

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістра

(освітній ступінь)

на тему: **Методи і засоби організації комп'ютерних систем захисту
стаціонарних фізичних об'єктів з використанням GSM- сигналізації**

Виконав: студент (ка) 6 курсу, групи СІм-61
спеціальності 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

	(підпис)	Іваницький В.А. (прізвище та ініціали)
Керівник	(підпис)	Жаровський Р.О. (прізвище та ініціали)
Нормоконтроль	(підпис)	Тиш Є.В. (прізвище та ініціали)
Завідувач кафедри	(підпис)	Осухівська Г.М. (прізвище та ініціали)
Рецензент	(підпис)	Петрик М. Р. (прізвище та ініціали)

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет комп'ютерно-інформаційних систем і програмної інженерії
Кафедра комп'ютерних систем та мереж

ЗАТВЕРДЖУЮ

Завідувач кафедри Осухівська Г.М.

« 11 » листопада 2024 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

студенту Іваницькому Віктору Андрійовичу
(прізвище, ім'я, по-батькові)

1. Тема проекту (роботи) Методи і засоби організації комп'ютерних систем захисту стаціонарних фізичних об'єктів з використанням GSM- сигналізації

Керівник проекту (роботи) Жаровський Руслан Олегович, к.т.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «29» листопада 2024 року №4/7-1144

2. Термін подання студентом завершеної роботи _____

3. Вихідні дані до роботи Принципи функціонування GSM-сигналізації, IoT пристрої розумного будинку, протоколи передачі даних у GSM-сигналізаціях

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз GSM-технології передачі даних у системах захисту стаціонарних об'єктів
2. Проектування комп'ютерної системи захисту стаціонарних фізичних об'єктів з
використанням GSM-сигналізації 3. Імплементация програмної моделі розпізнавання образів
та системного програмного забезпечення GSM-сигналізації 4. Охорона праці та безпека в
надзвичайних ситуаціях. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1.Актуальність і мета дослідження.

2. Задачі, об'єкт і предмет, наукова новизна і практична цінність дослідження.

3. Принципи роботи GSM-мереж

4. Існуючі рішення організації систем GSM-сигналізації

5. Архітектура комп'ютерної системи захисту фізичних стаціонарних об'єктів

6. Алгоритми роботи комп'ютерної системи

7. Топологія нейронної мережі розпізнавання облич.

8. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
<i>Охорона праці та безпека в надзвичайних ситуаціях</i>	<i>Осухівська Г.М., зав. каф. КС</i>		
	<i>Стручок В.С., ст. викладач. каф. ОХ</i>		

7. Дата видачі завдання 11.11.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	<i>Аналіз існуючих методів та засобів розв'язання науково-технічних проблем, що відповідають тематиці кваліфікаційної роботи.</i>	<i>20.11.2024 р. – 30.11.2024 р.</i>	<i>виконано</i>
2.	<i>Аналіз GSM-технології передачі даних у системах захисту стаціонарних об'єктів</i>	<i>30.11.2024 р.- 04.12.2024 р.</i>	<i>виконано</i>
3.	<i>Проектування комп'ютерної системи захисту стаціонарних фізичних об'єктів використанням GSM-сигналізації</i>	<i>04.12.2024 р.- 09.12.2024 р.</i>	<i>виконано</i>
4.	<i>Імплементация програмної моделі розпізнавання образів та системного програмного забезпечення GSM-сигналізації</i>	<i>09.12.2024 р.- 15.12.2024 р.</i>	<i>виконано</i> <i>виконано</i> <i>виконано</i>
5.	<i>Охорона праці та безпека в надзвичайних ситуаціях</i>	<i>15.12.2024 р.- 17.12.2024 р.</i>	<i>виконано</i>
6.	<i>Оформлення пояснювальної записки і графічного матеріалу</i>	<i>17.12.2024 р.</i>	<i>виконано</i>
7.	<i>Попередній захист кваліфікаційної роботи магістра</i>	<i>18.12.2024 р.</i>	<i>виконано</i>
8.	<i>Захист кваліфікаційної роботи магістра</i>		

Студент

(підпис)

Іваницький В.А.

(прізвище та ініціали)

Керівник проекту (роботи)

(підпис)

Жаровський Р.О.

(прізвище та ініціали)

АНОТАЦІЯ

Іваницький В.А. Методи і засоби організації комп'ютерних систем захисту стаціонарних фізичних об'єктів з використанням GSM-сигналізації: робота на здобуття кваліфікаційного ступеня магістра: спец. 123 — комп'ютерна інженерія / наук. кер. Р.О. Жаровський. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2024. — 92 с.

Ключові слова: технологія, розробка, GSM, сигналізація, розумний будинок.

Кваліфікаційна робота магістра присвячена дослідженню методів і засобів організації комп'ютерних систем захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації.

У роботі спроектовано архітектуру комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі мікроконтролерів ESP32 та ESP32-CAM з підключенням сенсорів газу, температури і вологості, датчика руху і сумісної камери з роздільною здатністю 2Мп, що дало можливість підвищити функціональність системи за рахунок інтеграції програмної моделі інтелектуального розпізнавання облич.

Окрім цього, запропоновано архітектуру нейромережі для забезпечення функції розпізнавання облич, що використовує топологію згорткової нейронної мережі і дає змогу оптимізувати використання апаратних ресурсів за рахунок використання лише одного нейрону у вихідному шарі, розроблено загальний і частковий алгоритми роботи комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації, проведено налаштування параметрів для функціонування мікроконтролерів ESP32 та ESP32-CAM при управлінні системою формування сповіщень GSM-модуля.

ABSTRACT

Ivanytskyi V.A. Methods and tools for organizing computer systems to protect stationary physical objects using GSM signaling. /Master's Graduation Thesis: speciality 123 - Computer engineering/supervisor R.O. Zharovskyi. Ternopil: Ternopil Ivan Puluj National Technical University, 2024. — 92 p.

Keywords: method, tool, development, computer system, GSM, alarm.

The master's qualification work is devoted to the study of methods and means of organizing computer systems for protecting physical stationary objects based on GSM-alarming.

The work designs the architecture of a computer system for protecting physical stationary objects based on ESP32 and ESP32-CAM microcontrollers with the connection of gas, temperature and humidity sensors, a motion sensor and a compatible camera with a resolution of 2MP, which made it possible to increase the functionality of the system by integrating a software model for intelligent face recognition.

In addition, a neural network architecture is proposed to provide the face recognition function, which uses the topology of a convolutional neural network and allows you to optimize the use of hardware resources by using only one neuron in the output layer, general and partial algorithms for the operation of a computer system for protecting physical stationary objects based on GSM-alarming have been developed, and parameters for the operation of ESP32 and ESP32-CAM microcontrollers when controlling the GSM module notification generation system have been set.

