

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Чорноморський національний університет**

**імені Петра Могили**

**Факультет комп'ютерних наук**

**Кафедра комп'ютерної інженерії**

ДОПУЩЕНО ДО ЗАХИСТУ

Завідувач кафедри,  
д-р техн. наук, проф.

\_\_\_\_\_ І. М. Журавська

«\_\_» \_\_\_\_\_ 2023 р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

**Автономний комплекс візуального  
моніторингу оселі**

Спеціальність 123 Комп'ютерна інженерія

123 – КБР.ПЗ.00 – 405.21910513

*Студент*

\_\_\_\_\_ К. В. Кочетов

*підпис*

«\_\_» \_\_\_\_\_ 202\_\_ р.

*Керівник ст. викладач*

\_\_\_\_\_ Є. С. Дарнапук

*підпис*

«\_\_» \_\_\_\_\_ 202\_\_ р.

**Миколаїв – 2023**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**Чорноморський національний університет імені Петра Могили**  
**Факультет комп'ютерних наук**  
**Кафедра комп'ютерної інженерії**

ЗАТВЕРДЖУЮ

Зав. кафедри \_\_\_\_\_ І. М. Журавська

« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ р.

**ЗАВДАННЯ**  
**на виконання кваліфікаційної бакалаврської роботи**

Видано студенту групи 405 факультету комп'ютерних наук

Кочетову Костянтину Вікторовичу  
*(прізвище, ім'я, по-батькові студента)*

1. Тема кваліфікаційної роботи

Автономний комплекс візуального моніторингу оселі

Затверджена наказом по ЧНУ від « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ р. № \_\_\_\_\_

2. Строк представлення кваліфікаційної роботи « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ р.

3. Очікуваний результат роботи та початкові дані, якщо такі потрібні

Очікуваним результатом роботи є: апаратне та програмне забезпечення комплексу візуального моніторингу оселі. Вхідними даними роботи є специфікація вимог, що описує характеристики зазначеного апаратного та програмног забезпечення.

4. Перелік питань, що підлягають розробці

- оглянути сучасні існуючі рішення подібних комплексів
- проаналізувати конкурентну базу
- розробка апаратної частини пристрою
- розробка програмної частини пристрою

5. Перелік графічних матеріалів

Слайди презентації

6. Завдання до спеціальної частини

- визначити вимоги щодо безпеки та захисту здоров'я працівників під час роботи з комп'ютерними приладами
- Аналіз вимог до роботи з електричним обладнанням

7. Консультанти:

Консультант	Кафедра (організація)	Частина роботи
А. О. Алексєєва, к.т.н., доцент	кафедра екології Медичного інституту ЧНУ імені Петра Могили	Спеціальна частина з охорони праці

Керівник роботи

ст. викладач Дарнапук Євген Сергійович

*(посада, прізвище, ім'я, по батькові)*

\_\_\_\_\_  
*(підпис)*

Завдання прийнято до виконання

Кочетов Костянтин Вікторович

*(прізвище, ім'я, по батькові студента)*

\_\_\_\_\_  
*(підпис)*

Дата видачі завдання « \_\_\_\_ » \_\_\_\_\_ 20\_\_ р.

## КАЛЕНДАРНИЙ ПЛАН

### виконання кваліфікаційної бакалаврської роботи

Тема: Автономний комплекс візуального моніторингу оселі

№	Найменування роботи	Початок	Закінчення	Примітки
1	Розробка та затвердження завдання на виконання КБР	20.12.2022	26.12.2022	Виконано
2	Огляд літератури за темою роботи	14.01.2023	01.02.2023	Виконано
3	Складання календарного плану КБР	04.02.2023	06.02.2023	Виконано
4	Аналіз предметної області	07.02.2023	02.03.2023	Виконано
5	Розробка проєктних рішень	03.03.2023	18.03.2023	Виконано
6	Моделювання апаратної частини	18.03.2023	06.04.2023	Виконано
7	Розробка програмного забезпечення та його тестування	07.04.2023	08.05.2023	Виконано
8	Написання розділу з охорони праці	09.05.2023	19.05.2023	Виконано
8	Відгук керівника КБР	20.05.2023	21.05.2023	Виконано
9	Оформлення КБР та презентації	22.05.2023	30.05.2023	Виконано
10	Перший передзахист КБР	30.05.2023	30.05.2023	Виконано
11	Другий передзахист КБР	13.06.2023	13.06.2023	Виконано
12	Рецензування	13.06.2023	20.06.2023	Виконано
14	Завершення оформлення КБР та презентації	13.06.2023	20.06.2023	Виконано
13	Захист кваліфікаційної бакалаврської роботи	27.06.2023	28.06.2023	Виконано

Розробив здобувач ВО Кочетов К. В.  
(прізвище, ім'я, по батькові) \_\_\_\_\_ (підпис)  
« \_\_\_\_ » \_\_\_\_\_ 2023 р.

Керівник роботи ст. викладач Дарнапук Є. С.  
(посада, прізвище, ім'я, по батькові) \_\_\_\_\_ (підпис)  
« \_\_\_\_ » \_\_\_\_\_ 2023 р.

## **АНОТАЦІЯ**

до кваліфікаційної бакалаврської роботи  
«Автономний комплекс візуального моніторингу оселі»  
Студент 405 гр. Кочетов Костянтин Вікторович  
Керівник: ст. викладач Дарнапук Євген Сергійович

Ця робота присвячена розробці автономного комплексу візуального моніторингу оселі. Головною метою проєкту є створення пристрою, за допомогою якого можна буде спостерігати за тим, що відбувається в оселі та передбачувати недопустимі ситуації.

**Об'єкт дослідження** – методи та засоби візуального моніторингу оселі.

**Предмет дослідження** – Автономний комплекс візуального моніторингу оселі на базі ESP32-CAM.

**Актуальність теми кваліфікаційної бакалаврської роботи** полягає у розробці автономного комплексу візуального моніторингу оселі для інформування власників або орендарів житлових приміщень для попередження незаконного проникнення до оселі.

**Метою бакалаврської кваліфікаційної роботи** є створення системи, яка забезпечує постійний нагляд та контроль за безпекою, доступом та станом будинку в режимі реального часу. Цей комплекс має на меті підвищити рівень безпеки, зручність та ефективність управління будинком, забезпечуючи його власникам спокій та впевненість у їхньому житловому просторі.

В першому розділі виконано огляд патентної інформації та наукових публікацій, також оглянуто існуючі рішення на ринку та встановлено основні задачі та вимоги до виконання кваліфікаційної бакалаврської роботи.

В другому розділі розглянуто тему безпеки будинку, використання комп'ютерного зору в системах моніторингу, також проаналізовано систему моніторингу в реальному часі та розроблено алгоритм роботи комплексу.

Третій розділ присвячений вибору компонентної бази, розробці апаратної частини комплексу та розробці програмної частини комплексу.

Додатки містять код програмного забезпечення та принципові схеми.

У висновку описано результати виконання кваліфікаційної роботи.

В спеціальній частині з охорони праці розглянуто безпеку при виробництві автономних комплексів та запобігання непередбачуваних ситуацій.

У додатку А наведено програмний код автономного комплексу візуального моніторингу оселі. У додатку Б довідка. В цілому, бакалаврська робота без додатків містить 60 сторінок, 30 ілюстрацій, 3 таблиці, 2 схеми, 15 джерел посилань.

Ключові слова: автономний комплекс, безпека, моніторинг.

## **ABSTRACT**

of the Bachelor's Thesis

"Autonomous complex for visual monitoring of the house"

Student : Kochetov Konstantin

Supervisor: Senior Lecturer Darnapuk Yevhen

This work is devoted to the development of an autonomous visual home monitoring system. The main goal of the project is to create a device that can be used to monitor what is happening in the home and to anticipate unacceptable situations.

Object of work – methods and means of visual monitoring of the home.

Subject of work – Autonomous complex of visual monitoring of the house based on ESP32-CAM.

The relevance of the topic – is to develop an autonomous complex of visual monitoring of the home to inform the owners or tenants of residential premises to prevent illegal entry into the home.

Objective – The objective is to create a system that provides continuous surveillance and control over the security, access, and condition of the home in real time. This complex aims to increase the level of security, convenience and efficiency of home management, providing its owners with peace of mind and confidence in their living space.

The first chapter reviews patent information and scientific publications, as well as reviews existing solutions on the market and sets out the main tasks and requirements for the bachelor's thesis.

The second chapter discusses the topic of home security, the use of computer vision in monitoring systems, and analyzes the real-time monitoring system and develops an algorithm for the complex.

The third section is devoted to the selection of the component base, the development of the hardware part of the complex, and the development of the software part of the complex.

The appendices contain the software code and schematic diagrams.

The conclusion describes the results of the qualification work.

The special part on labor protection considers safety in the production of autonomous systems and the prevention of unforeseen situations.

Appendix A contains the program code of the autonomous visual home monitoring system. Appendix B is a reference. In total, the bachelor's thesis without appendices contains 60 pages, 30 illustrations, 3 tables, 2 diagrams, and 15 references.

**Keywords:** autonomous complex, security, monitoring.



## ЗМІСТ

<b>ПЕРЕЛІК СКОРОЧЕНЬ.....</b>	<b>3</b>
<b>ВСТУП.....</b>	<b>4</b>
<b>1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ВІЗУАЛЬНОГО МОНІТОРИНГУ ДЛЯ БУДИНКІВ.....</b>	<b>6</b>
1.1 Огляд патентної інформації та наукових публікацій.....	6
1.2 Огляд існуючих рішень на ринку.....	12
1.3 Формування вимог до автономного комплексу моніторингу.....	19
Висновки до розділу 1.....	20
<b>2 МЕТОДИ ТА ЗАСОБИ КОМПЛЕКСУ ВІЗУАЛЬНОГО АВТОНОМНОГО МОНІТОРИНГУ ОСЕЛІ.....</b>	<b>22</b>
2.1 Безпека будинку.....	22
2.2 Використання комп'ютерного зору в системах моніторингу.....	25
2.3 Система безпеки для розумного будинку на основі технології IoT.....	28
2.4 Система моніторингу в реальному часі.....	29
2.5 Алгоритм роботи комплексу.....	30
Висновки до розділу 2.....	32
<b>3 РЕАЛІЗАЦІЯ АВТОНОМНОГО КОМПЛЕКСУ ВІЗУАЛЬНОГО МОНІТОРИНГУ ОСЕЛІ.....</b>	<b>34</b>
3.1 Вибір компонентної бази.....	34
3.2 Розробка апаратної частини комплексу.....	42
3.3 Розробка програмної частини комплексу.....	46
Висновки до розділу 3.....	55
<b>ВИСНОВКИ.....</b>	<b>57</b>
<b>ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....</b>	<b>59</b>
<b>ДОДАТОК А ДОВІДКА.....</b>	<b>61</b>
<b>ДОДАТОК Б ПРОГРАМНИЙ КОД АВТОНОМНОГО КОМПЛЕКСУ ВІЗУАЛЬНОГО МОНІТОРИНГУ ОСЕЛІ.....</b>	<b>62</b>

## **ПЕРЕЛІК СКОРОЧЕНЬ**

GPIO	–	General-Purpose Input/Output
HoS		House of Safety
HoQ		House of Quality
HTTP	–	Hypertext Transfer Protocol
IDE	–	Integrated Development Environment
IoT	–	Internet of Things
SSL	–	Sound Source Localization
TCP	–	Transmission Control Protocol

## ВСТУП

У сучасному світі зростає значущість безпеки та контролю над нашими будинками. Забезпечення захисту, ефективного управління та нагляду за будинком та його оточуючою територією є пріоритетом для багатьох людей. Виникає потреба у розробці нових технологічних рішень, які забезпечують надійний моніторинг і контроль за будинком, зокрема у візуальному аспекті. Одним з інноваційних напрямків у цій сфері є автономні комплекси візуального моніторингу, що поєднують в собі передові технології з області комп'ютерного зору, бездротового зв'язку та сенсорів.

Кваліфікаційна робота присвячена розробці та реалізації автономного комплексу візуального моніторингу будинку.

**Актуальність кваліфікаційної роботи** полягає у розробці автономного комплексу візуального моніторингу оселі для інформування власників або орендарів житлових приміщень для попередження незаконного проникнення до оселі.

**Метою** є забезпечення постійного нагляду та контролю за безпекою, доступом та станом будинку в режимі реального часу. Створений комплекс має на меті підвищити рівень безпеки, зручність та ефективність управління будинком, забезпечуючи його власникам спокій та впевненість у їхньому житловому просторі.

**Об'єкт:** методи та засоби візуального моніторингу оселі.

**Предмет:** Автономний комплекс візуального моніторингу оселі на базі ESP32-CAM.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- проведення порівняльного аналізу існуючих технічних рішень;
- обґрунтування вибору необхідних компонентів;
- створення блок-схем та алгоритмів роботи комплексу візуального моніторингу оселі;

– визначення функціональних вимоги комплексу, включаючи відеоспостереження, запис відеоматеріалу, віддалений доступ та керування системою, а також інтеграцію з датчиками руху та системою контролю доступу;

- проектування комплексу на базі ESP32-CAM;
- реалізація комплексу та створення прототипу.

### **Практичне значення отриманих результатів**

Отримані результати мають велике практичне значення, оскільки відкривають можливість створення автономного комплексу моніторингу оселі. Розроблений комплекс забезпечує власників та інших афільованих осіб надійною інформацією щодо будь-яких змін, що відбуваються у приміщенні, а також сповіщає про незаконні проникнення. Такий комплекс дозволяє оперативно реагувати на події та забезпечує підвищену безпеку для мешканців та власників приміщень. А також допомагає запобігти можливим злочинам, забезпечує контроль за доступом до приміщень і забезпечує спокій та комфорт у житлових просторах. Такий комплекс є ефективним інструментом для забезпечення безпеки і захисту власності, дозволяючи вчасно реагувати на будь-які небажані події та забезпечувати відповідні заходи безпеки.

# 1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ВІЗУАЛЬНОГО МОНІТОРИНГУ ДЛЯ БУДИНКІВ

## 1.1 Огляд патентної інформації та наукових публікацій

Проблема моніторингу осель та приміщень не є новою, і вона містить величезний шар наукових публікацій та патентної інформації в сфері розробок автономних систем охорони та моніторингу приміщень. Наукові статті, що присвячені цій темі, виявляють різнобічні аспекти таких систем, включаючи методи та алгоритми детекції, відеоспостереження, виявлення вторгнень, розпізнавання образів та звуків, а також інтеграцію з сучасними мережевими технологіями і зв'язком. Патентна інформація розкриває широкий спектр інноваційних рішень, що включають в себе розробку нових сенсорних пристроїв, бездротових комунікаційних технологій, систем розпізнавання біометричних даних, та інших технологічних вдосконалень. Використання розумних алгоритмів та штучного інтелекту значно полегшує автоматизований аналіз і обробку великого обсягу даних, забезпечуючи високу ефективність та точність систем охорони будинку.

В патенті US11288650B2. «Поєднання взаємодії комп'ютерного зору з комп'ютерним кіоском» описується система і спосіб для зв'язування спостережуваної людської активності на відео з обліковим записом користувача у переважному варіанті [1]. Ця система включає в себе три способи взаємодії. Перший спосіб – за допомогою системи моніторингу комп'ютерного зору виявлення та відстеження людини як змодельованої комп'ютерним зором особи в середовищі, причому система моніторингу комп'ютерного зору є частиною обчислювальної платформи, що керує процесом взаємодії користувача. Другий – за допомогою принаймні одного асоціативного механізму встановлення зв'язку між змодельованою комп'ютерним зором особою та принаймні одним асоціативним елементом і, таким чином, пов'язування змодельованої комп'ютерним зором особи з обліковим записом користувача, пов'язаним за допомогою асоціативного

елемента. Третій – керування процесом взаємодії користувача, щонайменше, частково, на основі комбінації змодельованої особи та принаймні облікового запису користувача.

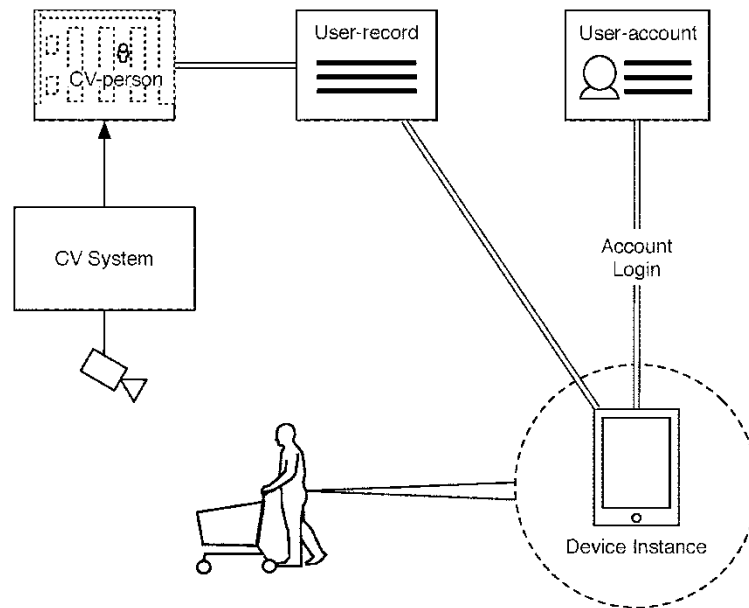


Рисунок 1.1 – Структура патенту US11288650B2

В патенті US11210526B2 «Система відеоспостереження, пристрій, метод та програма обробки відео» [2] описується пристрій обробки відео, що містить відеоаналізатор, який аналізує відеодані, захоплені камерою спостереження, виявляє подію, що належить до певної категорії, і виводить результат виявлення, контролер відображення, який відображає разом з відеоданими екран встановлення категорії для встановлення категорії події, включеної у відео, і накопичувач навчальних даних, який накопичує як навчальні дані разом з відеоданими інформацію про категорію, встановлену відповідно до операції, виконаної оператором на екрані встановлення категорії. Відеоаналізатор виконує обробку навчання, використовуючи навчальні дані, накопичені в накопичувачі навчальних даних.

