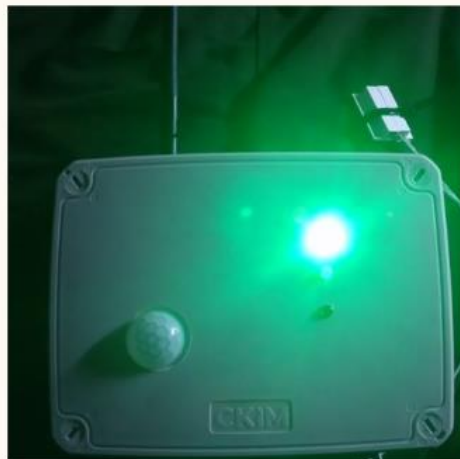
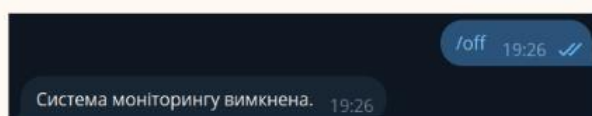
Система моніторингу активована! 19:24

/on 19:23 ✓



ФОТО:ПРИСТРІЙ У СТАНІ ВИМКНЕНОГО МОНІТОРИНГУ

На даному зображенні показано той самий пристрій, однак система переведена в режим вимкненого моніторингу про що свідчить зелений індикатор



ВИСНОВОК

Розроблена система сигналізації довела свою ефективність у тестовому середовищі. Вона демонструє переваги відкритої архітектури, гнучкість у налаштуванні, доступність компонентів та простоту розгортання. Telegram-бот забезпечує сучасний спосіб оповіщення та керування. Незважаючи на певні обмеження щодо професійного застосування, рішення ідеально підходить для домашнього використання.

ДЯКУЮ ЗА ВАШУ УВАГУ!

Додаток Г. Протокол перевірки на антиплагіат

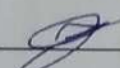
ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи:

Розробка програмно-апаратного комплексу сигналізації з функціями віддаленого керування та оповіщення на основі платформи Arduino

Тип роботи: бакалаврська кваліфікаційна робота

Підрозділ Кафедра менеджменту на безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
Гр. 2KITC-216

Керівник доцент Карпинець В.В. 

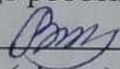
Показники звіту подібності
Strike Plagiarism

Оригінальність	94,57%
Загальна схожість	5,43%

Аналіз звіту подібності (відмітити потрібне)

- ☐ **Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату**
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений (-на) з повним звітом подібності, який був згенерований Системою щодо роботи (додається)

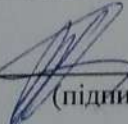
Автор 
(підпис)

Ніколайчук О.В.
(прізвище, ініціали)

Опис прийнятого рішення

- ☐ Допустити до захисту.

Особа, відповідальна за перевірку


(підпис)

Коваль Н.П.
(прізвище, ініціали)

Експерт
(за потреби)

(підпис)

(прізвище, ініціали, посада)