ЗМІСТ

ВСТУП

8

РОЗДІЛ 1 АНАЛІЗ GSM-ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ У СИСТЕМАХ ЗАХИСТУ СТАЦІОНАРНИХ ОБ'ЄКТІВ 13

1.1. Аналіз принципів функціонування GSM-мереж 13

1.2. Аналіз існуючих рішень організації систем безпеки фізичних стаціонарних об'єктів 20

1.2.1. Аналіз системи безпеки на основі Raspberry PI, GSM та Bluetooth 24

1.2.2. Аналіз системи GSM-сигналізації на основі Raspberry PI та Java 25

1.3. Висновки до розділу 27

РОЗДІЛ 2 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ СИСТЕМИ ЗАХИСТУ СТАЦІОНАРНИХ ФІЗИЧНИХ ОБ'ЄКТІВ 3

ВИКОРИСТАННЯМ GSM-СИГНАЛІЗАЦІЇ 29

2.1. Архітектура комп'ютерної системи захисту стаціонарних фізичних об'єктів 29

2.2. Обґрунтування і вибір апаратного забезпечення комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації 31

2.2.1. Контролер управління пристроями GSM-сигналізації 31

2.2.2. Функції GSM-модуля у системі забезпечення безпеки фізичних стаціонарних об'єктів 32

2.2.3. Сенсор руху, як тригер активації GSM-сигналізації 34

2.2.4. Сенсор газу як засіб сповіщувач небезпечної ситуації 36

2.2.5. Сенсор вимірювання температури і вологості у системі GSM-сигналізації 40

2.2.6. Модуль ESP32-CAM та камера OV2640, як апаратна складова інтелектуального розпізнавання облич 41

2.3. Проектування схем з'єднання та інсталяція компонентів системи GSM-сигналізації 47

2.4. Висновки до розділу	50
РОЗДІЛ 3 ІМПЛЕМЕНТАЦІЯ ПРОГРАМНОЇ МОДЕЛІ РОЗПІЗНАВАННЯ ОБРАЗІВ ТА СИСТЕМНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ GSM-СИГНАЛІЗАЦІЇ	52
3.1. Нейронна мережа для ідентифікації зображення з камери системи GSM-сигналізації	52
3.2. Проектування топології нейронної мережі для реалізації функції розпізнавання обличчя системи GSM-сигналізації	61
3.3. Розробка алгоритму роботи системи захисту стаціонарних об'єктів на основі GSM-сигналізації	64
3.4. Встановлення та налаштування бібліотек ESP32-CAM	67
3.5. Висновки до розділу	74
РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ	75
4.1. Охорона праці	75
4.2. Засоби захисту персоналу від уражень радіації	78
ВИСНОВКИ	82
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	84
ДОДАТОК А ТЕКСТ НАУКОВИХ ПУБЛІКАЦІЙ КВАЛІФІКАЦІЙНОЇ РОБОТИ МАГІСТРА	88

ВСТУП

Актуальність теми. Прогрес у галузі інформаційних технологій стимулює інтенсивне впровадження все нових технічних та водночас інтелектуальних рішень для забезпечення комфорту, розширення функціональності та надійності систем різного призначення. Зважаючи на те що, результати прогресу можна використати як для досягнення хороших цілей, так і для поганих, то актуальними завданнями є розробка систем захисту об'єктів, зокрема, фізичних стаціонарних та мобільних.

Сьогодні на ринку існує багато коробкових рішень, які дають змогу захистити будинок та забезпечують відлякування злодіїв. Однак основним їх недоліком є відсутність можливостей щодо оновлення та впровадження сучасних методів і засобів захисту. Зважаючи на це, доцільно впроваджувати нестандартні рішення, які використовують останні досягнення у галузі інтернету речей (IoT) та штучного інтелекту (машинного навчання). Комбінація таких методів і засобів забезпечують ефективність імплементації «розумних будинків», управління пристроями у якому можна виконувати дистанційно. При проектуванні систем захисту важливо забезпечити віддаленість керування компонентами у системі захисті і їх здатність формувати сповіщення з гарантією їх доставки кінцевому користувачу. Одним із способів формування та пересилання сповіщень є використання GSM-мережі, яка надає можливість відправки повідомлень або телефонування власнику системи.

Існує багато способів надсилання та отримання електронних повідомлень, але SMS є більш популярним. Технологія коротких повідомлень використовується як спосіб отримання одноразового паролю (OTP) при автентифікації у багатьох веб-додатках, при доступі до пристроїв інтернету речей (IoT), скидання пароля, мобільного банкінгу тощо. Цей протокол призначений для федеративного керування, тобто мобільна мережа частково керується багатьма незалежними операторами, і

їй не потрібно мати центрального оператора для всієї мережі. Крім того, багато незалежних централізованих мереж можуть з'єднуватися разом, щоб збільшити мережу. Окрім цього, цей протокол може забезпечити ідентифікацію, автентифікацію, цілісність, неспростовність, конфіденційність і доступність до даних.

Завдяки напрацюванням українських та закордонних вчених і таких корпорацій, як IBM, Google, Microsoft та інших, на сьогодні розроблено та експлуатується доволі багато рішень щодо побудови систем захисту на основі IoT. Більшість таких систем базуються на основі мікроконтролера управління по типу Arduino чи Raspberry PI, а також датчиків різного призначення. З іншого боку такі системи повинні бути більш інтелектуалізованими з точки зору розпізнавання об'єктів. Тому актуальними задачами є розробка методів і засобів, які забезпечили б симбіоз технологій IoT і машинного навчання для підвищення ефективності захисту фізичних стаціонарних об'єктів.

Мета кваліфікаційної роботи полягає у дослідженні методів і засобів захисту фізичних стаціонарних об'єктів на основі GSM-сигналізацій з використанням IoT пристроїв та алгоритмів розпізнавання образів.

Серед сукупності задач, які потрібно вирішити у кваліфікаційній роботі магістра, основними є:

- аналітичний огляд принципів і функціональності мереж передачі даних на основі технології GSM;
- аналіз сучасного стану досліджень у сфері захисту стаціонарних об'єктів на основі IoT;
- проектування архітектури системи захисту об'єктів на основі GSM-сигналізації з інтегрованою функцією розпізнавання облич;
- розробка оптимізованого алгоритму машинного навчання для виявлення та розпізнавання облич в режимі реального часу та в обмежених апаратних ресурсах;

- обґрунтування вибору апаратного і програмного забезпечення системи захисту стаціонарних об'єктів на основі GSM-сигналізації;
- налаштування апаратної і програмної складової комп'ютерної системи;
- розробка програмного забезпечення зчитування та управління сенсорами, а також програмна реалізація підсистеми розпізнавання облич.

Об'єкт дослідження: процеси побудови систем захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації.

Предмет дослідження: методи і засоби побудови GSM-сигналізацій на основі IoT, алгоритми машинного навчання при розпізнаванні образів.

Методи дослідження: Для вирішення поставлених у кваліфікаційній роботі задач використано методи: аналізу та узагальнення – при дослідженні особливостей функціонування GSM-мереж та систем на основі IoT, нейромережових технологій і машинного навчання – при розробці алгоритму і побудові моделі розпізнавання облич; проектування, програмування – при розробці апаратного і програмного забезпечення системи захисту фізичних стаціонарних об'єктів; експеримент та вимірювання – при тестуванні запропонованого рішення.

Наукова новизна отриманих результатів. Наукова новизна, одержаних у роботі результатів полягає в наступному.

- уперше спроектовано архітектуру комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі мікроконтролерів ESP32 та ESP32-CAM з підключенням сенсорів газу, температури і вологості, датчика руху і сумісної камери з роздільною здатністю 2Мп, що дало можливість підвищити функціональність системи за рахунок інтеграції програмної моделі інтелектуального розпізнавання облич, яка активується при спрацюванні тригера у вигляді сигналу від сенсора руху з подальшою передачею сповіщення за допомогою GSM-модуля власнику об'єкта.

- набули подальшого розвитку топології архітектури нейромережі для забезпечення функції розпізнавання облич, що

використовує топологію згорткової нейронної мережі і дає змогу оптимізувати використання апаратних ресурсів за рахунок використання лише одного нейрону у вихідному шарі.

Практичне значення одержаних результатів. Спроековано комп'ютерну систему захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації до складу якої входить мікроконтролери на базі ESP32/ESP32-CAM, сенсор температури і вологості, датчик газу, відеокамера та GSM-модуль, реалізовано програмне забезпечення управління сигналізацією та програмну модель розпізнавання облич на основі згорткової нейронної мережі, що дало змогу підвищити надійність і ефективність такого класу комп'ютерних систем.

Публікації. Результати дипломної роботи апробовані XII науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (18-19 грудня 2024 року) як тези конференцій.