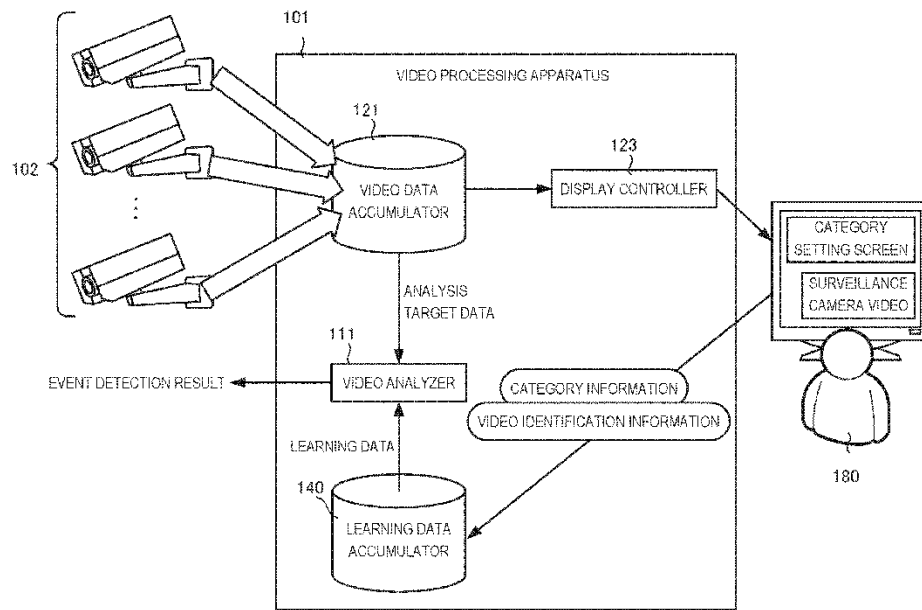


Рисунок 1.2 – Структура патенту US11210526B2

У публікації [3] описано способи обробки відео для систем охорони приміщень. В роботі представлено інтелектуальну систему спостереження та моніторингу, яка складається із захоплення зображень у реальному часі, передачі, обробки та розуміння інформації спостереження. Ця інформація є життєво важливою для безпеки людей і навіть національної безпеки. Обробка та аналіз відеоінформації для системи відеоспостереження є пілотним проєктом із реалізації такої інтелектуальної системи відеоспостереження, розробленої авторами. Розроблена система складається з 6 частин, а саме: реконструкція зображення з високою роздільною здатністю, виявлення підозрілих, відстеження підозрілих, виділення зовнішнього вигляду підозрілих, аналіз підозрілої активності та рішення про рівень обізнаності. Вихідною інформацією із запропонованої системи є підозрілі ознаки, шаблон і напрямок підозрілої діяльності та рівень підозрілого інциденту.

Робота [4] описує метод узагальнення відео з декількома видами (Multi-view video summarization, MVS) – це менш зайвий і більш стислий спосіб надання інформації з відеовмісту всіх камер у формі ключових кадрів або відеосегментів. У цьому документі представлено огляд існуючих стратегій, запропонованих для MVS, включаючи їхні переваги та недоліки. Робота охоплює загальні кроки в MVS, такі як попередня обробка відеоданих,

вилучення функцій і постобробка з подальшим створенням підсумків. Описано набори даних, які доступні для оцінки MVS. Розглянуто основні поточні проблеми, пов'язані з MVS.

У роботі [5] представлено комплексну методологію процесу прийняття рішень щодо організаційної безпеки та проектування системи безпеки. Він ґрунтується на домі якості (HoQ) (матриці планування вимог клієнта) шляхом розробки дому безпеки (the House of Quality, HoS), який може перевести ймовірність і серйозність сценаріїв атак на організації в структуру, що включає компоненти системи безпеки, ранжовані відповідно до їх ймовірної ефективності у запобіганні нападу. Ми припускаємо, що кореляції між компонентами системи можуть бути змінені для кожного сценарію, тобто кількох дахів, відповідно до кількості рядків у матриці HoS. Для порівняння різних систем безпеки, призначених для запобігання однаковим загрозам, запропоновано міру ефективності. Метод дисперсійного аналізу використовується для вибору життєво важливих компонентів безпеки шляхом поділу компонентів безпеки на дві групи: життєво мало та тривіально багато. Метод HoS реалізований для захисту готелю від терористичної атаки, виявляючи п'ять компонентів як домінуючих для безпеки: операційні процедури, телекамери, внутрішній персонал, контроль входу та аналіз візуальної інформації. Частковий аналіз для визначення найважливішого компонента для захисту конкретного місця (стоянки) показує, що кількість життєво важливих компонентів зменшується, а домінуючими компонентами для запобігання загрозам для паркування є робочі процедури та внутрішній персонал.

У статті [6] представлено розробку та впровадження вебсистеми домашньої безпеки та автоматизації. Ця система використовує датчик руху PIR для виявлення зловмисників у будинку. Цей датчик далі подається на мікроконтролер, який допоможе модулю GSM надіслати сповіщення власнику будинку про вторгнення. З іншого боку, датчик світла LDR використовується для забезпечення функції автоматичного освітлення, яка вмикатиме світло



вночі та приглушуватиме його вдень. Вебсистема функціонує як система дистанційного керування, за допомогою якої користувач може контролювати датчики та освітлення вдома з метою економії споживання енергії. Ця система доступна для користувача в будь-який час і в будь-якому місці, якщо є підключення до Інтернету.

Запропонована методологія дослідження [7] має на меті розробку загальної реалізованої структури для надання власнику/учаснику будинку негайного повідомлення про триваючу крадіжку (несанкціонований доступ до їхніх приміщень). Згідно з визначеною метою в роботі проведено ретельний аналіз існуючих систем, щоб виявити прогалини в попередніх подібних дослідженнях. Проблеми, виявлені в існуючих системах, полягали в тому, що вони можуть ідентифікувати зловмисника лише після крадіжки або не можуть розрізнити об'єкти, які не є людьми. Бездротові сенсорні мережі (WSN) у поєднанні з використанням Інтернету речей (IoT) і когнітивного Інтернету речей розширюють концепції та рішення розумного дому та їх застосування. У цьому дослідженні пропонується нова протиугінна система розумного дому, яка може виявити зловмисника, навіть якщо він частково/повністю приховав своє обличчя за допомогою одягу, шкіри, волокна або пластику. Запропонована система також може виявити зловмисника в темряві за допомогою камери відеоспостереження без можливості нічного бачення. Фундаментальна ідея полягала в тому, щоб розробити рентабельну та ефективну систему, щоб окрема особа могла виявляти будь-який вид крадіжки в режимі реального часу та миттєво сповіщати про крадіжку власника будинку. Система також обіцяє запровадити домашню безпеку з обробкою великих відеоданих у режимі реального часу. Результати дослідження підтверджують успішність запропонованої системи. Точність системи була підвищена до 97,01 %, 84,13 %, 78,19 % і 66,5 % у сценаріях, коли виявлений зловмисник не ховав своє обличчя, частково, повністю ховав своє обличчя та був виявлений у темряві з 85 %, 64,13 %, 56,70 % і 44,01 %.

Робота [8] описує сенсорну охоронну систему розумного будинку. Вона складається з кількох електронних пристроїв, таких як камера, датчик і пристрій бездротового зв'язку, які надають власникам віддалений доступ до системи безпеки, а також на бездротові пристрої вони отримують SMS-повідомлення. Є багато пристроїв камери, які можуть постійно стежити за сайтами. Пристрої камери складаються з PIR-датчиків, які використовуються для функцій виявлення руху та передають незвичні сигнали звітів про стан і необхідну інформацію про зображення на комунікаційний пристрій, коли спостерігаються рухи невідомої особи. Бездротовий зв'язок або SMS-зв'язок здійснюється через модуль GSM. Для передачі попереджувальної інформації в цілях безпеки використовується SMS-зв'язок. Якщо невідома особа намагається проникнути в будинок, на мобільний телефон, до якого приєднаний пристрій, надсилається сигнал тривоги, який інформує особу про присутність когось у будинку, а власника немає вдома. Потім власник будинку може вжити будь-яких дій, наприклад, викликати поліцію або свою сім'ю, щоб захистити свій будинок від невідомого зловмисника. Коли пристрій знаходиться в активному режимі, він також починає подавати сигнал тривоги, якщо в будівлю заходить невідома особа.

У дослідженні [9] обговорюється створення операційної системи домашньої автоматизації. Оскільки інноваційні системи для дому пропонують різні застосунки, які спрощують роботу, цифрове суспільство надзвичайно захоплюється ними. Сучасні бездротові технології та можливості онлайн-замовлення побутової техніки роблять життя мешканців простішим і більш організованим. Запропонована система спрямована на допомогу людям похилого віку та особам із фізичними вадами, надаючи підтримку та керуючи побутовою технікою. Реле використовуються в конструкції для фізичного підключення побутової техніки до вихідних портів вбудованої плати контролера. Продемонстровано систему, яка використовує цифрового помічника, такого як MPU6050, для отримання команд від людей з вадами, які використовують свої руки більш природно, наприклад, вмикають або

вимикають повсякденні електричні пристрої. Щоб увімкнути або вимкнути електропобутові прилади, підключені до яскравого подовжувача, або розумну Arduino, цифровий помічник може підключитися до них. Людині з обмеженими можливостями потрібно лише порухати рукою, щоб увімкнути або вимкнути прилад, змінивши положення MPU6050.

## 1.2 Огляд існуючих рішень на ринку

У сучасному світі, де безпека та зручність є важливими аспектами повсякденного життя, системи автономного візуального моніторингу будинків набувають все більшої популярності. Ці системи забезпечують постійний контроль за безпекою та дозволяють користувачам спостерігати за своїм житлом, навіть коли вони знаходяться віддалено. На ринку існує ряд комерційних аналогів, де одним з провідних виробників є компанія Ajax Systems. Їхні продукти відзначаються високою якістю, надійністю та функціональністю, що робить їх привабливим вибором для широкого кола користувачів.

Одним з ключових продуктів компанії Ajax Systems, який варто відзначити, є Ajax Hub 2 Plus (рис. 1.3) [10]. Цей пристрій є центральним елементом системи автономного візуального моніторингу будинків, забезпечуючи інтеграцію та керування всіма підключеними пристроями. Ajax Hub 2 Plus поєднує в собі передові технології та функціонал, що робить його потужним і надійним рішенням для забезпечення безпеки будинків. Він підтримує підключення бездротових датчиків різних типів, включаючи датчики руху, дверей та вікон, газові датчики, пожежні датчики та багато інших. Крім того, Ajax Hub 2 Plus забезпечує можливість відеомоніторингу за допомогою підключення камер безпеки. Завдяки вбудованому 4G-модулю, цей пристрій може функціонувати навіть при відсутності основного Інтернет-підключення або в разі відключення живлення. Завдяки всім цим функціям Ajax Hub 2 Plus заслужено визнаний як потужний і надійний пристрій для створення систем автономного візуального моніторингу будинків.



Рисунок 1.3 – Ajax Hub 2 Plus

Ajax MotionCam є також одним з ключових продуктів компанії Ajax Systems, який входить до складу системи автономного візуального моніторингу будинків (рис. 1.4). Цей датчик руху володіє рядом характеристик, що роблять його ефективним та надійним засобом забезпечення безпеки. Однією з головних особливостей Ajax MotionCam є його комбінована функціональність. Він поєднує в собі дві важливі функції: детекцію руху та відеозапис. Це дозволяє не лише виявляти рух у приміщенні, але й отримувати відеозаписи подій, що відбуваються, забезпечуючи додаткові дані для аналізу та вжиття заходів безпеки.



Рисунок 1.4 – Ajax MotionCam

Ajax MotionCam [11] працює на основі передової технології PIR-детектора, що забезпечує високу точність виявлення руху та мінімізує випадкові спрацювання. Це важливо для зменшення помилкових спрацювань і забезпечення надійної роботи системи. Оснащений вбудованою фотокамерою високої роздільної здатності, Ajax MotionCam дозволяє отримувати відеозаписи в режимі реального часу або зафіксувати фотографії під час виявлення руху. Це забезпечує додаткові докази та візуальну інформацію для аналізу подій та прийняття відповідних заходів.

Ajax MotionCam підтримує бездротове підключення до Ajax Hub 2 Plus, що дозволяє просту і швидку інтеграцію з системою моніторингу будинку. Він має вбудований акумулятор, що забезпечує роботу пристрою навіть при відключенні живлення, і може працювати в режимі очікування до 7 років.

Важливо зазначити, що Ajax MotionCam використовує передову систему шифрування Jeweller, що забезпечує високий рівень захисту передачі даних. Це робить його вразливим до піратства та несанкціонованого доступу.



Рисунок 1.5 – Система безпеки Vivint Smart Home

Система безпеки Vivint Smart Home [12] – це повноцінна система домашньої безпеки, яка забезпечує цілодобовий моніторинг і повний контроль над дверними замками, камерами, термостатами та освітленням (рис. 1.5). Однією з ключових особливостей Vivint Smart Home є їхній центральний контролер, який дозволяє користувачам керувати всіма підключеними до системи пристроями. Цей контролер може бути управлінням через спеціальну мобільну програму або зручними голосовими командами. Він дозволяє користувачам контролювати освітлення, температуру, систему безпеки, аудіо-та відеообладнання та багато іншого. Завдяки цьому, користувачі можуть налаштовувати свій будинок за власними уподобаннями та потребами. Складові компоненти системи включають наступні характеристики та властивості:

1) відеокамери: Vivint Smart Home пропонує різні типи відеокамер, включаючи внутрішні та зовнішні моделі. Вони мають високу роздільну здатність і можуть записувати відео у реальному часі. Камери оснащені функціями детекції руху, нічного бачення та зберігання відеозаписів на хмарному сервері;

2) система тривоги: Vivint Smart Home включає датчики руху, датчики дверей та вікон, які спрацьовують у разі виявлення незвичайних рухів або

вторгнення. Це сповіщає власника про потенційно небезпечні ситуації та може викликати аварійну допомогу у разі потреби;

3) мобільний застосунок: Користувачі можуть контролювати та моніторити свій будинок з використанням спеціального мобільного застосунку. Це дозволяє переглядати живі відеопотоки, отримувати сповіщення про події, включати або вимикати систему безпеки та керувати іншими функціями будинку віддалено;

4) хмарне зберігання: Відеозаписи, зняті відеокамерами, можуть бути збережені на хмарному сервері, що дозволяє користувачам переглядати архівні записи в будь-який час. Це забезпечує збереження важливих відеоматеріалів та можливість їх подальшого використання;

5) інтеграція з іншими системами: Vivint Smart Home може інтегруватись з іншими смарт-пристроями та системами в будинку, такими як освітлення, термостати, замки на дверях та інші. Це дозволяє створити цілісну систему управління будинком і спрощує керування всіма функціями з одного інтерфейсу.

Перевагами даного комплексу є:

1) швидка реакція на події. Комплекс забезпечує оперативну реакцію на події та повідомлення про них, що дозволяє оперативно реагувати на потенційні загрози або несподівані ситуації;

2) відмінний відеодзвінок. Комплекс забезпечує якісний відеодзвінок, що дозволяє взаємодіяти зі звіреними особами перед відкриттям дверей або виконанням інших дій;

3) дистанційне керування. Комплекс надає можливість дистанційного керування дверними замками, камерами, термостатами та датчиками, що забезпечує зручність та контроль над системою;

4) чутливий сенсорний екран. Комплекс має чутливий сенсорний екран, що спрощує взаємодію з системою та забезпечує зручне управління;

5) відсутність необхідності у тривалому контракті. Використання даного комплексу не потребує укладання тривалого контракту, що забезпечує більшу гнучкість та свободу в користуванні;

б) підтримка голосових команд Alexa та Google. Комплекс підтримує голосові команди з використанням популярних платформ, таких як Alexa та Google, що дозволяє зручно керувати системою безпеки.

Також визначено наступні недоліки:

1) щомісячна підписка на віддалений доступ. Для отримання віддаленого доступу до комплексу може бути необхідна щомісячна підписка, що може бути фінансовою витратою для користувача;

2) відсутність можливості налаштування звуків будильника. Комплекс може не мати можливості налаштовувати звуки будильника, що може бути обмеженням для деяких користувачів;

3) висока вартість компонентів. Деякі компоненти комплексу можуть бути дорогими, що може вплинути на загальну вартість системи та доступність для деяких користувачів.



Рисунок 1.6 – Система домашньої безпеки ADT Command

ADT Command [13] є потужним автономним комплексом візуального моніторингу будинку, розробленим компанією ADT, світовим лідером в галузі систем безпеки та моніторингу. Цей комплекс надає користувачам надійний



захист та контроль над їхнім житлом за допомогою передових технологій та інтелектуальних рішень (рис. 1.6). ADT Command пропонує широкий спектр характеристик та функцій, що роблять його привабливим вибором для тих, хто прагне забезпечити безпеку та контроль за своїм будинком. Однією з головних характеристик ADT Command є його інтегрована система відеоспостереження.

Комплекс включає в себе високоякісні відеокамери, розміщені у стратегічних місцях навколо будинку, що дозволяють отримувати якісний відеозапис у реальному часі. Ці камери мають вбудовану функцію рухомого датчика, що дозволяє автоматично включати запис при виявленні руху, а також можливість записувати відео високої роздільної здатності.

ADT Command також пропонує інтелектуальну систему детекції. Завдяки передовим алгоритмам розпізнавання, комплекс здатний розрізняти між рухом людей, транспортними засобами та іншими об'єктами, що зменшує кількість надійних сповіщень та позитивно впливає на ефективність моніторингу.

Крім того, ADT Command включає в себе інтерфейс керування та контролю, доступний через панель керування, мобільний застосунок та голосові команди. Це дозволяє користувачам зручно керувати різними функціями системи, включаючи активацію/деактивацію системи безпеки, перегляд відеозаписів та отримання сповіщень про події у будинку.

Значною перевагою ADT Command є його висока надійність та швидкість реагування. Комплекс підтримує безперебійний зв'язок зі спеціалізованим центром моніторингу ADT, який працює цілодобово. У разі виявлення надзвичайної ситуації, як-от вторгнення або пожежі, система негайно сповіщає відповідних експертів та активує необхідні заходи безпеки.

Враховуючи наведений опис аналогів, автономний комплекс візуального моніторингу оселі повинен включати в себе наступні складові компоненти для забезпечення його ефективності та функціональності:

- 1) центральний контролер керування комплексом: Цей центральний пристрій відповідає за керування та координацію роботи всього комплексу.

Він приймає дані від різних датчиків та камер, обробляє їх і забезпечує виведення необхідної інформації;

2) камери, що під'єднані до центрального контролера: Для забезпечення візуального спостереження важливо мати встановлені камери, які передають зображення та відео до центрального контролера. Це дозволяє відстежувати події та зміни, що відбуваються в режимі реального часу;

3) додаткові сенсори: Для збільшення функціональності комплексу важливо використовувати додаткові сенсори, такі як сенсори руху, газу, вологості та відкриття дверей. Вони допомагають виявляти відхилення від норми і вчасно сповіщати про можливі небезпеки або незвичайні події;

4) модуль виведення інформації: Для зручного доступу до отриманої інформації необхідний модуль виведення, який може бути у формі застосунку, вебсайту управління комплексом або фізичного пристрою з екраном. Цей модуль дозволяє користувачам отримувати інформацію про стан оселі, відеозаписи або сповіщення в зручний для них спосіб.

Застосування цих компонентів у автономному комплексі моніторингу оселі забезпечує ефективну роботу системи та надає користувачам можливість контролювати та захищати своє житло зручним та надійним способом

### **1.3 Формування вимог до автономного комплексу моніторингу**

Виходячи зі структури та функціоналу наявних систем моніторингу осель на ринку, можна сформувані наступні вимоги до комплексу:

1) відеозапис. Комплекс повинен мати здатність записувати відео у високій роздільній здатності та забезпечувати стабільну передачу відеопотоку на сервер або зберігати його локально;

2) руховий датчик. Система повинна включати руховий датчик, який спрацьовує при виявленні руху у зоні моніторингу. Це дозволить активувати відеозапис та сповістити користувача про потенційно небезпечну ситуацію;

3) датчики дверей та вікон. Додаткові датчики дверей та вікон можуть бути використані для виявлення незаконного вторгнення. Комплекс повинен

здатися на виявлення відкриття або закриття дверей та вікон та сповіщати про це користувача;

4) датчики пожежі. Важливо включити датчики пожежі для виявлення диму або збільшення температури. Це дозволить вчасно виявити пожежу та прийняти необхідні заходи безпеки;

5) система сповіщення. Комплекс повинен мати можливість сповіщати користувача про події, що відбуваються в будинку. Це може бути здійснено через мобільний застосунок, електронну пошту або SMS-повідомлення;

6) інтеграція з іншими системами. Важливо, щоб комплекс був сумісний з іншими системами автономного контролю будинку, такими як освітлення, термостати, замки та інші. Це забезпечить цілісну систему управління будинком;

7) енергоефективність. Комплекс повинен бути спроектований з урахуванням енергоефективності, забезпечуючи довготривалу роботу на батарейному живленні або низьке споживання електроенергії;

8) інтерфейс користувача. Комплекс повинен мати зручний інтерфейс користувача, який дозволяє легко налаштовувати, керувати та переглядати дані з системи візуального моніторингу.

## **Висновки до розділу 1**

В першому розділі кваліфікаційної бакалаврської роботи проаналізовано патентну інформацію та наукові публікації, що дозволило отримати цінні уявлення про існуючі технологічні рішення у галузі візуального моніторингу для будинків. Розглянуто та проаналізовано існуючі рішення на ринку, включаючи комерційні продукти та відкриті розробки. Проведений аналіз надав інформацію про технології, функціональні можливості та особливості доступних рішень, дозволив визначити мету роботи та завдання для її досягнення.

Сформульовані вимоги до автономного комплексу моніторингу, враховуючи отриману інформацію з огляду патентної інформації, наукових

публікацій та огляду існуючих рішень. Вимоги допоможуть забезпечити ефективну реалізацію моніторингової системи з використанням сучасних технологій візуального спостереження для будинків.

Загальною метою цього розділу було оглянути і проаналізувати сучасні технології візуального моніторингу для будинків. Дані кроки надали необхідну інформацію для подальшого проектування та розробки моніторингової системи з використанням найкращих доступних технологій візуального спостереження.

## 2 МЕТОДИ ТА ЗАСОБИ КОМПЛЕКСУ ВІЗУАЛЬНОГО АВТОНОМНОГО МОНІТОРИНГУ ОСЕЛІ

### 2.1 Безпека будинку

У сфері безпеки, менеджери повинні завжди бути готові до заходів, щоб запобігти терористичним або кримінальним атакам на будівлю. Для цього важливо мати комплексний підхід, який охоплює методологію прийняття рішень щодо безпеки будинку та проєктування системи безпеки. Ця методологія ґрунтується на концепції «будинку якості» (HoQ) або матриці планування вимог замовника (рис. 2.1). Вона допомагає розробити «будинок безпеки» (HoS) – комплексний підхід до забезпечення безпеки будівлі та її мешканців.

Методологія «будинку якості» (HoQ) використовується для систематичного аналізу вимог замовника щодо безпеки будинку. Це включає визначення потреб, очікувань та пріоритетів з точки зору безпеки. Застосування матриці планування вимог замовника дозволяє ідентифікувати ключові аспекти безпеки, які необхідно враховувати при проєктуванні системи безпеки будинку.

Концепція «будинку безпеки» (HoS) передбачає створення інтегрованої системи безпеки, яка охоплює фізичні, технічні та організаційні заходи. Ця система може включати в себе відеоспостереження, системи контролю доступу, пожежну сигналізацію, інтеграцію з охоронними службами та інші аспекти безпеки, що забезпечують цілісну захищеність будівлі та її мешканців.

Завдяки такому комплексному підходу до безпеки будинку, менеджери з безпеки можуть ефективно враховувати потреби та вимоги замовника, розробляти належні стратегії та виконувати необхідні заходи для забезпечення безпеки будівлі. Це допомагає запобігти потенційним загрозам та забезпечує спокій та захищеність для мешканців.

Концепція «будинку якості» (HoQ) використовується для забезпечення високої якості будівель та задоволення потреб клієнтів. Ця концепція

базується на тому, щоб виявити, розуміти і задовольняти вимоги та очікування клієнтів на кожному етапі проектування, будівництва та експлуатації будівлі.

Таблиця 2.1 – Основні складові концепції «будинку якості» (HoQ)

<b>Складова концепції</b>	<b>Опис</b>
Вимоги клієнтів	Виявлення та аналіз вимог та очікувань клієнтів.
Планування	Розроблення стратегічного плану, що враховує вимоги клієнтів.
Проектування	Розроблення детальних проєктів з урахуванням вимог клієнтів.
Будівництво	Здійснення будівельних робіт з дотриманням вимог якості.
Контроль та перевірка виробництва	Систематичний контроль та перевірка якості виробництва.
Експлуатація та обслуговування	Забезпечення належної експлуатації та обслуговування будівлі.
Задоволення клієнтів	Оцінка задоволення клієнтів та внесення виправлень за потреби.

HoS перетворює ймовірність і серйозність атак на будинок в структуру, що складається з компонентів системи безпеки, класифікованих за їхньою ймовірною ефективністю у запобіганні атакам.

Застосовуючи метод HoS, можна розробити декілька варіантів систем безпеки, в залежності від конкретного сценарію атаки. Для порівняння різних систем безпеки, спрямованих на запобігання однаковим загрозам, використовується міра ефективності. Для вибору найважливіших компонентів безпеки застосовується метод дисперсійного аналізу, який ділить компоненти безпеки на дві групи: життєво важливі (vital few) і тривіальні (trivial many).

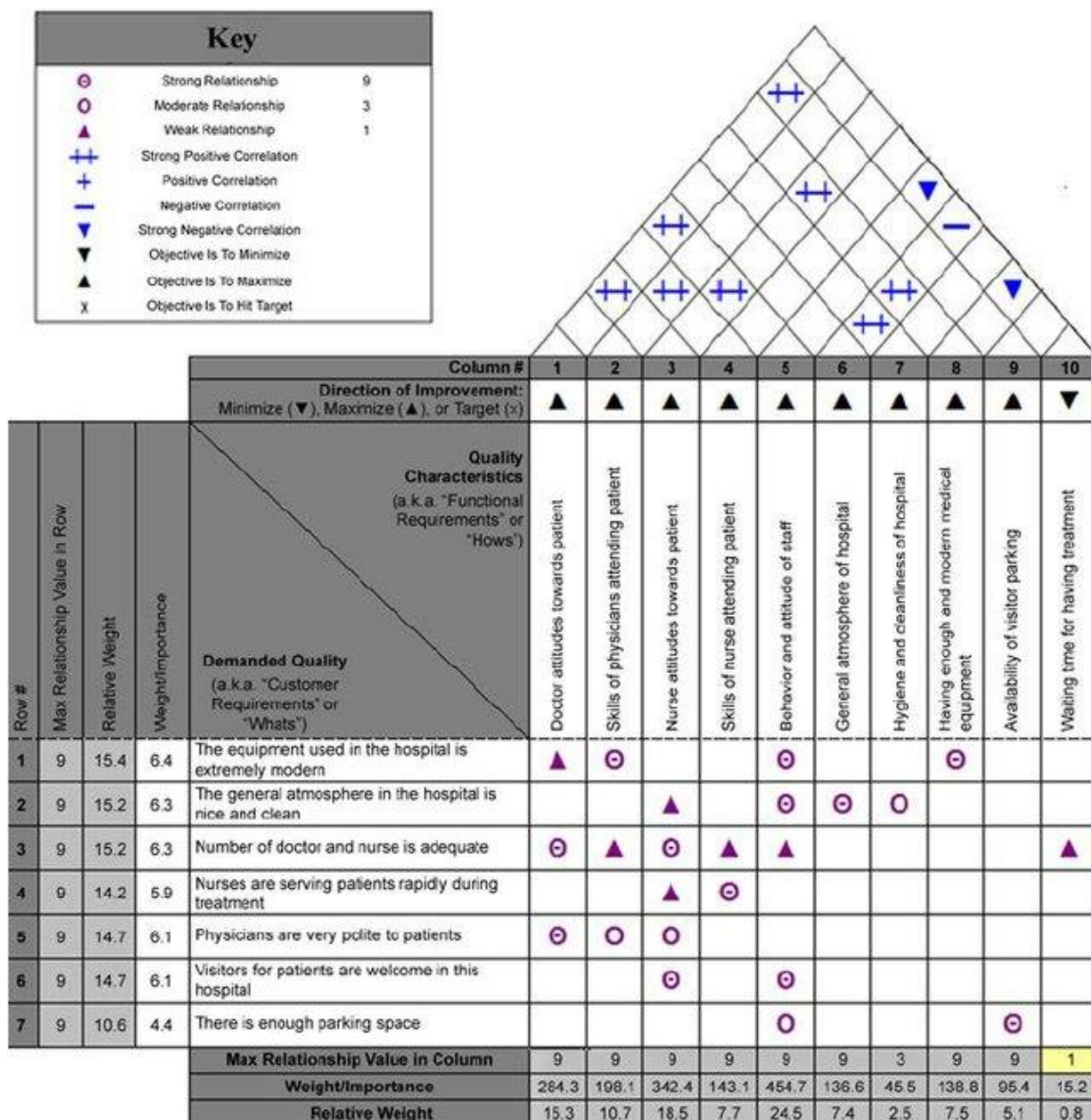


Рисунок 2.1 – Приклад будинку якості для приватної лікарні

У конкретному випадку захисту будинку від терористичної атаки, метод НоS виявив п'ять домінуючих компонентів безпеки: Операційні процедури, відеокамери, внутрішній персонал, контроль на вході та аналіз візуальної інформації. Крім того, частковий аналіз для визначення найважливішого компонента для захисту конкретної зони паркування показав, що операційні процедури та внутрішній персонал є домінуючими компонентами для запобігання загрозам на цій зоні.

В роботі розглянута методологія розробки системи безпеки для будинку, що дозволяє вибрати найефективніші компоненти безпеки для запобігання різним загрозам та атакам.

## 2.2 Використання комп'ютерного зору в системах моніторингу

Принцип роботи систем моніторингу з використанням комп'ютерного зору полягає у застосуванні спеціалізованих алгоритмів та технологій комп'ютерного зору для аналізу та інтерпретації візуальної інформації, отриманої з відеокамер або інших джерел зображень. Ці системи здатні автоматично виявляти, відслідковувати або класифікувати об'єкти, розпізнавати певні події або поведінку, а також генерувати сповіщення або вживати інші визначені дії на основі отриманих результатів. Вони забезпечують ефективний та надійний моніторинг у різних сферах, таких як безпека, транспорт, медицина та багато інших.

Переваги використання комп'ютерного зору в системах моніторингу включають:

- 1) автоматизація: комп'ютерний зір дозволяє автоматично виявляти, відстежувати та аналізувати об'єкти та події, що спрощує процес моніторингу і зменшує необхідність людського втручання;
- 2) висока швидкість та точність: технології комп'ютерного зору здатні оперативно обробляти великий обсяг візуальних даних та робити точні визначення та класифікації об'єктів;
- 3) посилення безпеки: системи моніторингу на основі комп'ютерного зору допомагають виявляти незвичайні або підозрілі події, забезпечуючи вчасне сповіщення та реагування на потенційні загрози.

Обмеження використання комп'ютерного зору в системах моніторингу можуть включати:

- залежність від якості зображень: якість вхідних зображень може впливати на ефективність системи комп'ютерного зору. Погане освітлення, рухливість або спотворення зображень можуть вплинути на точність та надійність результатів;
- складність обробки в реальному часі: вимоги до обчислювальних ресурсів та швидкості обробки можуть бути високими, особливо при



застосуванні комп'ютерного зору в реальному часі, коли великий обсяг даних потрібно аналізувати відразу;

– приватність та етичні питання: використання систем моніторингу з комп'ютерним зором може породжувати питання щодо захисту приватності та використання персональних даних. Необхідно дотримуватися відповідних правил та норм для забезпечення етичного використання цих технологій.

Сучасні технології комп'ютерного зору відкривають нові можливості для створення ефективних систем моніторингу та безпеки в домашньому середовищі. Завдяки використанню камер та спеціалізованого програмного забезпечення, системи комп'ютерного зору можуть виявляти рухомі об'єкти, розпізнавати обличчя, аналізувати поведінку та вчасно сповіщати власників про можливі загрози або небезпеки. Використання комп'ютерного зору в системах моніторингу дозволяє автоматизувати процес аналізу відеоданих і забезпечує більш ефективну та точну обробку інформації. Комп'ютерний зір використовує алгоритми та технології машинного навчання для розпізнавання об'єктів, детекції подій, аналізу поведінки та багато іншого.

Ось декілька способів використання комп'ютерного зору в системах моніторингу:

1) розпізнавання об'єктів. Комп'ютерний зір може розпізнавати різні об'єкти на відеозаписах, такі як люди, автомобілі, тварини тощо. Це дозволяє відфільтрувати незначні події та сповістити операторів про важливі події, наприклад, про вторгнення на об'єкт або загрозу безпеці;

2) виявлення руху. Комп'ютерний зір може аналізувати зміни в відеопотоці та виявляти рух. Це допомагає відокремити значущі події від незначних і дозволяє активувати сповіщення або виконати певні дії, коли виявляється рух у певній зоні;

3) відстеження об'єктів. Комп'ютерний зір може відстежувати рух об'єктів на відеозаписі. Наприклад, в системах відеоспостереження він може відстежувати рух людей або транспортних засобів і відслідковувати їх шляхи руху, що допомагає в розслідуванні подій або контролі трафіку;

4) аналіз поведінки. Комп'ютерний зір може аналізувати поведінку об'єктів на відеозаписі і виявляти незвичайні або підозрілі дії. Наприклад, система може розпізнати агресивну поведінку, падіння людини або неправильні дії на робочому місці. Це дозволяє операторам системи вчасно реагувати на потенційні небезпечні ситуації та зменшує ризик виникнення аварій або нещасних випадків;

5) аналіз трафіку та підрахунок. Комп'ютерний зір може використовуватись для аналізу трафіку на дорогах або в громадських просторах. Він може виявляти перешкоди, затори або навіть розпізнавати типи транспорту. Крім того, системи з комп'ютерним зором можуть підраховувати кількість людей, що проходять через певну зону або входять до приміщення. Це корисно для контролю потоків людей і планування безпеки.

Загалом, використання комп'ютерного зору в системах моніторингу значно покращує ефективність та точність аналізу відеоданих, дозволяє виявляти важливі події та забезпечує більш прогресивний рівень безпеки. З постійним розвитком технологій машинного навчання та комп'ютерного зору можна очікувати ще більші можливості в майбутньому.

Майбутні перспективи та розвиток використання комп'ютерного зору у системах моніторингу включають:

- покращена точність та розпізнавання: з використанням штучного інтелекту та глибокого навчання, системи комп'ютерного зору будуть здатні ще точніше ідентифікувати та класифікувати об'єкти та події;

- розширення функціональності: в застосунок до виявлення і розпізнавання об'єктів, системи комп'ютерного зору можуть розвиватися у напрямку аналізу емоцій, виявлення паттернів поведінки та прогнозування подій;

- інтеграція з іншими технологіями: комп'ютерний зір може поєднуватися з іншими технологіями, такими як датчики руху, системи відеоспостереження та «розумні» пристрої, для створення комплексних систем моніторингу та безпеки;

– застосування у різних галузях: використання комп'ютерного зору у системах моніторингу знаходить застосування в різних сферах, включаючи безпеку житла, виробництва, транспорту, медицину та багато інших.