1. Жаровський Р.О., Іваницький В.А. GSM-сигналізації як спосіб розширення функціональності розумних будинків та підвищення безпеки об'єктів нерухомості. . Матеріали XII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (18-19 грудня 2024 року). Тернопіль: ТНТУ. 2024. С. 124.

2. Жаровський Р.О., Іваницький В.А. Організація захисту стаціонарного об'єкту нерухомості на основі GSM-сигналізації та мікроконтролера Raspberry Pi. Матеріали XII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (18-19 грудня 2024 року). Тернопіль: ТНТУ. 2024. С. 125.

Структура роботи. Кваліфікаційна робота містить розрахунково-пояснювальну записку та графічний матеріал. До складу записки входить вступу, 4 розділи, загальні висновки, список використаних

джерел і додатки. Обсяг роботи: розрахунково-пояснювальна записка – 92 арк. формату А4, графічна частина – 8 аркушів формату А1.

РОЗДІЛ 1
АНАЛІЗ
GSM-ТЕХНОЛОГІЇ
ПЕРЕДАЧІ ДАНИХ У
СИСТЕМАХ
ЗАХИСТУ
СТАЦІОНАРНИХ
ОБ'ЄКТІВ

1.1. Аналіз принципів функціонування GSM-мереж

GSM є цифровою мобільною мережею, якою, зазвичай, користуються користувачі мобільних телефонів у Європі та в усьому світі. GSM, найпопулярніша з трьох систем цифрової бездротової телефонії (TDMA, GSM і CDMA) і є версією множинного доступу з розділенням часу (TDMA).

GSM перетворює та стискає дані перед тим, як відправити їх по каналу з двома іншими потоками даних користувача, кожен зі своїм часовим інтервалом.

GSM означає глобальну систему мобільного зв'язку та водночас є відкритою цифровою стільниковою технологією, яка використовується для мобільного зв'язку.

Дана технологія використовує 4 різні діапазони частот: 850 МГц, 900 МГц, 1800 МГц і 1900 МГц. При функціонуванні цієї мережі використовується комбінація FDMA і TDMA.

GSM має 4 різні розміри стільників, зокрема: макро, мікро, піко та «парасолька». У макро-стільнику встановлюється антена базової станції, а у мікро-стільнику- висота антени менша за середній рівень.

Піко-стілльники представляють собою дрібні ділянки (соти) діаметром кілька метрів. Стільник типу парасольки покриває затінені (заповнює проміжки між областями покриття) області.

До особливостей GSM належить:

- підтримка міжнародного роумінгу;
- висока якість звуку;
- можливість підтримки кількох портативних пристроїв;
- спектральна/частотна ефективність;
- підтримка портативних пристроїв малої потужності;
- простота доступу до мережі;
- міжнародна сумісність ISDN;
- низька вартість обслуговування;

Технологія GSM володіє такими новими функціями і послугами: BSS та OSS (рис. 1.1).

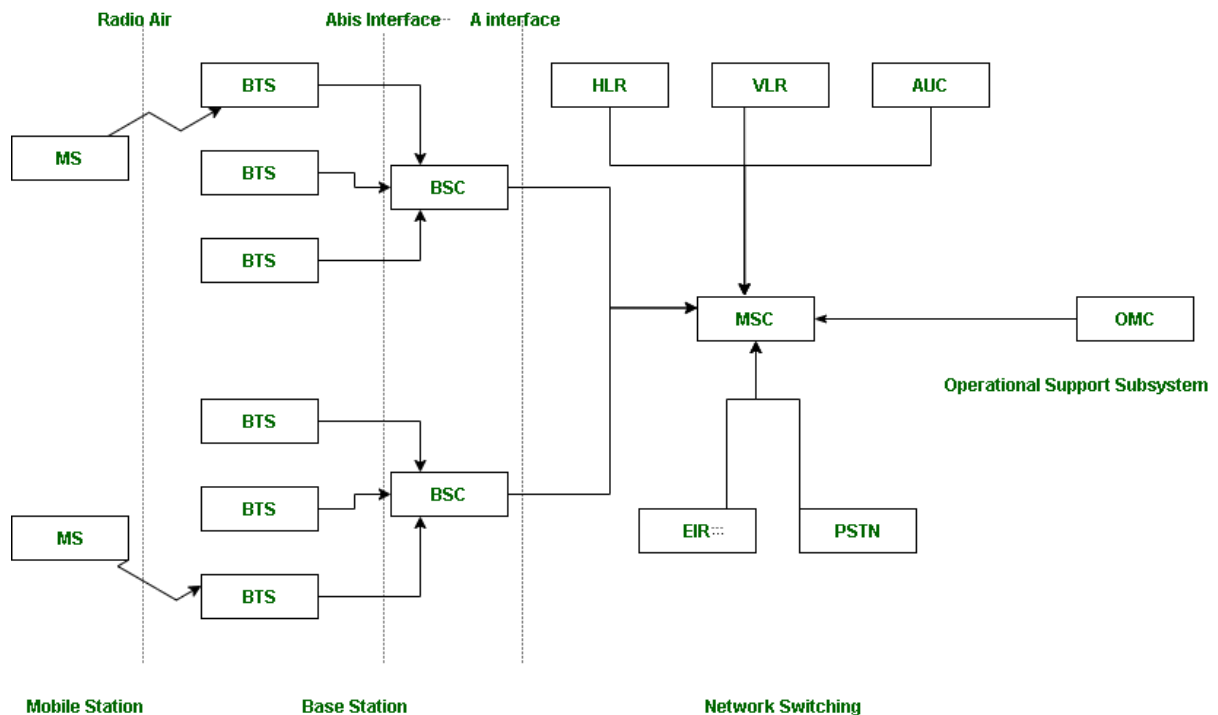


Рис. 1.1. Організація GSM-мережі на рівні інтерфейсів

BSS означає підсистему базової станції, що опрацьовує трафік і сигнали між мобільним телефоном і підсистемою комутації мережі. BSS складається з двох компонентів BTS і BSC.

NSS позначає підсистему мережі та комутації. NSS є базовою мережею GSM. Ця підсистема виконує функції керування викликами та мобільністю для мобільного телефону, присутнього в мережі. NSS мають різні компоненти, такі як VLR, HLR та EIR.

OSS інтерпретує операційну підсистему і є функціональним об'єктом, за допомогою якого мережевий оператор відстежує та контролює систему. OMC є частиною OSS. Мета OSS полягає в тому, щоб запропонувати клієнту економічно ефективну підтримку для всіх послуг з обслуговування GSM.

Припустимо, що є 3 мобільні станції, які підключені до вежі, і ця вежа підключена до BTS через TRX, а потім підключена до BSC і MSC.

Функції компонентів.

MS містить користувацьке обладнання та програмне забезпечення, необхідне для зв'язку з мобільною мережею. Мобільна станція (MS) = мобільне обладнання (ME) + модуль ідентифікації абонента (SIM). Тепер ці мобільні станції підключені до вежі, а вежа підключена до BTS через TRX.

TRX – це трансивер, який складається з передавача та приймача. Трансивер має дві характеристики: відправлення та отримання.

BTS означає базову приймально-передавальну станцію, яка забезпечує бездротовий зв'язок між обладнанням користувача та мережею. Кожна вежа має BTS.

BSC позначає контролер базової станції. BSC має кілька BTS. BSC можна розглядати як локальну станцію певної області, яка має кілька веж, а кілька веж мають BTS.

MSC позначає центр комутації мобільних пристроїв. MSC пов'язаний із функціями комутації зв'язку, такими як встановлення виклику, розблокування виклику та маршрутизація. Відстеження викликів,

переадресація викликів, усі функції виконуються на рівні MSC, який містить додаткові компоненти, зокрема VLR, HLR, AUC, EIR і PSTN.