### **2.3 Система безпеки для розумного будинку на основі технології IoT**

У сучасному світі домашня безпека стає необхідною, оскільки можливості вторгнення зростають з кожним днем. Цей дизайн використовує ідею «близьких до реального життя і простих у використанні Інтернет речей» в якості концепції дизайну і будує систему розумного будинку на основі інтернет речей. Модулі, включені в цей дизайн, включають в себе модуль вихідної плати, модуль вузла і модуль APP.

Основні реалізовані функції: ПК може відображати дані про температуру і вологість, зібрані вузловою платою, через браузер і контролювати стан перемикання світлодіодного індикатора плати керуючого вузла через браузер, а також може відображати дані про температуру і вологість, зібрані вузловою платою, через застосунок і контролювати стан перемикання світлодіодного індикатора пластини накладки. Зв'язок між ПК та вузловою платою та зв'язок між застосунком та вузловою платою повинні передаватися через плату шлюзу, тому плата шлюзу є комунікаційним мостом всієї системи. Для того, щоб реалізувати роль комунікаційного моста плати шлюзу, конструкція плати шлюзу використовує LPC1769 від NPC в якості головного MCU. Система будує контролер послуг Ethernet за допомогою вбудованого модуля Ethernet LPC1769 та мікросхеми DP83848. Побудована система шлюзу з модулем Wi-Fi, модулем NB-IOT і мікросхемою пам'яті W25Q128. Програмне забезпечення базується на операційній системі реального часу uC/OS-II, оснащене завданнями протоколу uIP та іншими модулями завдань, а також вбудованою функцією вебсервера.

## 2.4 Система моніторингу в реальному часі

Така методологія дослідження має на меті розробити загальноприйнятну систему для надання власнику/мешканцю будинку негайного повідомлення про крадіжку (несанкціонований доступ до їхнього помешкання). Для цього проведено ретельний аналіз існуючих систем для виявлення прогалин у дослідженні. Проблеми, виявлені в існуючих системах, полягали в тому, що вони можуть ідентифікувати зловмисника лише після крадіжки, або не можуть розрізнити об'єкти, що належать і не належать людині, і об'єкти, що не належать людині. Бездротові сенсорні мережі (WSN) у поєднанні з використанням Інтернету речей (IoT) та когнітивного Інтернету речей розширюють концепції та рішення для розумного будинку, а також їх застосування. У цьому дослідженні пропонується нова система захисту розумного будинку від крадіжок, яка може виявити зловмисника, навіть якщо він частково/повністю приховав своє обличчя за одягом, шкірою, волокном або пластиковими матеріалами. Запропонована система також може виявити зловмисника в темряві за допомогою камери відеоспостереження без функції нічного бачення. Основна ідея полягала в тому, щоб розробити економічну та ефективну систему, яка б дозволяла приватній особі виявити будь-яку крадіжку в режимі реального часу та миттєво сповістити про неї власника будинку. Система також обіцяє реалізувати домашню безпеку з обробкою великих обсягів відеоданих в режимі реального часу. Результати дослідження підтверджують успішність запропонованої системи. Точність системи була підвищена до 97,01 %, 84,13 %, 78,19 % і 66,5 % у сценаріях, коли виявлений зловмисник не приховував свого обличчя, приховував обличчя частково, повністю і був виявлений в темряві з 85 %, 64,13 %, 56,70 % і 44,01 %.

Методи SSL (Sound Source Localization - локалізація звукових джерел) використовуються для визначення місцезнаходження акустичних джерел шляхом аналізу інформації, яку надають датчики. У бездротових акустичних мережах це досягається за допомогою вимірювання енергії вхідних сигналів, визначення часу їх надходження або різниці в часі надходження, визначення

напрямку, з якого звук надходить, та аналізу потужності керованого відгуку, що виникає при поєднанні сигналів, отриманих з декількох мікрофонів.

Ці методи дозволяють створити точні моделі розташування акустичних джерел, що можуть мати важливе значення у багатьох сферах. Наприклад, вони можуть застосовуватися у системах безпеки для виявлення звуків, пов'язаних з потенційно небезпечними подіями, або у робототехніці для навігації рухомих об'єктів.

Використання SSL в бездротових акустичних мережах забезпечує широкий спектр можливостей. Збір і аналіз інформації від датчиків дозволяє точно визначити місцезнаходження звукових джерел і здійснити відповідні дії на основі цих даних. Отримані результати можуть бути використані для покращення безпеки, оптимізації процесів або покращення загального досвіду користувачів. Такі методи мають потенціал для подальшого розвитку і впровадження в різних галузях, де важлива точна локалізація акустичних джерел.

## **2.5 Алгоритм роботи комплексу**

Алгоритм роботи комплексу візуального моніторингу оселі складається з декількох етапів, які наведені на рис. 2.2. Цей алгоритм розроблений для ефективної і надійної роботи системи. Всього існує кілька типів «подій», на які система має реагувати.

Під «подіями» розуміються як події, детектовані сенсорами та/або камерою, про які інформація надсилається користувачеві через Telegram-бота, так і події, що виникають в результаті команд, надісланих користувачем для управління автономним комплексом візуального моніторингу оселі за допомогою бота.

Алгоритм розрахований на взаємодію між датчиками, камерою та Telegram-ботом. Коли датчики або камера виявляють певні події, вони генерують відповідні сигнали. Ці сигнали передаються до системи, яка

аналізує їх і визначає, яку дію потрібно виконати. При необхідності, система надсилає відповідну інформацію через Telegram-бота користувачеві.

З іншого боку, користувач також може взаємодіяти з системою шляхом відправки команд через Telegram-бота. Ці команди спрямовуються до автономного комплексу візуального моніторингу оселі, і система виконує відповідні дії відповідно до отриманих команд.

Таким чином, алгоритм роботи комплексу візуального моніторингу оселі забезпечує взаємодію між датчиками, камерою, Telegram-ботом та користувачем, що дозволяє ефективно контролювати та керувати системою моніторингу.

Після початку роботи комплексу, відбувається спроба підключення його до WiFi мережі. У випадку, якщо підключення не є вдалим та кількість повторних спроб перевищує п'яти, то система автоматично відключається. Наступний етап – перевірка ключа-токена доступу API для Telegram-боту. У випадку, якщо ключ не є коректним, то система так само відключається. Далі йде очікування події як зі сторони користувача, так і зі сторони навколишнього середовища на яке реагують сенсори.

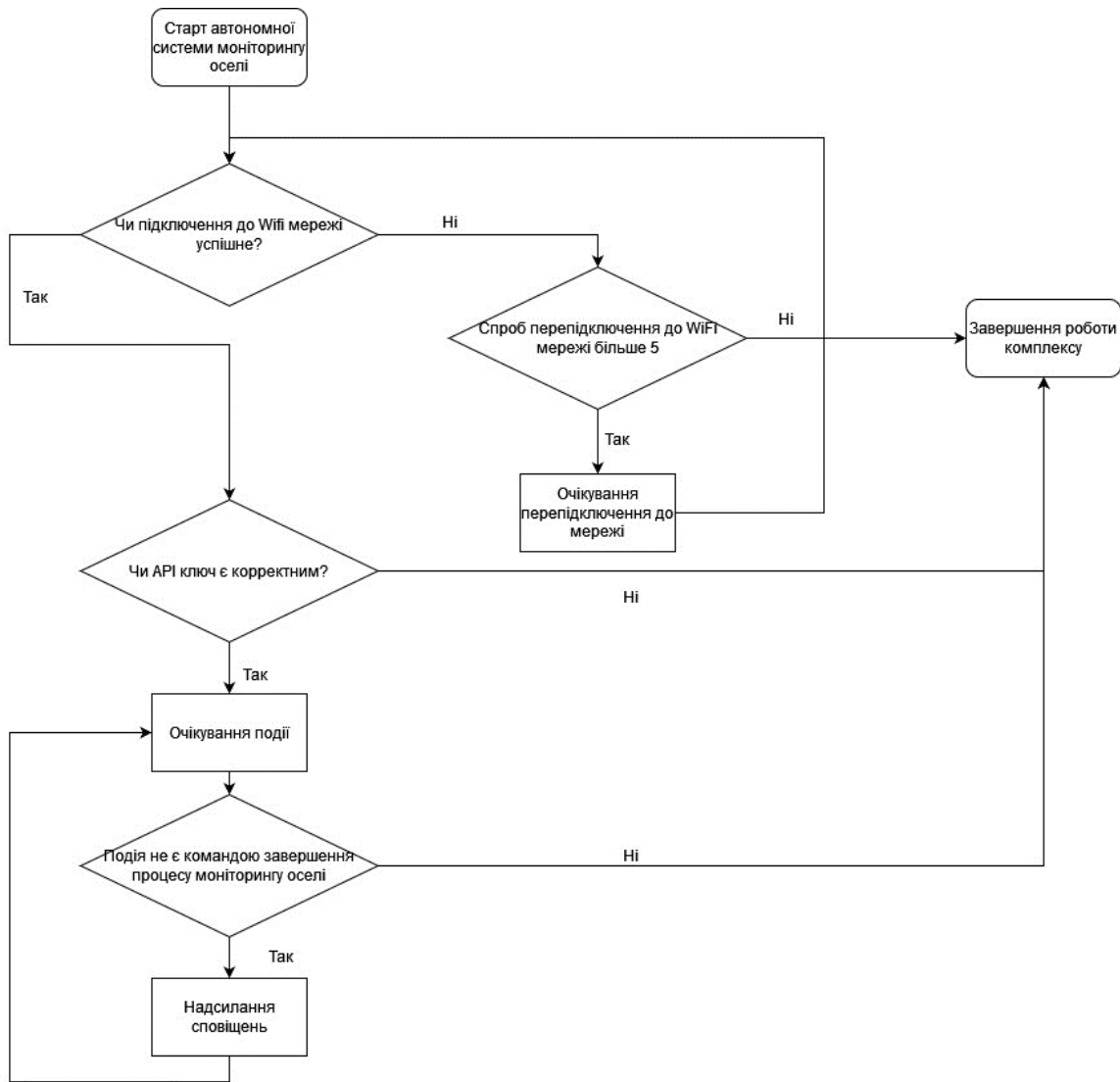


Рисунок 2.2 – Узагальнений алгоритм роботи комплексу візуального моніторингу оселі

Якщо один з сенсорів системи реагує на певні зміни, то сповіщення одразу відправляється користувачеві. Якщо користувач за допомогою команд в Telegram-боті комплексу намагається змінити конфігурацію комплексу, то в результаті цих змін користувач так само отримує сповіщення. У випадку, якщо користувач надсилав команду завершення роботи комплексу – то комплекс вимикається.

## Висновки до розділу 2

В другому розділі проведено огляд та аналіз методів та засобів, які можуть бути використані для забезпечення безпеки будинку. Враховано різні

аспекти, такі як контроль доступу, виявлення небажаних подій та реагування на них. Проаналізовано роль комп'ютерного зору у системах моніторингу, зокрема його використання для виявлення руху, розпізнавання об'єктів та інших важливих функцій. Досліджено можливості використання IoT для створення системи безпеки розумного будинку, яка забезпечує зв'язок між різними пристроями та дозволяє контролювати та керувати безпековими функціями.

Розглянуто принципи та методи реалізації системи моніторингу, яка здатна оперативно передавати дані та інформувати про події в реальному часі.

Розроблено алгоритм роботи комплексу візуального автономного моніторингу оселі, який включає в себе послідовність дій з виявлення, аналізу та сповіщення про події.



## **3 РЕАЛІЗАЦІЯ АВТОНОМНОГО КОМПЛЕКСУ ВІЗУАЛЬНОГО МОНІТОРИНГУ ОСЕЛІ**

### **3.1 Вибір компонентної бази**

В цьому розділі кваліфікаційної роботи бакалавра розглядається важливий аспект розробки автономної системи візуального моніторингу оселі. Один із ключових кроків у процесі реалізації такої системи – це вибір відповідної компонентної бази. Оскільки від цього вибору залежить ефективність, функціональність та надійність системи, особлива увага приділяється визначенню оптимальних компонентів, які забезпечать потрібний функціонал та забезпечать якісне візуальне моніторингове середовище.

Для розробки прототипу комплексу візуального автономного моніторингу оселі були використані різноманітні компоненти, що гарантують його надійну та ефективну роботу. Центральним компонентом прототипу є мікроконтролер ESP32-CAM, який забезпечує збір та обробку відеоданих з камери. Крім того, у склад прототипу входять датчики MQ-6 для виявлення наявності газу, магнітні дверні сенсори для контролю відкриття дверей, PIR-сенсор для виявлення руху, інфрачервоний сенсор для виявлення пожежі. Для живлення прототипу використовується спеціальна плата живлення, яка забезпечує стабільну роботу всіх компонентів. Вибір цих компонентів був здійснений з метою забезпечення комплексного та надійного моніторингу оселі, що дозволить власникам отримувати вчасну інформацію про будь-які події та зміни стану приміщення..

ESP32-CAM (рис. 3.1) є мікроконтролером на базі мікросхеми ESP32, розробленим компанією Espressif Systems. Він представляє собою компактний інтегрований модуль з вбудованою камерою, який поєднує в собі потужність мікроконтролера ESP32 та можливості відеозйомки та обробки [14]. ESP32-CAM пропонує широкий спектр функціональних можливостей, що робить

його привабливим вибором для реалізації автономних систем візуального моніторингу будинку.

Однією з ключових переваг ESP32-CAM є його потужний двоядерний мікропроцесор ESP32 з тактовою частотою до 240 МГц. Це забезпечує достатню обчислювальну потужність для обробки відеопотоку та виконання різноманітних алгоритмів обробки зображень, таких як детекція руху, розпізнавання облич, аналіз сцени та інші. Крім того, ESP32-CAM має достатньо оперативної пам'яті та містке флеш-сховище для зберігання програмного коду та відеоданих.



Рисунок 3.1 – ESP32-CAM

ESP32-CAM має вбудовану камеру з датчиком зображення, яка дозволяє здійснювати якісний захоплення зображень та відеозйомку. Камера підтримує різні роздільні здатності та формати відео, що дозволяє налаштовувати систему відповідно до потреб візуального моніторингу. Крім того, ESP32-CAM має можливість підключення зовнішньої камери через інтерфейсовий роз'єм. Завдяки вбудованому Wi-Fi модулю ESP32, ESP32-CAM може здійснювати зв'язок з локальною мережею або Інтернетом. Це відкриває широкі можливості для віддаленого керування та моніторингу системи візуального моніторингу будинку через мобільні пристрої або вебінтерфейс.

Застосування ESP32-CAM як центрального компонента для автономної системи візуального моніторингу будинку є доречним і має багато переваг. Цей компонент володіє компактним розміром, що дозволяє зручно розміщувати його у будь-яких місцях будинку. Водночас, ESP32-CAM забезпечує високу продуктивність та можливість безпроводового зв'язку, що є важливим для ефективної передачі відеоданих і забезпечення зв'язку з іншими компонентами системи.

Центральний вузол на базі ESP32-CAM виконує багатофункціональну роль у системі моніторингу. Він здатний збирати, обробляти та передавати відеодані, а також координувати роботу інших компонентів системи, таких як датчики руху, датчики дверей та вікон, а також системи сповіщення. Це дозволяє створити єдину систему, яка забезпечує повний контроль та безпеку будинку.

Однією з переваг ESP32-CAM є його розширюваність. Це означає, що до центрального вузла можна підключити додаткові модулі та сенсори для розширення функціональності системи моніторингу. Наприклад, можна підключити додаткові камери для розширення зони охоплення або підключити датчики вимірювання якості повітря. Це робить систему більш гнучкою та адаптованою до конкретних потреб користувача.

Сенсор MQ-6 [15] (рис. 3.2) є газовим датчиком, розробленим для виявлення наявності газу LPG (скрапленого нафтового газу), який використовується в побутових газових системах. Він відноситься до сімейства газових сенсорів MQ, які базуються на принципі зміни опору провідника під впливом взаємодії з окремими газами. Застосування сенсора MQ-6 в автономній системі візуального моніторингу будинку може забезпечити додатковий рівень безпеки та раннє виявлення потенційно небезпечних ситуацій, пов'язаних з витоком газу.

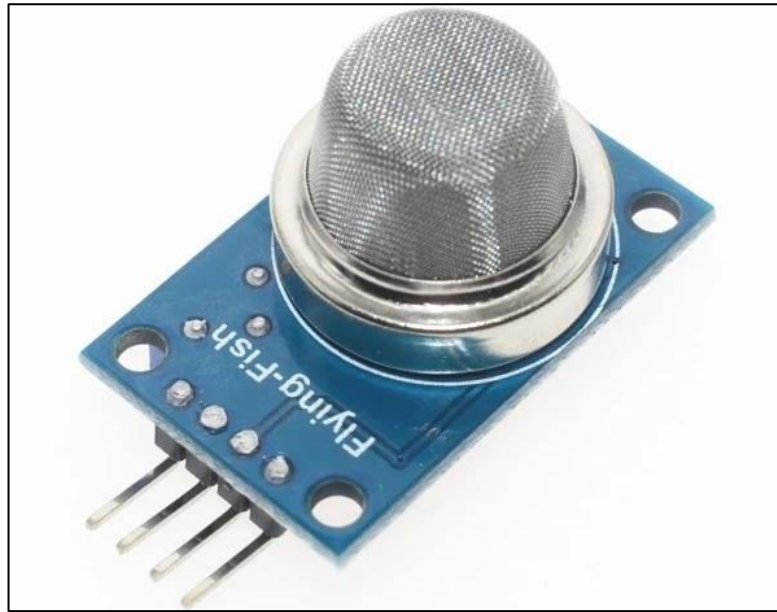


Рисунок 3.2 – Сенсор MQ-6

Основна функція сенсора MQ-6 – це виявлення наявності газу LPG у повітрі. Він працює на принципі зміни опору провідника, коли йому піддаються молекули газу LPG. Ця зміна опору може бути виміряна та проаналізована мікроконтролером або іншим пристроєм, що контролює систему візуального моніторингу.