VLR – це база даних, яка містить точне місцезнаходження всіх абонентів мобільного зв'язку, які зараз знаходяться в зоні обслуговування MSC. Якщо хтось переходить з однієї області в іншу, то запис позначається в базі даних VLR.

HLR розшифровується як Home Location Register – це база даних, що містить відповідні дані щодо абонентів, яким дозволено користуватися мережею GSM. HLR схожий на дім, який містить усі дані, як-от підтвердження посвідчення особи, який тарифний план обрано, яку мелодію абонент використовує тощо.

AUC є центром автентифікації. Даний компонент забезпечує автентифікацію мобільного абонента, який хоче підключитися до мережі.

EIR визначає реєстр ідентифікації обладнання і є базою даних, яка веде облік усіх дозволених або заборонених дій у мережі. Якщо абонент заблокований у мережі, то відповідно він не може увійти в мережу та не зможе здійснювати дзвінки.

PSTN інтерпретує комутаційну телефонну мережу загального користування. PSTN підключається до MSC і колись була мережею фіксованих аналогових телефонних систем. Зараз вона майже повністю цифрова мережа та включає мобільні та інші мережі, а також стаціонарні телефони. Попередні стаціонарні телефони, які розміщуються у будинках, є нічим іншим, як PSTN.

OMC означає Operation Maintenance Center. OMC контролює та підтримує роботу кожної MS, BSC та MSC у системі GSM. Три підсистеми BSS, NSS і OSS з'єднані один з одним через інтерфейси. Всього існує три інтерфейси:

Безпроводний інтерфейс також відомий як інтерфейс UM. Інтерфейс між MS і BTS називається інтерфейсом UM, оскільки він є мобільним аналогом U-інтерфейсу ISDN.

Інтерфейс Abis: це внутрішній інтерфейс BSS, який зв'язується з BTS і BSC і забезпечує комунікацію між BSS і MSC.

GSM – це всесвітньо визнаний протокол цифрового стільникового зв'язку, що створений у Європейському інституті стандартів телекомунікації з метою опису процедур функціонування другого покоління цифрових мереж мобільного зв'язку.

Це широкомасштабна програма комунікаційних технологій, яка використовує цифрові радіоканали для забезпечення аудіо, інформації та мультимедійних систем зв'язку. Кожен радіоканал GSM має ширину 200 кГц і далі розділений на кадри з восьми часових інтервалів.

Система GSM складається з мобільних станцій, базових станцій і систем комутації. Технологія GSM дозволяє від 8 до 16 аудіокористувачів використовувати один радіоканал, і кожна радіостанція може мати численні радіоканали. Завдяки своїй простоті, вартості та доступності GSM зараз є найбільш часто використовуваною мережевою технологією в IoT. Структура GSM-мережі на рівні підсистем представлена на рис. 1.2.

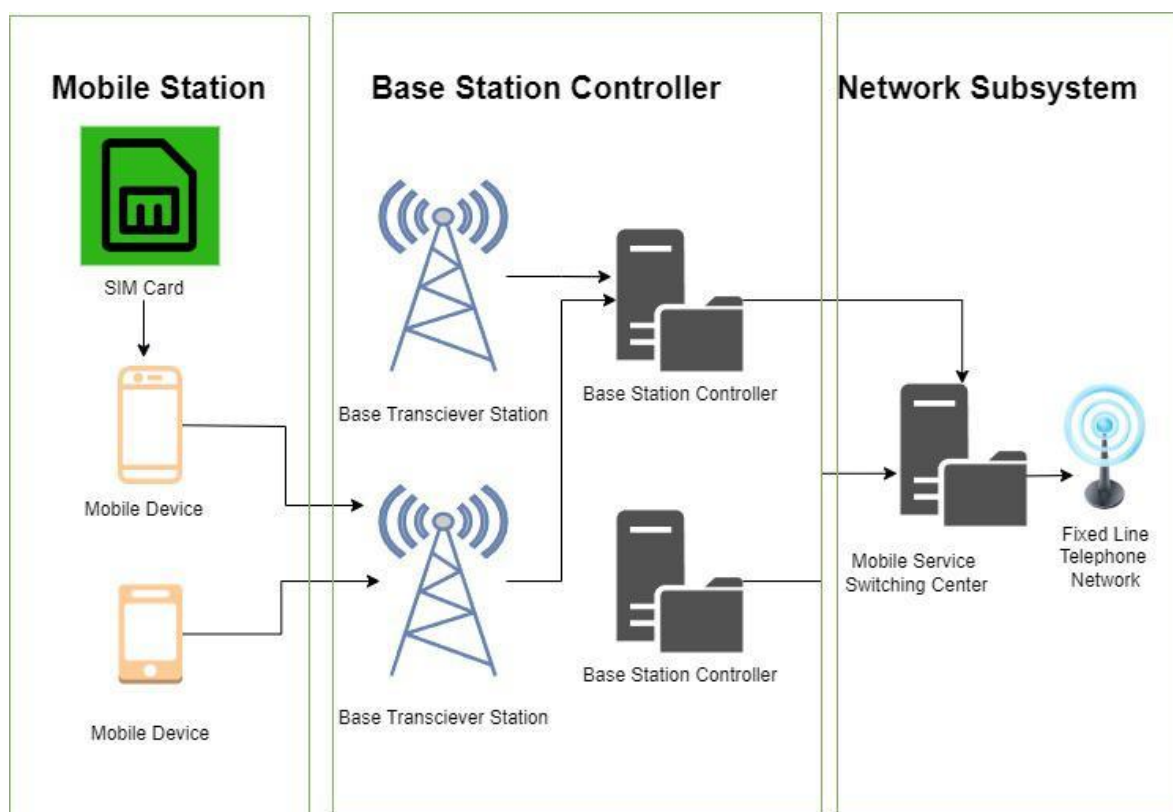


Рис. 1.2. Схема організації GSM-мережі на рівні підсистем

До послуг, що забезпечує GSM 2-го покоління належать описані нижче сервіси.

Сервіс носія трансферу інформації, що пропонує відмінний від існуючого, механізм передавання даних. Технологія GSM дає змогу забезпечити швидкість передачі на рівні до 9600 біт/с. при цьому може використовуватися як прозорий, так і непрозорий трансфер інформації.

Прозорі послуги-носії використовують лише фізичний рівень для передачі даних. Передача даних має постійну затримку пропускну здатності, якщо не виникає помилка передачі.

Непрозорі послуги-носії – використовують протоколи другого та третього рівня, щоб реалізувати виправлення помилок і керування потоком (рівень каналу даних і мережевий рівень).

Телепослуги включають в себе відеодзвінки, текст з відео, смайли та короткі текстові повідомлення (SMS).

Додаткові послуги, які надає GSM стосується:

- конференц-дзвінків;
- функції очікування дзвінка;
- переадресації дзвінків;
- функцій безпеки.

GSM пропонує кілька засобів захисту, використовуючи конфіденційну інформацію, що зберігається в AUC та на окремій SIM-картці. SIM-карта зберігає особисті секретні дані та захищена PIN-кодом від несанкціонованого використання.

Серед основних застосувань GSM потрібно відмітити наступні:

- мобільна телефонія;
- інтеграція VoIP SMS (служба коротких повідомлень)
- мобільний банкінг;
- системи розумного будинку;

- телемедицина;
- системи спостереження;
- системи сигналізації;
- стільникове мовлення.

До переваг GSM відноситься:

- сумісність – GSM широко використовується в усьому світі, тому він сумісний з багатьма різними мережами та пристроями.
- ефективний рівень безпеки – наявність сервісів аутентифікації, шифрування та конфіденційності дозволяють зберегти конфіденційність і дані користувача.
- ефективне використання смуги пропускання – GSM використовує техніку мультиплексування з часовим поділом (TDM), яка дозволяє багатьом користувачам використовувати один і той самий частотний канал у різний час, що забезпечує ефективне використання доступної смуги пропускання.
- роумінг – GSM дозволяє користувачам здійснювати міжнародний роумінг і використовувати свої мобільні телефони в інших країнах, які використовують той самий стандарт.
- широкий набір функцій – GSM підтримує широкий набір функцій, включаючи переадресацію дзвінка, очікування дзвінка, голосову пошту, конференц-дзвінки тощо.

До недоліків GSM можна віднести наступні:

- обмежене покриття – мережі GSM можуть мати обмежене покриття в деяких віддалених районах, що може ускладнити користувачам здійснення дзвінків або доступ до Інтернету.
- перевантаження мережі – мережі GSM можуть бути перевантаженими в години пік, що може призвести до переривання дзвінків або низької якості дзвінка.

- уразливості безпеки – наявність розширених функцій безпеки не гарантує стійкості до вразливостей, зокрема таких типів атак, як прослуховування чи підміна.

- швидкість передачі даних – мережі цього класу пропонують відносно низьку продуктивність у порівнянні з новими технологіями, такими як 3G і 4G.

- обмежений об'єм – для опрацювання великих даних мережі GSM володіють обмеженою ємністю і це створює незручності користувачам, які потребують високошвидкісного доступу до Інтернету або іншого програмного забезпечення, що інтенсивно опрацьовує дані.

GSM, CDMA та LTE (тривала еволюція) стільниково-бездротового зв'язку суттєво відрізняються з точки зору технології та бізнес-цілей.

GSM є найстарішим із трьох, який створений і прийнятий як стандарт у Європі для кодування і декодування даних. За допомогою технології процесора/чіпа, доступної на той час, тоді як CDMA в основному є методом доступу до каналу, а також є прикладом множинного доступу.

Множинний доступ по суті означає, що інформація кількома передавачами може надсилатися одночасно на один канал зв'язку, а LTE забезпечує швидку пікову передачу даних із початковою швидкістю до 100 Мбіт/с у низхідній частині та 30 Мбіт/с у вихідній. Завдяки високій швидкості, низькій затримці та вдосконаленим можливостям LTE дозволяє користувачам насолоджуватися вищою швидкістю передачі даних, безперебійним переглядом веб-сторінок і покращеним користувацьким досвідом.

GSM автоматизує та кодує інформацію перед передачею її через канал, який містить три унікальні потоки даних про користувача в кожному часовому інтервалі. Пристрої GSM використовують роумінгову SIM-карту, яка приймає найпотужніший сигнал мобільної мережі та не потребує

стаціонарного зв'язку. Датчик GSM – це модуль або чіп, який підключає пристрій до стільникових мереж GSM.

1.2. Аналіз існуючих рішень організації систем безпеки фізичних стаціонарних об'єктів

Із розвитком технологій також зростає і загроза безпеки, отскільки прогрес можна використовувати як у хороших цілях, так і навпаки.

Сьогодні розроблено і впроваджено досить багато рішень у сфері автоматизації безпеки та охоронної сигналізації. Більшість з них використовує управління за допомогою GSM-технологій і застосовується для забезпечення оптимальної безпеки житлових приміщень та інших фізичних стаціонарних об'єктів. Так для прикладу, комп'ютеризована система блокування дверей з сервоприводом дозволяє затримувати злодіїв всередині приміщення і є додатковою перевагою у порівнянні з іншими подібними системами. У даному випадку виконується контроль за датчиком блокування дверей і у випадку, коли коло розмикається власник або довірені особи об'єкту нерухомості чи автомобіля отримують телефонний дзвінок. При цьому, протягом деякого короткого часу двері блокуються і особа, що вторглась потрапляє у пастку. Такі системи є доволі точними при виконанні покладених на неї функцій завдяки доступу до мережі Інтернет.

Ще одним прикладом системи безпеки об'єктів нерухомості є системи розумних будинків, які базуються на технологіях GSM і Bluetooth. Характерною особливістю таких типів систем є високий рівень надійності за оптимальною вартістю. В основі таких систем центральним пристроєм керування можуть виступати різного роду мікроконтролери, наприклад, Arduino. Однак варто відмітити і той факт, що точність передачі даних між компонентами системи захисту є досить низькою, а її складна інтеграція підключення аудіодинаміків передбачає споживання великої кількості

енергії. З метою уникнення цих недоліків у [3] запропоновано альтернативну систему перетворення сповіщень за допомогою Raspberry Pi.

У публікаціях [3, 4] запропоновано проект системи захисту стаціонарних об'єктів із застосування радіочастотного методу пасивного типу та мікроконтролер atmega 16. У цьому випадку сканер виконує зчитування унікального ідентифікаційного номера з RFID-мітки. Автор пропонує потужну систему безпеки за невелику вартість та з відсутністю помилок.

Автори у [5] пропонують систему авторизації ключів, використовуючи випадковий пароль через мобільний телефон. Користувач може ввести пароль лише тричі, якщо пароль правильний, авторизована особа може отримати доступ до об'єкта. Якщо пароль неправильний, то вмикається і лунає звуковий сигнал, а замок неможливо відкрити і він залишається у заблокованому стані. При еталонній архітектурі двигун постійного струму використовується для замикання та відкривання дверей стаціонарного об'єкту, інтерфейс RS-232 забезпечує обмін даними через GSM.

У [6] пропонують дві системи реалізації: система блокування відкриття і закриття. При цьому застосовуються такі компоненти, як герконове реле, соленоїдний замок тощо. Блокувальний стаціонарного об'єкта вмонтовується у двері приміщення, де також поміщено і реле зчитування. Соленоїд розміщений на верхній стороні реле зчитування разом із замком дверей. Основною частиною архітектури замка є соленоїд. Соленоїд повністю вставляється в засув і відпускається, коли користувач повинен розблокувати двері.

У [7] запропонували рішення безпеки, яке можна застосовувати у банках, офісах, а також багатьох інших сферах. Автор рекомендував реалізацію запропонованого рішення, що дозволить, на його думку, безпечно охороняти коштовності та документи. Система блокування

передбачає також генерацію повідомлення на телефон користувача. Керування біометричною системою здійснюється за допомогою сенсорного пристрою Arduino та модуля GSM.

У [8] описано біометричну систему блокування на основі Arduino з використанням даних спеціалізованої картки. Для забезпечення персональних даних людини реалізовано модуль зчитування відбитків пальців і модуль HC05 Bluetooth для біометричної безпеки. Сервомотор використовується для самостійного розблокування, коли відбиток пальця правильно зчитаний уповноваженою особою. Дані картки зберігаються в хмарі і керуються за допомогою мобільного додатку. Веб-сторінка використовується для перегляду оновлень про негайні дії. Картка користувача сканується через QR-код, який знаходиться в датчиках, і зберігає інформацію в таблиці Google. Користувач може отримати доступ до цієї таблиці за допомогою імені користувача та пароля. Веб-сторінка доступна з мобільного додатку, куди користувач може отримати доступ з будь-якого місця. Ця запропонована система є зручною біометричною системою блокування для всіх користувачів.

У [9] пропонується більш комплексна система, яка може одночасно використовуватися у багатоквартирних будинках, при керуванні в'їзними воротами і шлагбаумами та ін. Вона передбачає наявність кількох ключів. Зберігання цих ключів викликає занадто багато плутанини. Щоб уникнути цієї проблеми, інноваційна система замків пропонується як прототип із використанням нової технології. Цей новий метод матиме вдосконалення та інновації порівняно з існуючим прототипом. Пропонована система має розумну цифрову систему замикання для всіх типів дверей. Система дверних замків містить секретний кодовий замок замість ключів. Централізований вбудований модуль підходить для системи дверного замка при відкриванні дверей. Ця система дає змогу уникнути додаткових труднощів і має більш надійний механізм для загальної використання.