Один з основних аспектів застосування сенсора MQ-6 полягає у його надійності та швидкості реакції. Він може ефективно реагувати на виток газу LPG та швидко сповіщати про наявність цього газу в середовищі. Це дає можливість прийняти необхідні заходи для безпеки, такі як відключення газового постачання, сповіщення власника будинку або активація аварійної сигналізації. Додатковою перевагою сенсора MQ-6 є його невеликі розміри та низьке споживання електроенергії, що дозволяє використовувати його в складі автономної системи візуального моніторингу без значного впливу на загальну енергоефективність системи.

Застосування сенсора MQ-6 в якості компонента для автономної системи візуального моніторингу будинку може підвищити безпеку та надати оперативну реакцію на потенційні небезпеки, пов'язані з витоком газу LPG. Він може бути інтегрований з іншими компонентами системи, такими як відеокамери, системи сповіщення або системи автоматичного відключення

газу. Такий комплексний підхід до візуального моніторингу може значно підвищити рівень безпеки оселі та забезпечити спокій та захищеність його мешканців.

Сенсор вогню від DFRobot є високоякісним пристроєм, призначеним для виявлення присутності вогню та пожежних ситуацій. Він має велику чутливість, що дозволяє надійно виявляти навіть слабкі джерела вогню та спалахи. Сенсор працює на принципі спостереження за інфрачервоним випромінюванням, що виникає від пламені, і відтворює це випромінювання як аналоговий сигнал.



Рисунок 3.3 – Сенсор вогню від DFRobot

Таблиця 3.1 – Характеристики сенсора вогню від DFRobot

Характеристика	Опис
Робоча напруга	3.3V-5V
Вихідний сигнал	Аналоговий сигнал, залежний від інтенсивності вогню
Чутливість	Висока, виявлення вогню на відстані до 1 метра
Реагування на спалах	Швидка реакція на спалахи та займання
Стабільна робота	Стабільна робота та низький рівень шуму
Вбудований захист	Захист від перенапруги та зворотного поляритету
Широка сумісність	Сумісний з різними мікроконтролерами та пристроями
Простий у використанні	Легко підключається та інтегрується з іншими пристроями
Довговічність	Довгий термін служби та надійна робота

Основні характеристики сенсору вогню від DFRobot наведено в табл. 3.1. Сенсор також має вбудований захист від перенапруги та зворотного

поляритету, широку сумісність з різними мікроконтролерами та пристроями, простоту в використанні, довговічність та надійну роботу. Використовуючи цей сенсор, можна ефективно виявляти вогонь та займання, забезпечуючи безпеку та захист від пожеж у проєкті.

Сенсор вогню від DFRobot може бути успішно застосований в якості компоненту для автономної системи візуального моніторингу будинку. Його можна інтегрувати з відеокамерами та іншими датчиками безпеки, що дозволяє створити комплексну систему, яка не тільки виявлятиме вогонь, але й надаватиме візуальне підтвердження пожежної ситуації та сприятиме вжиттю необхідних заходів для запобігання поширенню пожежі. Застосування сенсора вогню у такій системі дозволяє забезпечити високий рівень безпеки та реагувати на пожежні загрози вчасно та ефективно.

В рамках автономної системи візуального моніторингу будинку використовується PIR (Passive Infrared) сенсор AM312, який є одним з найпоширеніших варіантів на ринку. Цей сенсор базується на принципі виявлення руху за допомогою інфрачервоного випромінювання, що випромінюється тілами з температурою вище навколишньої.



Рисунок 3.4 – PIR-сенсор AM312

Таблиця 3.2 – Характеристики PIR сенсора AM312

Характеристика	Значення
----------------	----------

Робочий принцип	Два піррозачення, що реагують на зміни інфрачервоного випромінювання
Дальність визначення	3–5 метрів
Кут охоплення	Приблизно 100 градусів
Чутливість	Налаштовувана
Використання в темряві	Є інфрачервоний світлодіодний емітер
Напруга живлення	2.7–12 В
Струм споживання	Менше 50 мкА
Час спрацювання	Приблизно 2 секунди
Робоча температура	–20 °С до +60 °С
Розміри	10 x 23 мм
Інтерфейс зв'язку	Цифровий (вихідний сигнал TTL)

Сенсор АМ312 є ідеальним рішенням для автономних систем візуального моніторингу будинків, завдяки своїй компактності і простоті в використанні. Його надійна детекція руху робить його ефективним компонентом у забезпеченні безпеки і нагляду над оселію. Завдяки своїм компактним розмірам, сенсор АМ312 може бути легко встановлений у різних місцях будинку, забезпечуючи широкий охоплюючий кут детекції та надійне виявлення будь-яких рухів у заданому діапазоні. Його простий інтерфейс зв'язку і налаштування чутливості дозволяють легко адаптувати його до конкретних умов і забезпечити точні і надійні результати моніторингу. Завдяки низькому споживанню енергії, сенсор АМ312 є економічним рішенням для довготривалого використання в автономних системах моніторингу. Він може бути успішно використаний як в домашніх, так і в комерційних будівлях, дозволяючи забезпечити надійний і ефективний контроль за безпекою та моніторингом приміщень.

Сенсор відкриття дверей Reed Switch є одним із компонентів, який може бути використаний у складі автономної системи візуального моніторингу будинку. Цей сенсор базується на принципі роботи рейкового перемикача (reed switch) і забезпечує виявлення стану відкритості дверей або вікон.

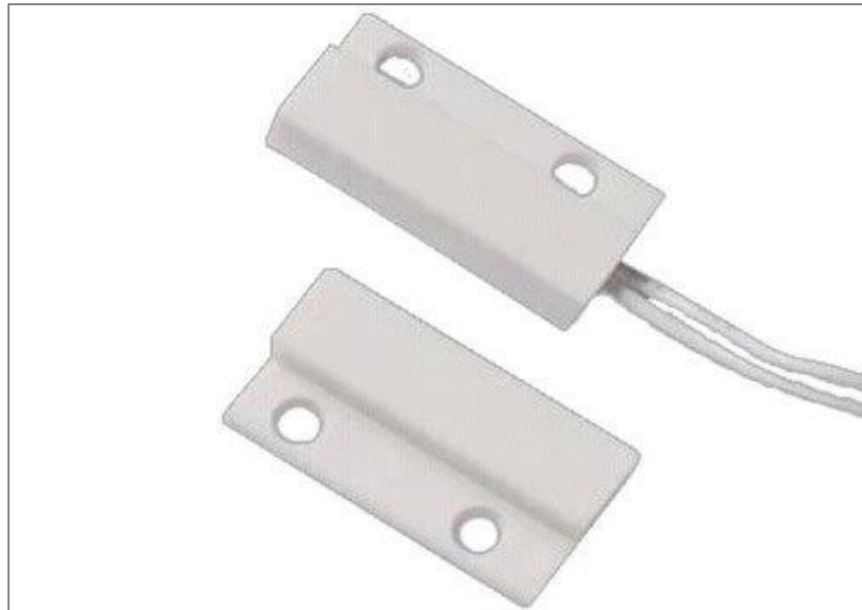


Рисунок 3.5 – Сенсор відкриття дверей Reed Switch

Сенсор відкриття дверей Reed Switch (реле Ріда) є електромеханічним пристроєм (рис. 3.5), який використовується для виявлення відкриття або закриття дверей, вікон або інших об'єктів. Принцип роботи цього сенсора базується на використанні ефекту Ріда, який виявлений американським фізиком В. Боуменом Рідом у 1936 році.

Сам сенсор складається з двох частин: магнітного контакту і реле Ріда. Магнітний контакт представляє собою два кінця дроту з феромагнітним ядром, розташовані внутрішньо в захисному кожуху. Реле Ріда містить два металевих контакти, які знаходяться поруч з магнітним контактом. Коли немагнітний матеріал (наприклад, двері) розташовується поруч з сенсором і магнітне поле змінюється, відбувається викривлення лінійного магнітного поля, що активує реле Ріда. Це в свою чергу змінює стан контактів в реле.

Коли двері чи вікно закриті, магнітний контакт прилягає до реле Ріда, і контакти в реле залишаються закритими. При відкритті дверей магнітний контакт віддаляється від реле Ріда, що призводить до розкриття контактів у реле. Це створює перерив у цепі, який може бути використаний для спостереження та визначення стану дверей або вікон.

Перевагою сенсора відкриття дверей Reed Switch є його простота та надійність. Він не вимагає енергії для своєї роботи і може працювати протягом



тривалого періоду часу без необхідності обслуговування. Крім того, він може бути легко інтегрований з іншими системами моніторингу або зв'язку.

Однак, обмеженням сенсора Ріда є його обмежена дальність виявлення. Магнітний контакт і реле повинні бути досить близькими, щоб відбувалася активація сенсора. Крім того, наявність сильних магнітних полів у навколишньому середовищі може спотворити його роботу, викликаючи неправильні виміри або ложні спрацювання.

### 3.2 Розробка апаратної частини комплексу

Структура комплексу показана на рис. 3.6. Комплекс включає в себе чотири сенсори, центральний контролер ESP32-CAM, плату живлення, плату логічного зсуву та резистори на 10 Ом для роботи сенсорів відкриття дверей.

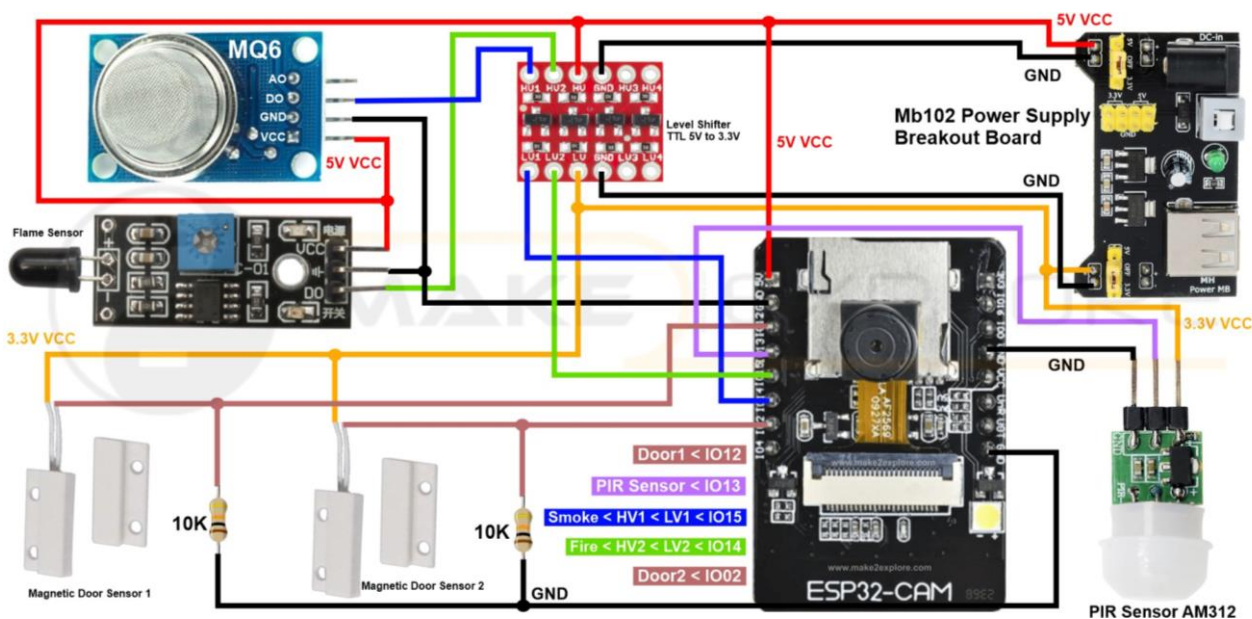


Рисунок 3.6 – Схема підключення компонентів комплексу до ESP32-CAM

Принцип роботи апаратної частини є наступним:

Усі датчики, включаючи датчики руху, температури та вологості, ефективно і зручно підключаються до потужної та універсальної плати розробки ESP32-CAM. Ця плата розробки є потужним мультимедійним пристроєм, що поєднує в собі функції камери та мікроконтролера, а також забезпечує підтримку Wi-Fi. Завдяки цьому, ESP32-CAM може легко

підключатися до бездротового маршрутизатора і встановлювати зв'язок з Інтернетом. Це дає можливість здійснювати моніторинг, управління та отримання повідомлень у режимі реального часу, а також забезпечує дистанційний доступ до системи моніторингу з будь-якого місця, де є доступ до Інтернету. Завдяки бездротовому підключенню, ESP32-CAM може працювати в режимі мобільності та бути легко розміщеним в будь-якому місці, де потрібно здійснювати моніторинг та контроль. Застосування плати розробки ESP32-CAM у системах моніторингу відкриває безліч можливостей для забезпечення безпеки, зручності та ефективності управління різними приміщеннями та об'єктами.

Щоб взаємодіяти з системою безпеки та отримувати сповіщення про всі сповіщення, потрібно створити Telegram Bot у застосунку «Telegram» в смартфоні або на персональному комп'ютері. За допомогою цього бота Telegram можна ввімкнути/вимкнути (поставити/зняти з охорони) комплекс візуального моніторингу оселі та всі сповіщення. У застосунку Telegram також можемо робити/отримувати фотографії зони моніторингу, де встановлено ESP32-CAM.

Якщо всі датчики та сповіщення ввімкнено, система надсилатиме сповіщення в Telegram про кожну подію, пов'язану з безпекою оселі, а саме, наприклад, – оповіщення про пожежу або дим. Сповіщення можуть бути надіслані комплексом працювати з будь-якої точки світу, для їх отримання потрібен лише застосунок Telegram з авторизованим ботом і підключення до Інтернету на телефоні. Лише дозволені/авторизовані користувачі (ідентифікатор чату яких зареєстровано) зможуть взаємодіяти з цим ботом.

Для завантаження прошивки до ESP32-CAM потрібно використовувати програматор, наприклад, FDTI програматор (рис. 3.7). Цей компонент забезпечує з'єднання між USB та UART інтерфейсами та працює з різними напругами на виході, наприклад, 5 В або 3,3 В.

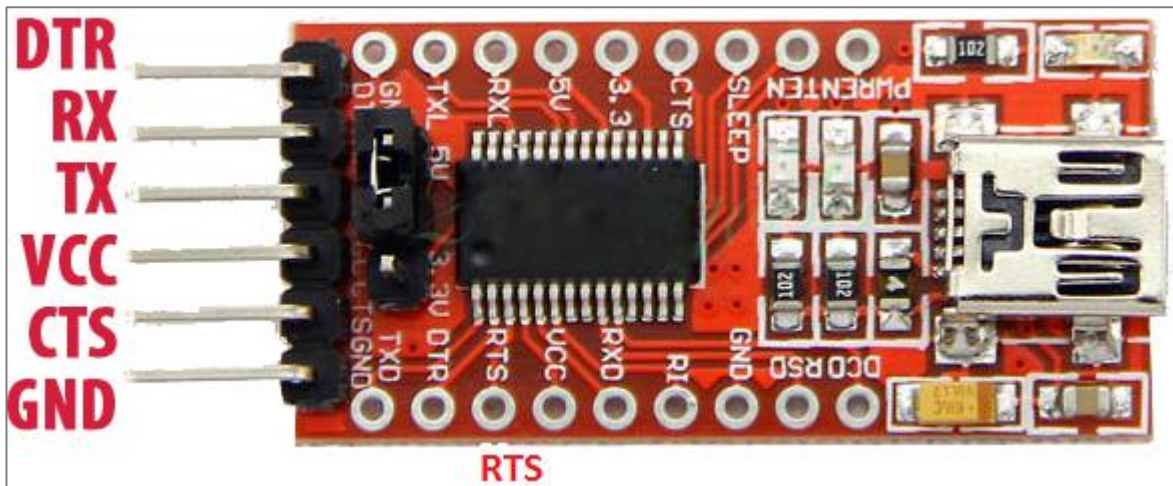


Рисунок 3.7 – FDTI програматор та позначення його пінів

На рис. 3.7 показано піни підключення цього програматора. Їх функціональність є наступною:

- DTR – Скидання інших апаратних пристроїв
- RX – Використовується для отримання послідовних даних.
- TX – Використовується для надсилення послідовних даних.
- VCC – Вихідна напруга (3,3В або 5В)
- CTS – Перемикання режиму програмування пристрою
- GND – Заземлення

Схема підключення FDTI програматора до ESP32-CAM зазначена на рис. 3.8.

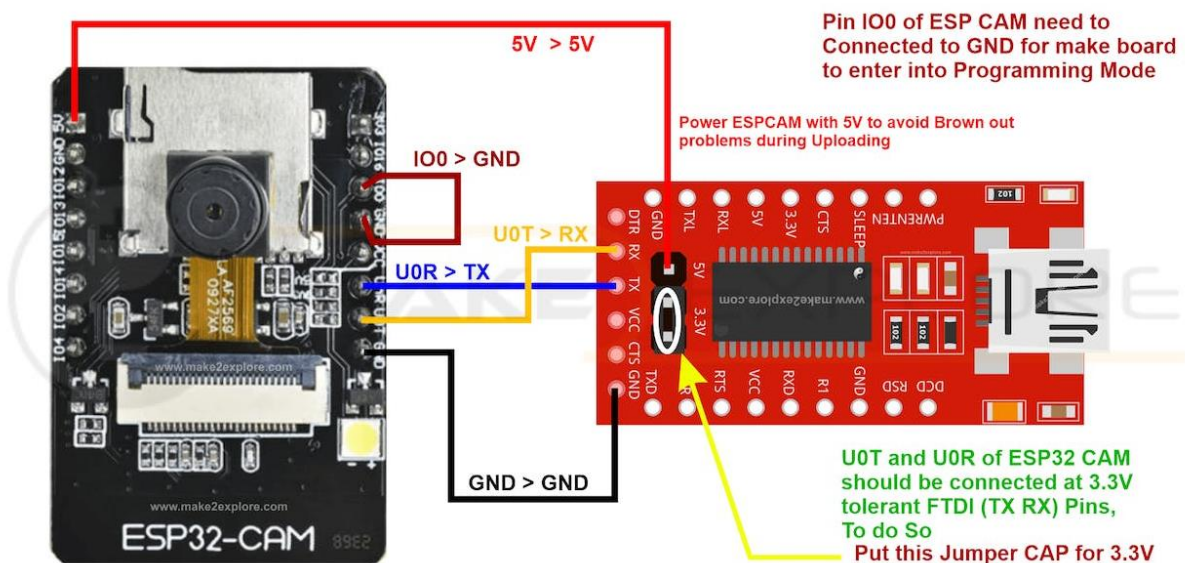


Рисунок 3.8 – Схема підключення програматора

Пін U0R має бути підключеним до TX піну програматора, U0T до RX піну відповідно. На ESP32-CAM піни IO0 та GND мають бути закорочені для переведення плати в режим програмування. Піни 5V та GND мають бути з'єднані на обох пристроях. Так як U0T та U0R піни ESP32-CAM мають бути під'єднані до FTDI плати, що підтримує живлення від 3,3 В, то для цього на платі програматора треба під'єднати джампер, що перемикає режим живлення з 5В на 3,3В.

Після цього можна під'єднати програматор до комп'ютеру та завантажувати зібрану прошивку за допомогою Arduino IDE. Варто взяти до уваги, що для програмування ESP32-CAM за допомогою FTDI в середовищі Arduino IDE потрібно обрати COM-порт, до якого підключено пристрій, тип програматора та модель плати. І лише після цього можна запускати процес компілювання та завантаження програми на ESP32.

На рис. 3.9 показано зібраний прототип апаратної частини комплексу візуального моніторингу оселі.

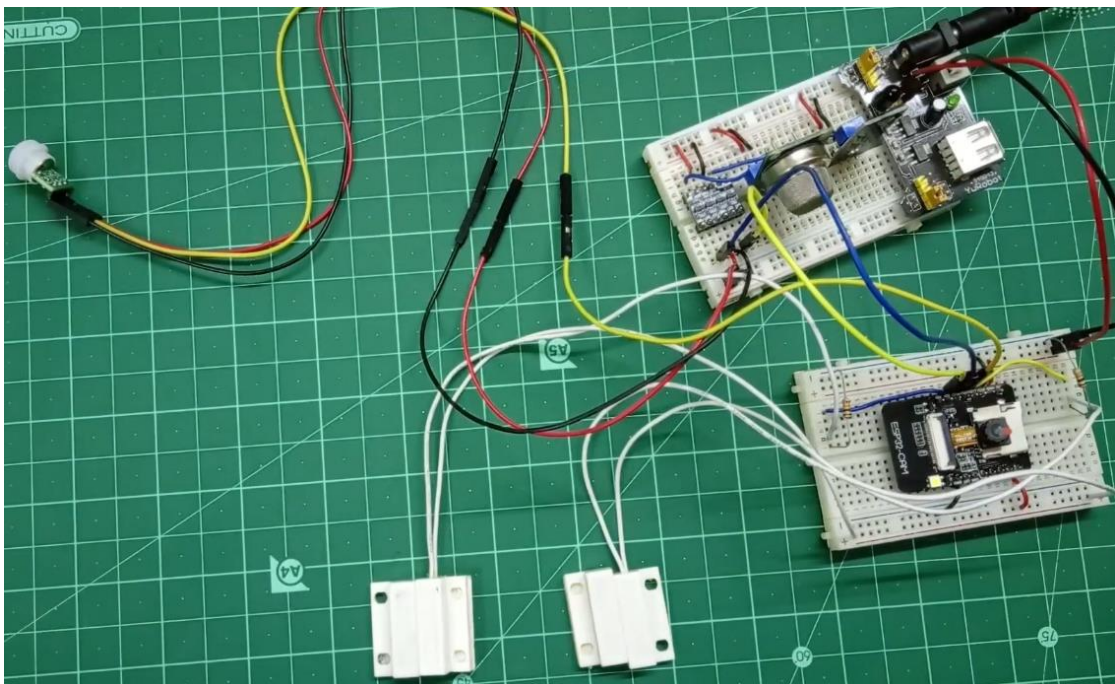


Рисунок 3.9 – Зібраний прототип апаратної частини комплексу

Прототип складається з наступних компонентів:

- 1) AI Thinker ESP32-CAM Dev Board
- 2) Сенсор визначення руху AM312

- 3) Сенсор відкриття дверей (2 штуки)
- 4) Сенсор визначення газу або диму MQ-6
- 5) Інфрачервоний сенсор визначення вогню
- 6) 10 кОм резистори (2 штуки)
- 7) 4-канальний перетворювач логічних рівнів
- 8) FTDI програматор
- 9) Breadboard MB102
- 10) Плата живлення MB102 Breadboard
- 11) Кабелі підключення
- 12) Літій-полімерна батарея напругою 7,4 В

### **3.3 Розробка програмної частини комплексу**

Розробка програмної частини комплексу для забезпечення його функціональності включає два основних етапи, які необхідно пройти:

1) перший етап – створення Telegram-бота та отримання його ключів за допомогою сервісу BotFather. Даний етап включає в себе реєстрацію бота в Телеграмі та налаштування його параметрів. Після успішної реєстрації, отримано необхідні ключі доступу, які дозволять боту взаємодіяти з платформою;

2) другий етап – розробка програми в середовищі Arduino IDE та завантаження її на ESP32-CAM. Етап передбачає створення програмного коду, який буде відповідати функціональним вимогам комплексу. Використовуючи Arduino IDE, можна програмувати мікроконтролер ESP32-CAM для забезпечення взаємодії з Telegram-ботом, зчитування даних з сенсорів, керування різними пристроями та виконання інших задач, необхідних для оптимальної роботи комплексу.

Описані два етапи взаємодіють між собою, створюючи комплексну програмну частину, яка забезпечує роботу системи моніторингу та взаємодію з користувачами через месенджер Telegram. Такий підхід дозволяє створити

потужний та функціональний інструмент для візуального моніторингу оселі та отримання важливих повідомлень та сповіщень у реальному часі.

Створення Telegram-бота включає в собі декілька кроків. Першим кроком є пошук @botfather в Telegram. Для цього треба увійти до облікового запису Telegram та виконати пошук «@botfather» у полі пошуку (рис. 3.10). Бот @botfather є офіційним ботом Telegram, який дозволяє створювати та керувати іншими ботами.

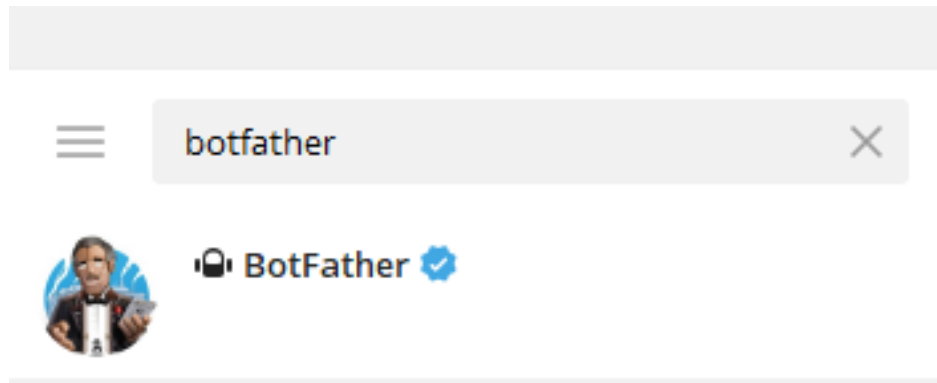
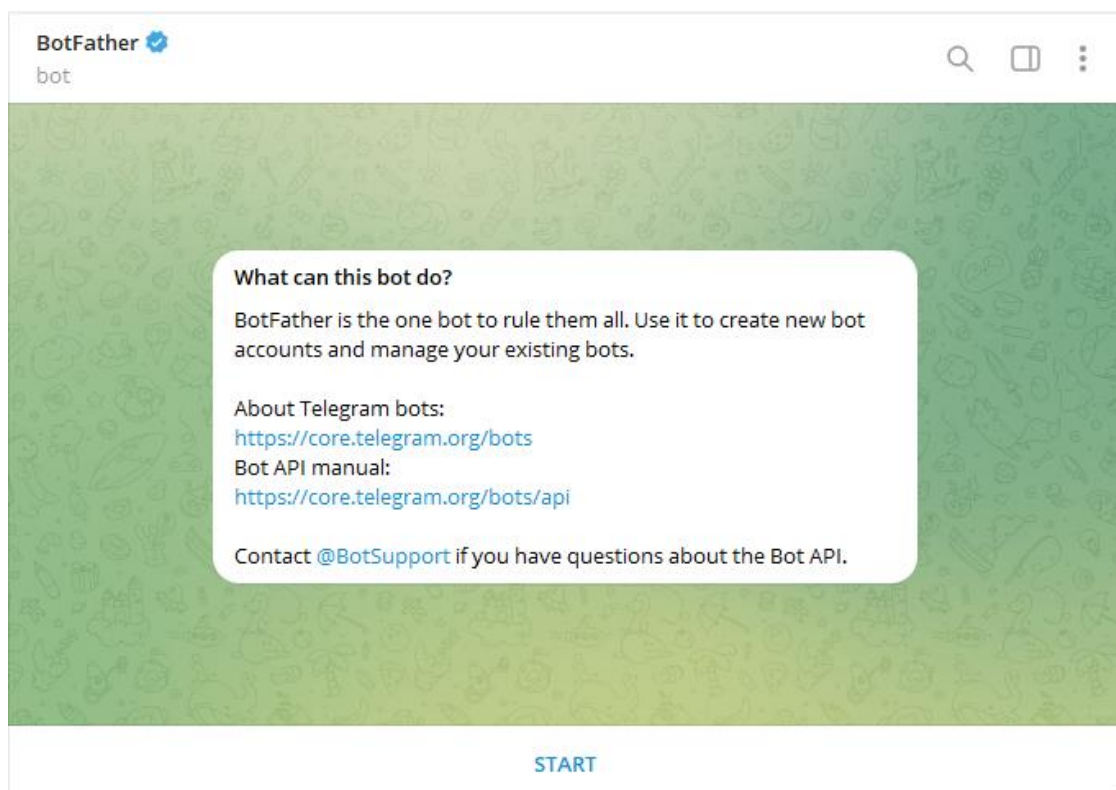


Рисунок 3.10 – Пошук Telegram-бота BotFather для отримання API-ключів

Наступним кроком є створення нового бота. Після знаходження @botfather, треба розпочати діалог з ним, натиснувши на кнопку «Start» або увівши команду «/start» (рис. 3.11).



### Рисунок 3.11 – Початок роботи з @BotFather

Після натискання кнопки «Start», з'являється список доступних команд для @botfather, які відповідають за створення нових та керування наявними Telegram-ботами користувачів (рис. 3.12).

Для продовження створення бота потрібно ввести команду «/newbot». Після цього @botfather запропонує ввести ім'я для нового бота. Потрібно обрати відповідне ім'я, яке буде використовуватися для ідентифікації бота. Після цього буде запропоновано ввести ім'я користувача для новоствореного бота. Це є унікальне ім'я користувача, закінчується на «bot» (рис. 3.13). Після успішного створення бота @botfather надасть токен доступу. Цей токен є унікальним ідентифікатором бота, який використовується для з'єднання з API Telegram.

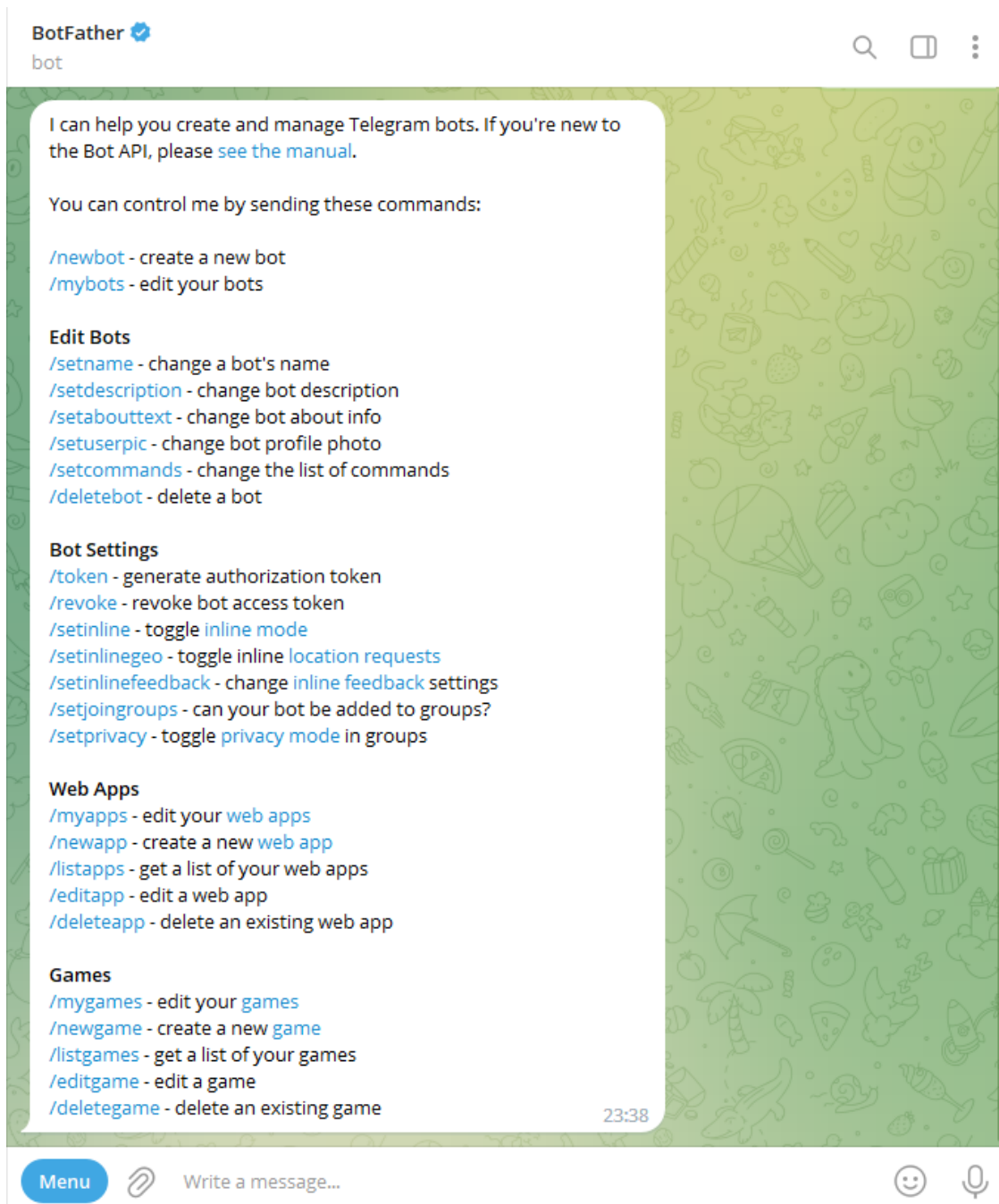


Рисунок 3.12 – Список доступних команд керування

За бажанням є можливість налаштувати додаткові параметри для новоствореного бота, такі як опис, фото профілю, команди, повідомлення привітання тощо. Ці налаштування допоможуть покращити взаємодію користувачів з ним.



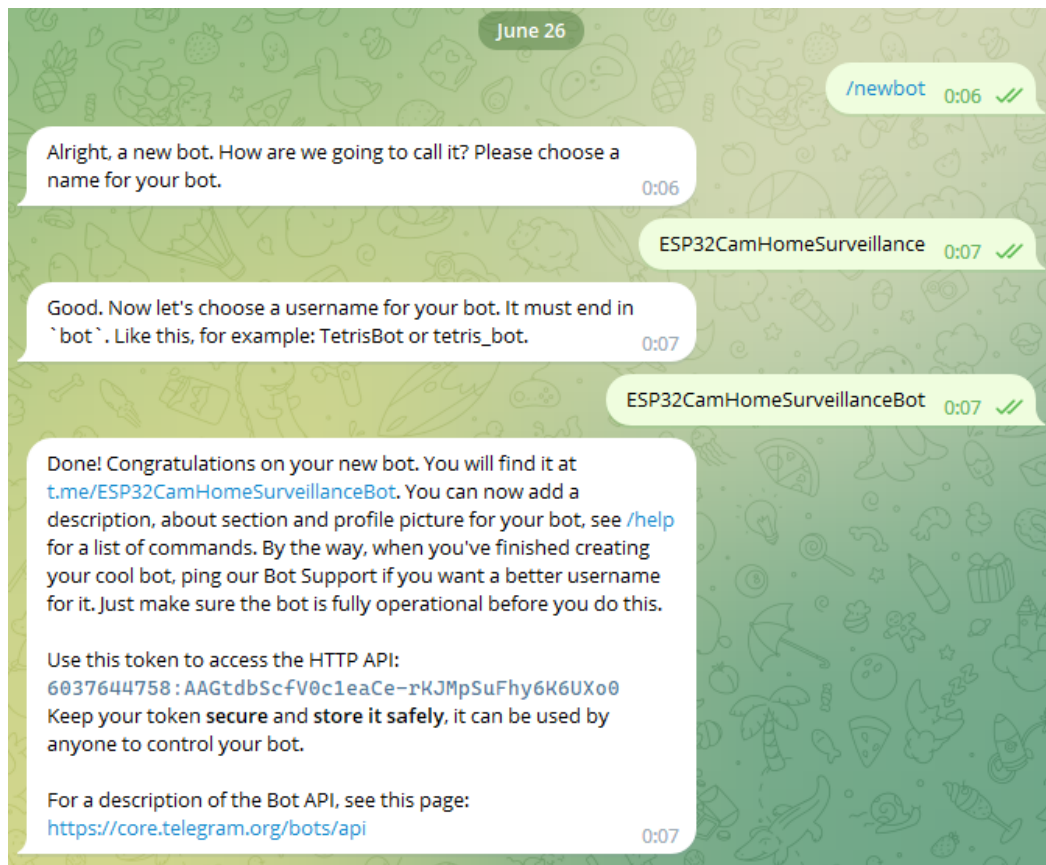


Рисунок 3.14 – Процес створення бота та отримання токена доступу до нього

Інтерфейс новоствореного бота з іменем ESP32CamHomeSurveillanceBot для отримання сповіщень та керуванням автономним комплексом візуального моніторингу оселі наведено на рис. 3.15.