Найбільшою перевагою є те, що за мінімальних зусиль і витрат можна легко отримати доступ і встановити інфраструктуру.

У [10] автор пропонує метод радіочастотної ідентифікації для системи доступу до дверних замків. Ця система RFID вже використовується в усіх типах додатків IoT для задач інвентаризації та виявлення речей. При такому підході блокування виконується поетапно, що передбачає виконання таких кроків як активація, автентифікація і перевірка користувача, розблокування дверей. Основним використанням і перевагою запропонованого рішення є низька потужність і порівняно з активними мітками, пасивна мітка легша та дешевша. Основна інформація бази даних користувачів зберігається до реєстрації та виходу користувача. Розроблена система є недорогою, легко встановлюваною та надійною з використанням бездротової технології GSM, Bluetooth.

1.2.1. Аналіз системи безпеки на основі Raspberry Pi, GSM та Bluetooth

Структурно систему безпеки на основі технологій GSM та Bluetooth представлено на рис. 1.3.

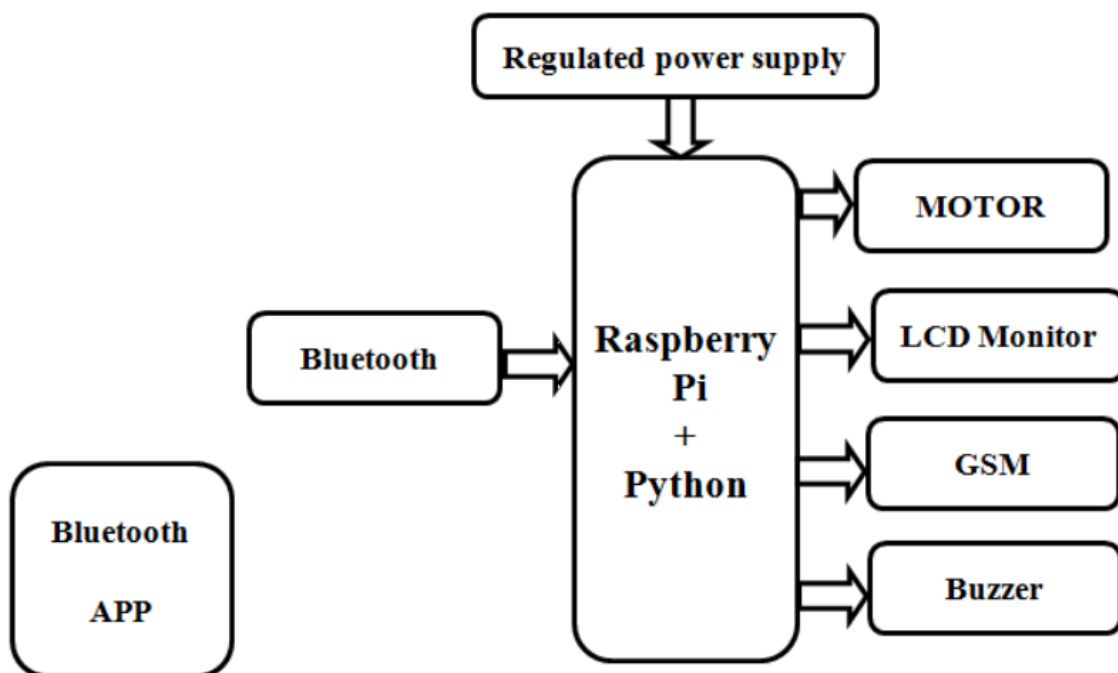


Рис. 1.3. Структура системи безпеки на основі Raspberry PI, GSM та Bluetooth

Система, представлена на рис. 1.3, реалізується за допомогою бездротової технології передачі даних та передбачає застосування програмного забезпечення керування мікроконтролером, яке вбудовано у модуль Bluetooth. Функціями програми є надсилання запиту паролю на мобільний пристрій і у випадку, коли відповідь збігається з наявним у базі даних паролем, то замок дверей розблоковується. У користувача є три спроби введення паролю, якщо у жодній із спроб не зазначено вірного паролю, то відбувається автоматичне надсилання GSM-сповіщення авторизованій особі, а зумер сповіщає про сповіщення про неправильний пароль через динаміки.

1.2.2. Аналіз системи GSM-сигналізації на основі Raspberry PI та Java

Технологія систем організації безпеки об'єктів на основі Java дає змогу реалізувати досить надійні рішення у цій області. Однак при цьому вимагається доволі дорога дротова установка та використання високоякісних персональних комп'ютерів [11]. Попередні системи безпеки цілком і повністю залежали від телефонної лінії та використовували в якості пульта дистанційного керування мобільний телефон [12].

Для дистанційного керування та моніторингу будинку за допомогою Інтернету потрібен потужний ноутбук або комп'ютер, який важко носити з собою цілий день. Таким чином, альтернативою можуть бути мобільні телефони з операційною системою на ньому для дистанційного керування та моніторингу будинку.

Система використовує бездротову технологію для зв'язку між пристроями. Завдяки вбудованій технології Bluetooth пристрої утворюють мережу, у якій вони можуть спілкуватися один з одним. Проте існують певні проблеми, пов'язані з проектуванням системи автоматизації. Зокрема, це стосується масштабованості системи.

Система повинна бути масштабованою, щоб новий пристрій можна було легко інтегрувати в неї. Існує два підрозділи системи безпеки; комерційна та домашня система безпеки. Оскільки комерційна система безпеки, зазвичай, вимагала надто великих витрат, щоб покрити витрати звичайної родини, була розроблена система домашньої безпеки своїми руками та поєднана з модулями Bluetooth [5].

У літературних дослідженнях пропонується низка систем безпеки, заснованих на нових технологіях, таких як мережа сенсорів, FPGA, DSP та мікроконтролери [6].

Бездротова технологія має деякі значні переваги порівняно з дротовою, наприклад, полегшує інсталяцію та обслуговування. Технології і протоколи передачі даних на основі Bluetooth, ZigBee, стандарту 802.11 є найпопулярнішими технологіями в області домашніх бездротових мереж.

Інтернет речей – це технологія, що може використовуватися для покращення домашньої безпеки та охорони мережі фізичних об'єктів, пристроїв, будівель, транспортних засобів та інших предметів, вбудованих датчиків і підключення до мережі, яка дозволяє використовувати електроніку, програмне забезпечення, щоб ці об'єкти мали можливість збирати й обмінюватися даними, а також фізичний пристрої могли б з'єднуватися з інтернет датчиками [11].

Ключовою відмінністю між бездротовою сенсорною мережею та GSM є її широка зона покриття, що сприяє комунікації на дуже великій відстані.

На рис. 1.4 представлено схему організації системи безпеки, яка запропонована у [12].