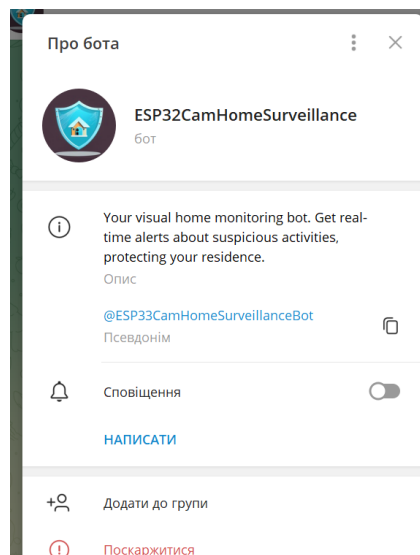


Рисунок 3.15 – Опис новоствореного Telegram-бота для автономного комплексу візуального моніторингу оселі

Відкривши час з цим ботом можна побачити повідомлення з коротким описом, що саме може робити ESP32CamHomeSurveillanceBot. Скріншот з цим повідомленням наведено на рис. 3.16

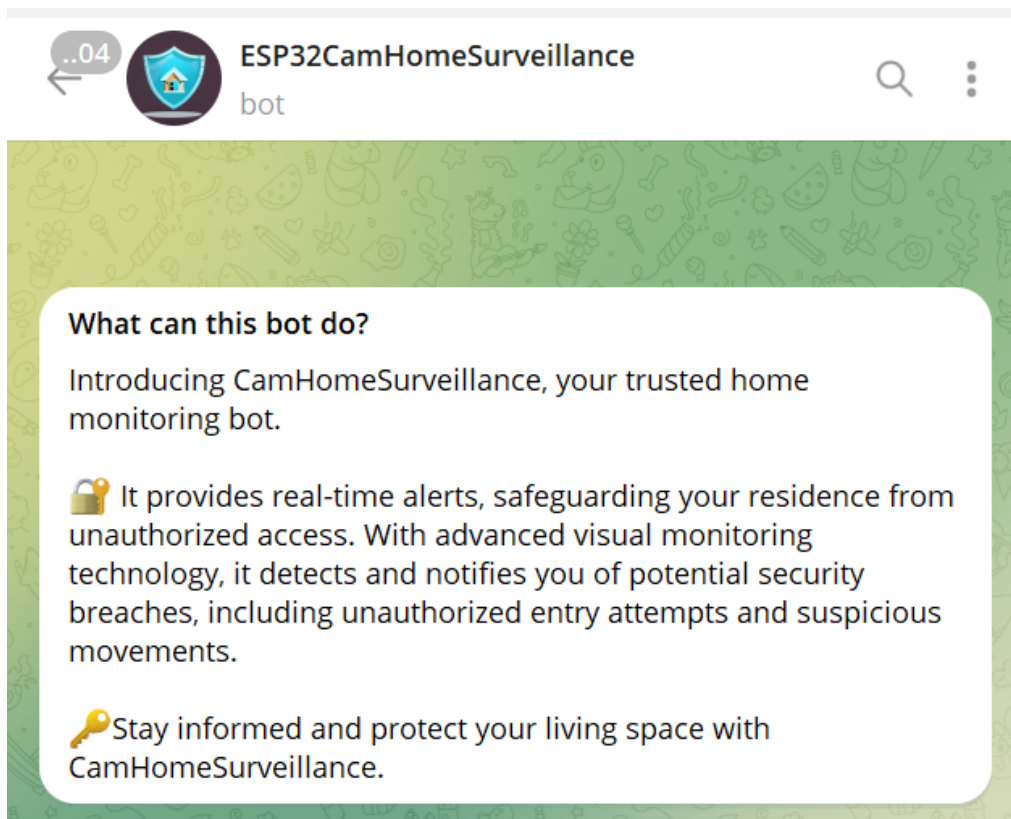


Рисунок 3.16 – Повідомлення-опис Telegram-боту  
ESP32CamHomeSurveillanceBot

Після натиснення на кнопку «Start», з'являється кнопка «Menu», що містить список команд для керування автономним комплексом візуального моніторингу оселі (рис. 3.17).

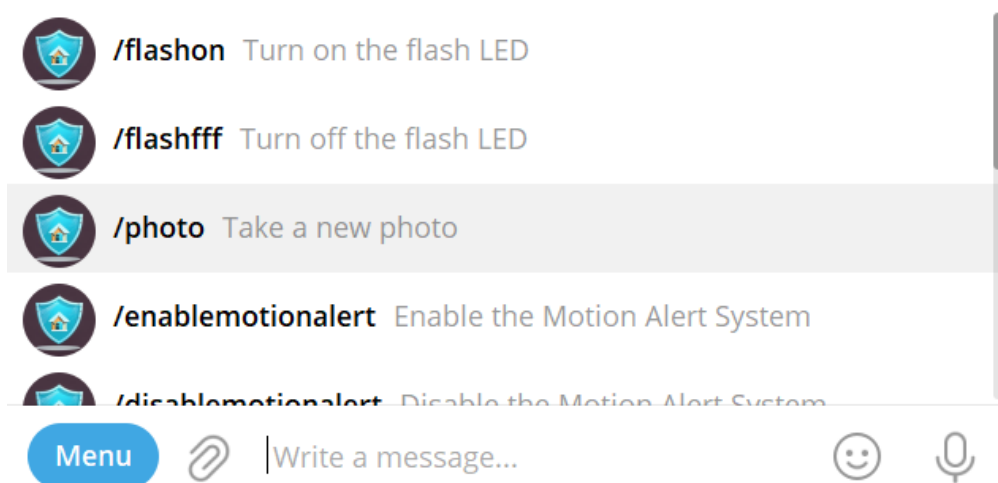


Рисунок 3.17 – Список команд, доступний для керування комплексом

Наступний етап розробки – це реалізація програмної компоненти автономного комплексу візуального моніторингу оселі. Для цього, за допомогою Arduino IDE, потрібно встановити потрібні для роботи бібліотеки. За допомогою Tools > Manage Libraries потрібно встановити бібліотеку UniversalTelegramBot для взаємодії з Telegram API (рис. 3.18).

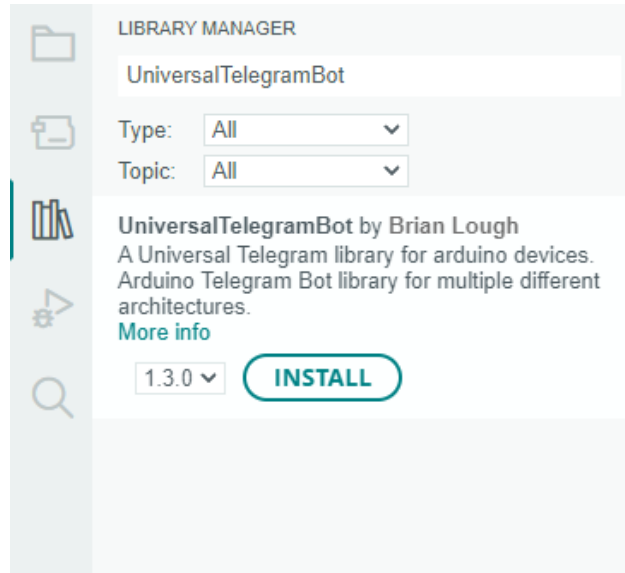


Рисунок 3.18 – Встановлення бібліотеки UniversalTelegramBot

Також для формування JSON запитів та читання JSON відповідей потрібно встановити бібліотеку ArduinoJSON (рис. 3.19).

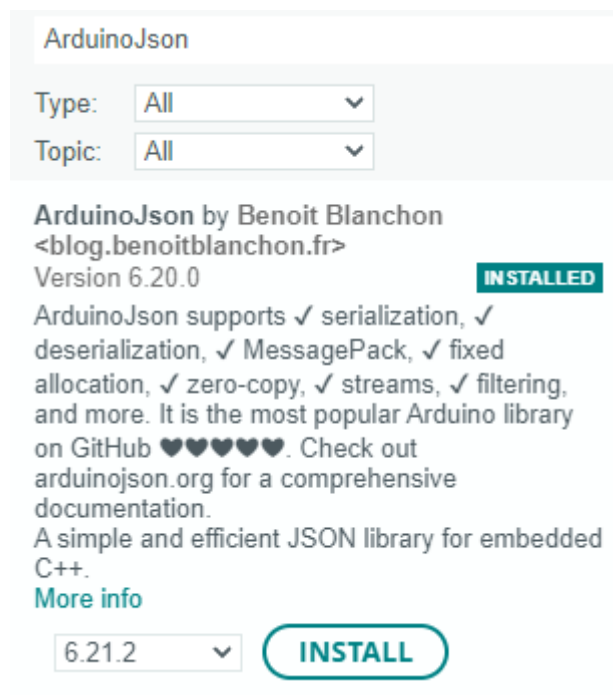


Рисунок 3.19 – Встановлення бібліотеки ArduinoJSON

Повний код програми для автономного комплексу візуального моніторингу оселі наведено в додатку А. Сама програмна частина реалізує функціонал управління апаратною частиною використовуючи TelegramBot API а саме – за допомогою команд бота.

Список команд для додавання в меню ESP32CamHomeSurveillanceBot:

– flashOn – Увімкнути спалах LED. Команда вмикає спалах LED на пристрої для освітлення. Використовується, коли потрібне додаткове освітлення для фотографування або для покращення видимості в темряві. Код цієї команди наведено на рис. 3.20.

```
if (text == "/flashOn") {  
    flashState = true;  
    bot.sendMessage(chat_id, "Flash is set to ON", "");  
    digitalWrite(FLASH_LED_PIN, flashState);  
}
```

Рисунок 3.20 – Частина коду для реалізації команди /flashOn

– flashOff – Вимкнути спалах LED. Команда вимикає спалах LED на пристрої. Використовується, якщо більше не потрібне додаткове освітлення або для економії енергії пристрою. Код цієї команди наведено на рис. 3.21.

```
if (text == "/flashOff") {  
    flashState = false;  
    bot.sendMessage(chat_id, "Flash is set to OFF", "");  
    digitalWrite(FLASH_LED_PIN, flashState);  
}
```

Рисунок 3.21 – Частина коду для реалізації команди /flashOff

– photo – Зробити нове фото. Ця команда дозволяє зробити нове фото за допомогою пристрою. Користувач отримає актуальний знімок оселі, який можна використовувати для моніторингу або збереження як доказу в разі потреби. Частина коду наведено для отримання фото наведено на рис. 3.22.

```
uint8_t *fbBuf = fb->buf;
size_t fbLen = fb->len;
for (size_t n=0;n<fbLen;n=n+1024) {
    if (n+1024<fbLen) {
        clientTCP.write(fbBuf, 1024);
        fbBuf += 1024;
    }
    else if (fbLen%1024>0) {
        size_t remainder = fbLen%1024;
        clientTCP.write(fbBuf, remainder);
    }
}

clientTCP.print(tail);

esp_camera_fb_return(fb);
```

Рисунок 3.22 – Блок коду, що захоплює зображення з камери ESP32-CAM

– enableMotionAlert – Увімкнути систему оповіщення про рух. Команда вмикає систему оповіщення про рух. Користувач отримуватиме сповіщення в режимі реального часу, якщо буде виявлено підозрілі рухи біля оселі, в зоні видимості присрою. Це допоможе вчасно виявити незаконні дії чи потенційно небезпечні ситуації.

– disableMotionAlert – Вимкнути систему оповіщення про рух. Команда вимикає систему оповіщення про рух. Ви не будете отримувати сповіщення про рух біля вашої оселі. Рекомендується використовувати цю команду, якщо ви тимчасово не потребуєте оповіщень або відсутні на місці.

– enableDoorAlert – Увімкнути систему оповіщення про відкриття дверей. Команда вмикає систему оповіщення про відкриття дверей. Ви будете отримувати сповіщення, якщо будь-яка дверь у вашій оселі буде відкрита без дозволу. Це допоможе вчасно виявити потенційні вторгнення або небажані ситуації.

– disableDoorAlert – Вимкнути систему оповіщення про відкриття дверей. Команда вимикає систему оповіщення про відкриття дверей. Ви не будете отримувати сповіщення, якщо будь-яка дверь у вашій оселі буде

відкрита. Рекомендується використовувати цю команду, якщо ви тимчасово не потребуєте оповіщень або відсутні на місці.

– `enableSmokeAlert` – Увімкнути систему оповіщення про дим. Команда вмикає систему оповіщення про дим. Ви будете отримувати сповіщення, якщо буде виявлено дим у вашій оселі. Це допоможе вчасно виявити пожежу або потенційно небезпечну ситуацію.

– `disableSmokeAlert` – Вимкнути систему оповіщення про дим. Команда вимикає систему оповіщення про дим. Ви не будете отримувати сповіщення про дим у вашій оселі. Рекомендується використовувати цю команду, якщо ви тимчасово не потребуєте оповіщень або відсутні на місці.

– `enableFireAlert` – Увімкнути систему оповіщення про пожежу. Команда вмикає систему оповіщення про пожежу. Ви будете отримувати сповіщення, якщо буде виявлений ознаки пожежі у вашій оселі. Це допоможе вчасно виявити пожежу та вжити необхідні заходи безпеки.

– `disableFireAlert` – Вимкнути систему оповіщення про пожежу. Команда вимикає систему оповіщення про пожежу. Користувач не буде отримувати сповіщення про пожежу в оселі. Рекомендується використовувати цю команду, якщо користувач тимчасово не потребує оповіщень або відсутній на місці.

### **Висновки до розділу 3**

В третьому розділі проведено огляд і аналіз доступних компонентів для створення комплексу візуального моніторингу оселі. Враховані функціональні вимоги та вибрані необхідні компоненти для подальшої розробки.

Здійснено проєктування та розробку апаратної частини комплексу візуального моніторингу. Використано обрані компоненти, такі як відеокамери, датчики руху та інші необхідні елементи. Реалізовано функції збирання відеоданих та детекції подій.

Розроблено програмне забезпечення для управління та аналізу даних, отриманих від апаратної частини комплексу. Програма забезпечує можливість

візуального моніторингу, аналізу зображень, виявлення руху та інших параметрів безпеки.

Отже, під час реалізації автономного комплексу візуального моніторингу оселі були використані відповідні компоненти, розроблена апаратна і програмна частини. Зроблено значний прогрес у створенні функціонального та надійного комплексу для забезпечення безпеки та моніторингу оселі.

## ВИСНОВКИ

Під час виконання кваліфікаційної роботи розроблено прототип автономного комплексу візуального моніторингу оселі. В якості контролера управління обрано плату ESP32-CAM, яка є одночасно і пристроєм для візуального моніторингу будівлі.

Кваліфікаційна робота включала огляд патентної інформації та наукових публікацій, що дозволило отримати цінні уявлення про наявні технологічні рішення у галузі візуального моніторингу для оселі. Розглянуто та проаналізовано існуючі рішення на ринку, включаючи комерційні продукти та відкриті розробки, з метою отримання інформації про технології, функціональні можливості та особливості цих рішень.

На основі зібраної інформації були сформульовані вимоги до автономного комплексу візуального моніторингу оселі, які враховували патентну інформацію, наукові публікації та існуючі рішення. Ці вимоги були спрямовані на забезпечення ефективної реалізації моніторингової системи з використанням сучасних технологій візуального спостереження для будинків.

В розділі, присвяченому аналізу методів та засобів безпеки будинку, було розглянуто різні аспекти, такі як контроль доступу, виявлення небажаних подій та реагування на них. Особлива увага була приділена ролі комп'ютерного зору в системах моніторингу, зокрема його використанню для виявлення руху, розпізнавання об'єктів та інших важливих функцій. Досліджено можливість використання IoT для створення системи безпеки розумного будинку, яка забезпечує зв'язок між різними пристроями та дозволяє контролювати та керувати безпековими функціями.

Розглянуто принципи та методи реалізації системи моніторингу, яка здатна оперативно передавати дані та надавати інформацію про події в реальному часі. Розроблено алгоритм роботи комплексу візуального автономного моніторингу оселі, який включає послідовність дій з виявлення, аналізу та сповіщення про події.