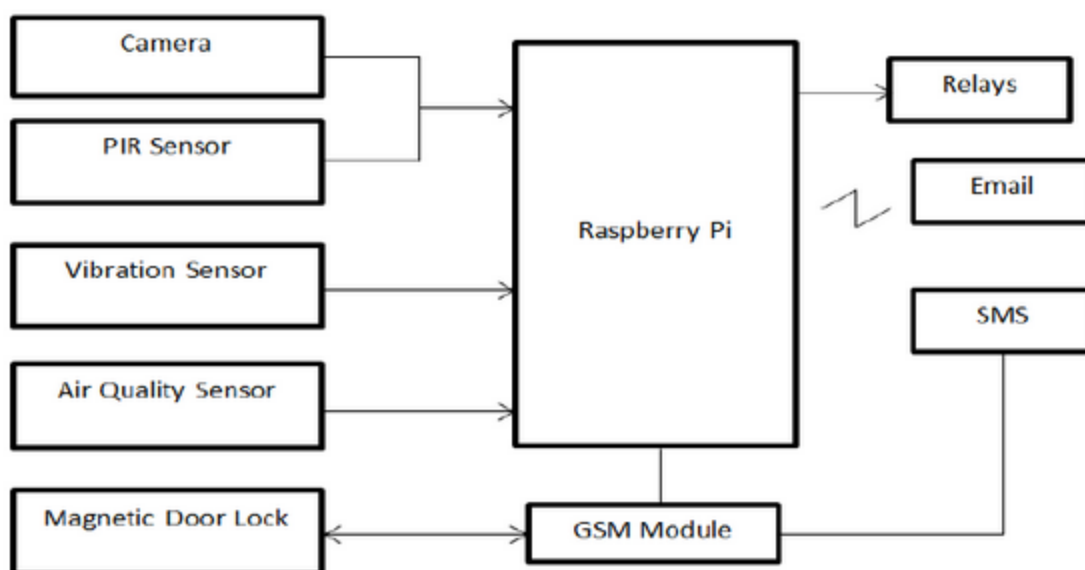


Рис. 1.4. Один з варіантів схеми організації системи безпеки будинку

Плата Raspberry PI управляє ланцюгом реле для керування вентилятором і освітленням і захоплення зображення за допомогою камери. Ця система складається також з GSM-модему для надсилання повідомлення разом із посиланням на зображення [12].

Датчики руху і вібрації підключаються до мікроконтролера Arduino, а кодувальник паролів закріплений на дверях. Якщо прийде особа, інформацію про яку існує у базі даних, то після введення паролю вона потрапить до будинку.

Робот має датчик температури, де, якщо температура підвищується, з'являється звуковий сигнал, який сповіщає власників будинку. Є кілька різних функцій, доступних у зв'язку GSM, які є зручними для запропонованої системи, як-от низька вартість, малий розмір, зручний інтерфейс, генерація екстреної сигналізації, дуже короткий час відгуку та головна особливість – широка зона покриття. Таким чином, користувач може взаємодіяти з системою навіть з дуже віддаленого місця, далеко від міських районів.

Різні датчики встановлюються в різних місцях будинку. USB-камера та PIR-датчик, встановлені біля входних дверей будинку, підключаються до

Raspberry PI. Коли PIR-датчик видає високий рівень сигналу або USB-камера ввімкнена, відбувається захоплення зображення відвідувача та надсилання на пошту ідентифікатор користувача власника, а також сповіщення надсилає на номер мобільного телефону власника.

Датчик вібрації встановлений на вікнах будинку. Коли датчики вібрації перевищують пороговий рівень, повідомлення надсилається на мобільний телефон користувача через GSM і активується зумер.

Датчик якості повітря встановлюється всередині будинку. Коли рівень забруднення перевищує пороговий рівень, повідомлення надсилається на мобільний телефон користувача через GSM і контролює забруднення.

1.3. Висновки до розділу

У даному розділі одержано наступні результати:

1 Проведено аналіз принципів і технології організації GSM-зв'язку, у результаті якого визначено переваги і недоліки їх застосування у системах на основі мікроконтролерів та IoT-пристроїв. Обгрунтовано доцільність їх застосування при організації систем захист фізичних стаціонарних об'єктів.

2 Проаналізовано особливості проектування та імплементації систем захисту фізичних стаціонарних об'єктів на основі GSM-сигналізацій, що дало змогу визначити їх мінімальну необхідну функціональність та запропонувати шляхи вдосконалення шляхом імплементації у мікроконтролери моделей розпізнавання облич при спрацюванні сенсору руху.

1.

РОЗДІЛ 2

ПРОЕКТУВАННЯ

КОМП'ЮТЕРНОЇ

СИСТЕМИ ЗАХИСТУ

СТАЦІОНАРНИХ

ФІЗИЧНИХ ОБ'ЄКТІВ

З ВИКОРИСТАННЯМ

GSM-СИГНАЛІЗАЦІЇ

2.1. Архітектура комп'ютерної системи захисту стаціонарних фізичних об'єктів

Для захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації пропонується для початку визначити найбільш критичні потреби користувачів.

Перш за все, для забезпечення безпеки стаціонарного об'єкту за відсутності власників, варто аналізувати появу руху у приміщеннях. Не менш критичним є фіксація витоку газу у приміщенні. Окрім цього, важливо у випадку проникнення до об'єкту сторонніх осіб, зафіксувати їх на фото.

Додатковими функціями, які можна імплементувати у системі захисту, є сповіщення про відхилення від норми температури і вологості. Це буде корисно у тому випадку, коли у приміщенні вже використовуються елементи «розумного будинку». Сам GSM-модуль потрібно налаштувати на відправлення сповіщень у вигляді SMS-повідомлень власнику фізичного стаціонарного об'єкту, або довіреним контактам.

Враховуючи вище наведені вимоги до функцій GSM-сигналізації, спроектовано архітектуру комп'ютерної системи на рівні базових компонентів та мікроконтролера управління ESP32.

Тригерами відправки сповіщень за допомогою GSM-модуля виступають пристрої, які контролюють різні аспекти захисту фізичного стаціонарного об'єкту. Центральним компонентом управління захистом приміщень виступає мікроконтролер ESP32. До нього через плату розширення підключаються всі інші пристрої. На рис. 2.1 представлено запропоновану архітектуру комп'ютерної системи.

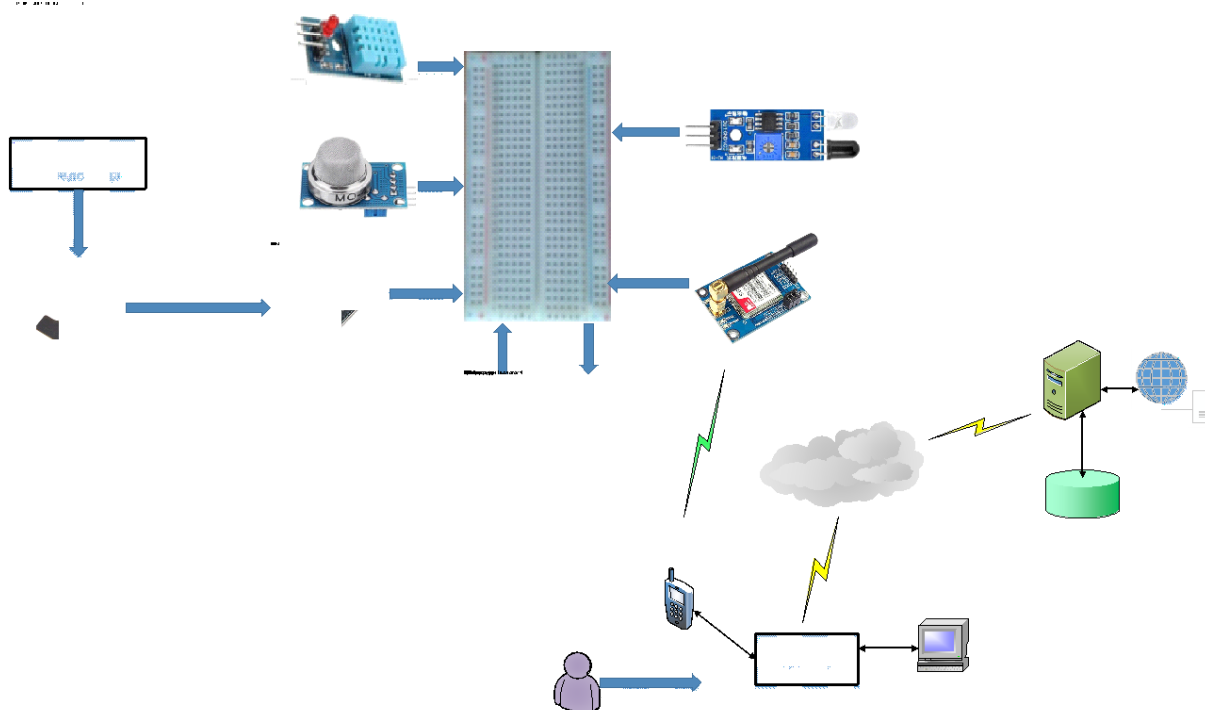


Рис. 2.1. Архітектура системи захисту стаціонарних фізичних об'єктів на основі GSM-сигналізації