Здійснено проєктування та розробку апаратної частини комплексу візуального моніторингу з використанням обраних компонентів, таких як відеокамери, датчики руху та інші необхідні елементи. Реалізовано функції збирання відеоданих та детекції подій. Також було розроблено програмне забезпечення для управління та аналізу даних, отриманих від апаратної частини комплексу. Саме управління комплексом відбувається за допомогою команд з Telegram-бота, так само як і отримання сповіщень користувачем.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. US11288650B2 – Linking computer vision interactions with a computer kiosk - Google Patents. Google Patents. URL: <https://patents.google.com/patent/US11288650B2/en?q=US11288650B2> (Last accessed: 01.06.2023).
2. US11210526B2 – Video surveillance system, video processing apparatus, video processing method, and video processing program - Google Patents. Google Patents. URL: <https://patents.google.com/patent/US11210526B2/en?q=US11210526B2+> (Last accessed: 01.06.2023).
3. Video processing and analysis for surveillance applications / S. Aramvith et al. 2009 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS 2009), Kanazawa, Japan, 7–9 January 2009. 2009. URL: <https://doi.org/10.1109/ispacs.2009.5383765> (Last accessed: 01.06.2023).
4. A comprehensive survey of multi-view video summarization / T. Hussain et al. Pattern Recognition. 2021. Vol. 109. P. 107567. URL: <https://doi.org/10.1016/j.patcog.2020.107567> (Last accessed: 01.06.2023).
5. Dror S., Bashkansky E., Ravid R. House of security: a structured system design & analysis approach. International Journal of Safety and Security Engineering. 2012. Vol. 2, no. 4. P. 317–329. URL: <https://doi.org/10.2495/safe-v2-n4-317-329> (Last accessed: 21.06.2023).
6. Mohd Yusof N., Jidin A. Z., Sze L. M. Web Based Home Security and Automation System. International Journal of Reconfigurable and Embedded Systems (IJRES). 2016. Vol. 5, no. 2. P. 92. URL: <https://doi.org/10.11591/ijres.v5.i2.pp92-98> (Last accessed: 01.06.2023).
7. Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol / S. Pandya et al. Applied System Innovation. 2018. Vol. 1, no. 4. P. 42. URL: <https://doi.org/10.3390/asi1040042> (Last accessed: 01.06.2023).
8. Tripathi R. C., Singh H., Chakravarty A. Smart home sensorized security

system. INSTRUMENTATION ENGINEERING, ELECTRONICS AND TELECOMMUNICATIONS – 2021 (IEET-2021): Proceedings of the VII International Forum, Izhevsk, Russian Federation. 2023. URL: <https://doi.org/10.1063/5.0125061> (Last accessed: 01.06.2023).

9. A Way for Smart Home Technology for Disabled and Elderly People / S. M. U. Sankar et al. 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 14–16 March 2023. 2023. URL: <https://doi.org/10.1109/icidadca56705.2023.10099817> (Last accessed: 01.06.2023).

10. Hub 2 Plus – Просунута централь з 4 каналами зв'язку від Ajax Systems. URL: <https://ajax.systems/ua/products/hub2-plus/> (дата звернення: 01.06.2023).

11. Ajax MotionCam - Датчик руху з фотоверифікацією тривоги. Ajax Systems. URL: <https://ajax.systems/ua/products/motioncam/> (дата звернення: 01.06.2023).

12. Vivint Home Security & Smart Home Systems. Vivint. URL: <https://www.vivint.com/> (Last accessed: 01.06.2023).

13. ADT Command Review. PCMAG. URL: <https://www.pcmag.com/reviews/adt-command> (Last accessed: 04.06.2023).

14. Hemanth Kumar MS. ESP32-CAM for Face Mask Detection. International Journal of Advanced Research in Science, Communication and Technology. 2022. P. 86–93. URL: <https://doi.org/10.48175/ijarsct-2509> (date of access: 26.06.2023).

15. MQ6 Datasheet | HANWEI - Datasheetspdf.com. Datasheetspdf.com - Free electronic components datasheet pdf search & download site. URL: <https://datasheetspdf.com/datasheet/MQ6.html> (date of access: 06.06.2023).

## ДОДАТОК А ДОВІДКА

про перевірку на унікальність пояснювальної записки  
кваліфікаційної роботи бакалавра  
на тему: «Автономний комплекс візуального моніторингу оселі»  
студента спеціальності 123 «Комп'ютерна інженерія»,  
групи 405  
Кочетова Костянтина  
прізвище, ім'я, по-батькові

Перевірку тексту здійснено сервісом: онлайн-сервіс Unicheck.  
Результат перевірки тексту роботи: схожість складає 3.11%.



Ім'я користувача:  
Євген Дарнапук

ID перевірки:  
1015695070

Дата перевірки:  
27.06.2023 00:56:46 EEST

Тип перевірки:  
Doc vs Internet + Library

Дата звіту:  
27.06.2023 00:58:31 EEST

ID користувача:  
100012258

Назва документа: Кочетов\_К\_В\_405\_Кваліфікаційна\_бакалаврська\_робота

Кількість сторінок: 25 Кількість слів: 10470 Кількість символів: 84092 Розмір файлу: 84.77 KB ID файлу: 1015338862

**3.11%**  
**Схожість**

Найбільша схожість: 0.38% з Інтернет-джерелом (<https://er.nau.edu.ua/bitstream/NAU/57125/1/%d0%a4%d0%9a%d0%...>)

2.97% Джерела з Інтернету 325

Сторінка 27

0.53% Джерела з Бібліотеки 51

Сторінка 28

**0% Цитат**

Вилучення цитат вимкнено

Вилучення списку бібліографічних посилань вимкнено

**0%**  
**Вилучень**

Немає вилучених джерел

**Модифікації**

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 4

Студент

\_\_\_\_\_ К. В. Кочетов  
підпис ініціали, прізвище

Керівник

ст. викладач  
\_\_\_\_\_ Є. С. Дарнапук  
підпис ініціали, прізвище

Дата: «\_\_» \_\_\_\_\_ 2023 р.



```
#define FLASH_LED_PIN 4
bool flashState = LOW;

// Motion Sensor
const byte motionSensor = 13;
bool motionDetected = false;
bool motionDetectEnable = false;

// Door Sensor
const byte door1 = 12;
const byte door2 = 2;
bool door1stat = true;
bool door2stat = true;
bool doorLockMonitor = false;

// fire sensor
bool fireDetectMonitor = false;
const byte firePin = 14;
bool fire = false;

// MQ6 Smoke LPG gas leak Detector
bool smokeDetectMonitor = false;
const byte smokePin = 15;
bool smoke = false;

int botRequestDelay = 1000; // mean time between scan messages
long lastTimeBotRan; // last time messages' scan has been done

void handleNewMessages(int numNewMessages);
String sendPhotoTelegram();

// ISR (Interrupt Service Routine) Indicates when motion is detected
static void IRAM_ATTR detectsMovement(void * arg){
  //Serial.println("MOTION DETECTED!!!");
  motionDetected = true;
}

void setup(){
  WRITE_PERI_REG(RTC_CNTL_BROWN_OUT_REG, 0);
  Serial.begin(115200);

  // Set All Sensors Pin As INPUT
  pinMode(door1, INPUT);
  pinMode(door2, INPUT);
  pinMode(firePin, INPUT);
  pinMode(smokePin, INPUT);

  // Camera Flash
  pinMode(FLASH_LED_PIN, OUTPUT);
  digitalWrite(FLASH_LED_PIN, flashState);
```

```
// Initialize WiFi
WiFi.mode(WIFI_STA);
Serial.println();
Serial.print("Connecting to ");
Serial.println(ssid);
WiFi.begin(ssid, password);
while (WiFi.status() != WL_CONNECTED) {
    Serial.print(".");
    delay(500);
}
Serial.println();
Serial.print("ESP32-CAM IP Address: ");
Serial.println(WiFi.localIP());

camera_config_t config;
config.ledc_channel = LEDC_CHANNEL_0;
config.ledc_timer = LEDC_TIMER_0;
config.pin_d0 = Y2_GPIO_NUM;
config.pin_d1 = Y3_GPIO_NUM;
config.pin_d2 = Y4_GPIO_NUM;
config.pin_d3 = Y5_GPIO_NUM;
config.pin_d4 = Y6_GPIO_NUM;
config.pin_d5 = Y7_GPIO_NUM;
config.pin_d6 = Y8_GPIO_NUM;
config.pin_d7 = Y9_GPIO_NUM;
config.pin_xclk = XCLK_GPIO_NUM;
config.pin_pclk = PCLK_GPIO_NUM;
config.pin_vsync = VSYNC_GPIO_NUM;
config.pin_href = HREF_GPIO_NUM;
config.pin_sscb_sda = SIOD_GPIO_NUM;
config.pin_sscb_scl = SIOC_GPIO_NUM;
config.pin_pwdn = PWDN_GPIO_NUM;
config.pin_reset = RESET_GPIO_NUM;
config.xclk_freq_hz = 20000000;
config.pixel_format = PIXFORMAT_JPEG;

//init with high specs to pre-allocate larger buffers
if(psramFound()){
    config.frame_size = FRAMESIZE_UXGA;
    config.jpeg_quality = 10; //0-63 lower number means higher quality
    config.fb_count = 2;
} else {
    config.frame_size = FRAMESIZE_SVGA;
    config.jpeg_quality = 12; //0-63 lower number means higher quality
    config.fb_count = 1;
}

// camera init
esp_err_t err = esp_camera_init(&config);
if (err != ESP_OK) {
```

```
Serial.printf("Camera init failed with error 0x%x", err);
delay(1000);
ESP.restart();
}

// Drop down frame size for higher initial frame rate
sensor_t * s = esp_camera_sensor_get();
s->set_framesize(s, FRAMESIZE_CIF); //
UXGA|SXGA|XGA|SVGA|VGA|CIF|QVGA|HQVGA|QQVGA

// PIR Motion Sensor mode INPUT_PULLUP
//err = gpio_install_isr_service(0);
err = gpio_isr_handler_add(GPIO_NUM_13, &detectsMovement, (void *) 13);
if (err != ESP_OK) {
    Serial.printf("handler add failed with error 0x%x \r\n", err);
}
err = gpio_set_intr_type(GPIO_NUM_13, GPIO_INTR_POSEDGE);
if (err != ESP_OK) {
    Serial.printf("set intr type failed with error 0x%x \r\n", err);
}

delay(40000); // Give time for PIR and MQ6 Gas Sensor to get Stable
Serial.printf("PIR Sensor Initilized!! \n");
}

void loop() {

    if (sendPhoto) {
        Serial.println("Preparing photo");
        sendPhotoTelegram();
        sendPhoto = false;
    }

    // If Door 1 is got Opened
    door1stat = digitalRead(door1);
    if(!door1stat && doorLockMonitor){
        bot.sendMessage(chatId, "Alert - Door1 Opened !!", "");
        Serial.println("Door1 Opened");
        door1stat = t
        rue;
    }

    // If Door 2 is got Opened
    door2stat = digitalRead(door2);
    if(!door2stat && doorLockMonitor){
        bot.sendMessage(chatId, "Alert - Door2 Opened !!", "");
        Serial.println("Door2 Opened");
        door2stat = true;
    }

    // If Fire got detected in house
```



```
fire = digitalRead(firePin);
if(!fire && fireDetectMonitor){
    bot.sendMessage(chatId, "Alert - Fire at house !!", "");
    Serial.println("Fire Detected");
    fire = false;
}

// If Smoke got detected in house
smoke = digitalRead(smokePin);
if(!smoke && smokeDetectMonitor){
    bot.sendMessage(chatId, "Alert - Something is Burning !!", "");
    Serial.println("Smoke Detected");
    smoke = false;
}

// If Intruder Motion got detected in house
if(motionDetected && motionDetectEnable){
    bot.sendMessage(chatId, "Motion detected!!", "");
    Serial.println("Motion Detected");
    sendPhotoTelegram();
    motionDetected = false;
    delay(2000);
}

if (millis() > lastTimeBotRan + botRequestDelay){
    int numNewMessages = bot.getUpdates(bot.last_message_received + 1);
    while (numNewMessages){
        Serial.println("got response");
        handleNewMessages (numNewMessages);
        numNewMessages = bot.getUpdates (bot.last_message_received + 1);
    }
    lastTimeBotRan = millis();
}
}

String sendPhotoTelegram(){
    const char* myDomain = "api.telegram.org";
    String getAll = "";
    String getBody = "";

    camera_fb_t * fb = NULL;
    fb = esp_camera_fb_get();
    if(!fb) {
        Serial.println("Camera capture failed");
        delay(1000);
        ESP.restart();
        return "Camera capture failed";
    }

    Serial.println("Connect to " + String(myDomain));
```

```
if (clientTCP.connect(myDomain, 443)) {
    Serial.println("Connection successful");

    String head = "--make2explore\r\nContent-Disposition: form-data;
name=\"chat_id\"; \r\n\r\n" + chatId + "\r\n--make2explore\r\nContent-
Disposition: form-data; name=\"photo\"; filename=\"esp32-
cam.jpg\"\r\nContent-Type: image/jpeg\r\n\r\n";
    String tail = "\r\n--make2explore--\r\n";

    uint16_t imageLen = fb->len;
    uint16_t extraLen = head.length() + tail.length();
    uint16_t totalLen = imageLen + extraLen;

    clientTCP.println("POST /bot"+BOTtoken+"/sendPhoto HTTP/1.1");
    clientTCP.println("Host: " + String(myDomain));
    clientTCP.println("Content-Length: " + String(totalLen));
    clientTCP.println("Content-Type: multipart/form-data;
boundary=make2explore");
    clientTCP.println();
    clientTCP.print(head);

    uint8_t *fbBuf = fb->buf;
    size_t fbLen = fb->len;
    for (size_t n=0;n<fbLen;n=n+1024) {
        if (n+1024<fbLen) {
            clientTCP.write(fbBuf, 1024);
            fbBuf += 1024;
        }
        else if (fbLen%1024>0) {
            size_t remainder = fbLen%1024;
            clientTCP.write(fbBuf, remainder);
        }
    }

    clientTCP.print(tail);

    esp_camera_fb_return(fb);

    int waitTime = 10000; // timeout 10 seconds
    long startTimer = millis();
    boolean state = false;

    while ((startTimer + waitTime) > millis()){
        Serial.print(".");
        delay(100);
        while (clientTCP.available()) {
            char c = clientTCP.read();
            if (state==true) getBody += String(c);
            if (c == '\n') {
                if (getAll.length()==0) state=true;
                getAll = "";
            }
        }
    }
}
```

```
    }
    else if (c != '\r')
        getAll += String(c);
    startTimer = millis();
}
if (getBody.length() > 0) break;
}
clientTCP.stop();
Serial.println(getBody);
}
else {
    getBody = "Connected to api.telegram.org failed.";
    Serial.println("Connected to api.telegram.org failed.");
}
return getBody;
}

void handleNewMessages(int numNewMessages) {
    Serial.print("Handle New Messages: ");
    Serial.println(numNewMessages);

    for (int i = 0; i < numNewMessages; i++) {
        // Chat id of the requester
        String chat_id = String(bot.messages[i].chat_id);
        if (chat_id != chatId) {
            bot.sendMessage(chat_id, "Unauthorized user", "");
            continue;
        }

        // Print the received message
        String text = bot.messages[i].text;
        Serial.println(text);

        String fromName = bot.messages[i].from_name;

        // Implementation of all the Commands from START
        if (text == "/flashOn") {
            flashState = true;
            bot.sendMessage(chat_id, "Flash is set to ON", "");
            digitalWrite(FLASH_LED_PIN, flashState);
        }

        if (text == "/flashOff") {
            flashState = false;
            bot.sendMessage(chat_id, "Flash is set to OFF", "");
            digitalWrite(FLASH_LED_PIN, flashState);
        }

        if (text == "/photo") {
            sendPhoto = true;
            bot.sendMessage(chat_id, "Capturing Photo...", "");
        }
    }
}
```

```
Serial.println("New photo request");
}

if (text == "/EnableMotionAlert") {
    motionDetectEnable = true;
    bot.sendMessage(chat_id, "Motion Alert - Enabled", "");
    Serial.println("Enable the Motion alert");
}

if (text == "/DisableMotionAlert") {
    motionDetectEnable = false;
    bot.sendMessage(chat_id, "Motion Alert - Disabled", "");
    Serial.println("Disable the Motion alert");
}

if (text == "/EnableDoorAlert") {
    doorLockMonitor = true;
    bot.sendMessage(chat_id, "Monitor Doors - Enabled", "");
    Serial.println("Enable the Monitor Doors");
}

if (text == "/DisableDoorAlert") {
    doorLockMonitor = false;
    bot.sendMessage(chat_id, "Monitor Doors - Disabled", "");
    Serial.println("Disable the Monitor Doors");
}

if (text == "/EnableFireAlert") {
    fireDetectMonitor = true;
    bot.sendMessage(chat_id, "Fire Detector - Enabled", "");
    Serial.println("Enable the Fire Detector");
}

if (text == "/DisableFireAlert") {
    fireDetectMonitor = false;
    bot.sendMessage(chat_id, "Fire Detector - Disabled", "");
    Serial.println("Disable the Fire Detector");
}

if (text == "/EnableSmokeAlert") {
    smokeDetectMonitor = true;
    bot.sendMessage(chat_id, "Smoke Detector - Enabled", "");
    Serial.println("Enable the Smoke Detector");
}

if (text == "/DisableSmokeAlert") {
    smokeDetectMonitor = false;
    bot.sendMessage(chat_id, "Smoke Detector - Disabled", "");
    Serial.println("Disable the Smoke Detector");
}
}
```

```
if (text == "/start"){
    String welcome = "Welcome to the make2explore ESP32-CAM Telegram
bot.\n\n";
    welcome += "Use the following command to Setup the ESPCAM.\n\n";
    welcome += "/flashOn : Turn on the flash LED\n";
    welcome += "/flashOff : Turn off the flash LED\n";
    welcome += "/photo : takes a new photo\n\n";
    welcome += "/EnableMotionAlert : enables the motion Alert System\n";
    welcome += "/DisableMotionAlert : disables the motion Alert
System\n\n";
    welcome += "/EnableDoorAlert : enables the door Open Alert System\n";
    welcome += "/DisableDoorAlert : disables the door Open Alert
System\n\n";
    welcome += "/EnableSmokeAlert : enables the Smoke Alert System\n";
    welcome += "/DisableSmokeAlert : disables the Smoke Alert System\n\n";
    welcome += "/EnableFireAlert : enables the Fire Alert System\n";
    welcome += "/DisableFireAlert : disables the Fire Alert System\n\n";
    welcome += "You'll receive a photo whenever motion is detected.\n";
    bot.sendMessage(chatId, welcome, "Markdown");
}
}
}
```