Згідно приведеної на рис. 2.1 схеми, основними функціональними модулями і пристроями GSM-сигналізації виступають::

- сенсор температури і вологості – призначений для вимірювання параметрів навколишнього середовища у приміщенні, виступає в якості тригера для відправлення певного типу повідомлення GSM-сигналізацією при відхиленні від налаштувань;
- датчик газу – забезпечує вимірювання концентрації газу у приміщенні і у випадку перевищення встановленої норми виступає тригером спрацювання GSM-сигналізації;

- сенсор руху – призначений для виявлення несанкціонованого руху у приміщенні і виступає тригером для увімкнення камери для захоплення зображення і відправки сповіщення у випадку, коли обличчя особи відсутнє у списку довірених осіб;
- мікроконтролер на базі ESP32-CAM – виконує функції захоплення відео з камери OV2640, запуску сервісу розпізнавання обличчя, зберігання фото на SD-картку і передачу інформації до центрального контролера на базі ESP 32;
- GSM-модуль – призначений для безпосередньої передачі даних в форматі SMS власнику або довіреним особам з налаштовуваного списку про наявність проблем в залежності від типу сенсора, який активує GSM-модуль;
- сервер – зберігає зображення та логи щодо спрацювання GSM-сигналізації;
- смартфон – виступає в якості приймача SMS-повідомлень;
- ПК – забезпечує звернення до бази даних та резервної копії моделі розпізнавання облич.

2.2. Обґрунтування і вибір апаратного забезпечення комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації

2.2.1. Контролер управління пристроями GSM-сигналізації

В якості центрального пристрою керування GSM-сигналізацією запропоновано обрати мікроконтролер ESP 32. Він представляє собою невелику інтегральну схему, яка здатна керувати електронними пристроями чи системами. Даний тип мікроконтролера розроблений таким чином, щоб забезпечувати універсальність застосування та конфігурованість для легкого програмування з використанням ефективного програмного забезпечення та систем.

Мікроконтролер, який відіграє найбільш важливу роль при організації системи безпеки фізичних стаціонарних об'єктів, складається з центрального процесора, який виконує команди програми. До його складу також входять компоненти, які зберігають програмний і виконуваний код програм (оперативна пам'ять) і «пам'ять даних», яка містить дані та змінні, які використовує програма.

На рис. 2.2 показано зовнішній вигляд цього мікроконтролера, а на рис. 2.3 – структуру портів і функціональних елементів.



Рис. 2.2. Зовнішній вигляд ESP32

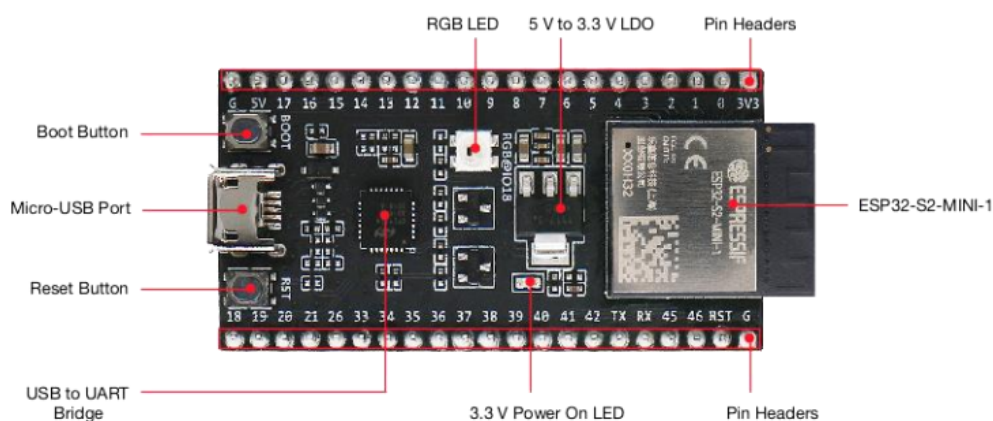


Рис. 2.3. Порти та функціональні компоненти ESP32

Як видно з рис. 2.3, мікроконтролер має можливість отримувати вхідні та вихідні команди з периферійних інтерфейсів для забезпечення зв'язку з іншими зовнішніми пристроями. Для цього можуть

застосовуватися різні комунікаційні інтерфейси, зокрема, UART, SPI та I2C, які дозволяють таку взаємодію.

2.2.2. Функції GSM-модуля у системі забезпечення безпеки фізичних стаціонарних об'єктів

Мікроконтролер ESP32 може взаємодіяти з мобільною мережею завдяки модулю GSM. Він забезпечує стільниковий зв'язок для проектованої інтелектуальної системи безпеки, дозволяючи їй надсилати SMS і здійснювати телефонні дзвінки у разі будь-якого порушення визначених правил безпеки. Ця функція корисна, коли з'єднання з Інтернетом не працює або недоступне.

GSM-модуль діє як мобільний телефон, підключений до системи, яка проектується у кваліфікаційній роботі. Він використовує SIM-карту, яка запрограмована на надсилання SMS-повідомлень на мобільний телефон користувача, коли система безпеки виявляє будь-яку незвичайну активність.

На рис. 2.4 показано зовнішній вигляд використовуваного GSM-модуля, а на рис. 2.5 – призначення його портів.



Рис. 2.4. GSM-модуль системи безпеки фізичного стаціонарного об'єкту

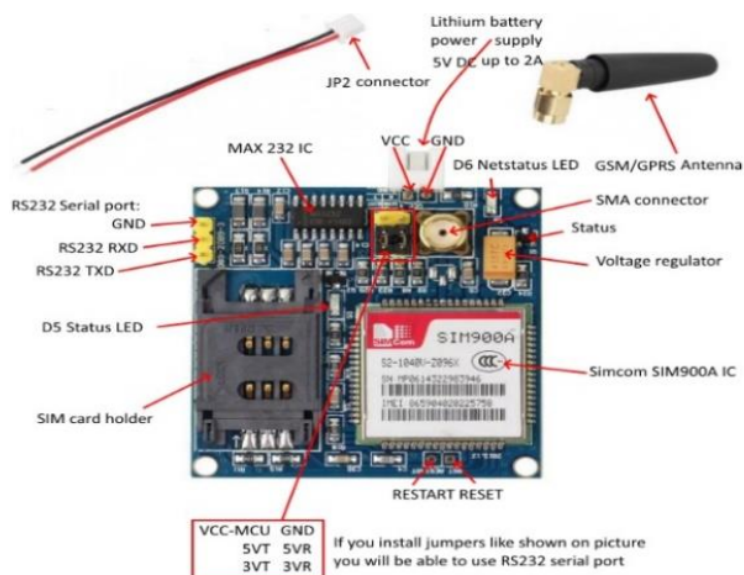


Рис. 2.5. Порти і структура GSM-модуля

SMS-повідомлення надсилаються від відправника у даному випадку ESP32 до одержувача за допомогою технології мережі GSM. Для повного доступу до обладнання та контролю за порушеннями у деякому фізичному стаціонарному об'єктів використовується передача та отримання SMS. Технологія може надсилати споживачам інструкції через SMS з мобільного номера, щоб змінити стан побутової техніки відповідно до визначених вимог і специфікацій.

Здатність системи автоматично генерувати SMS-повідомлення з вмістом відносно сенсора який спрацював, у відповідь на виявлення вторгнення, яке сповіщає користувача про загрозу безпеці, ось як виконується друга частина сповіщення безпеки. Технологія GSM дозволить спілкуватися з усіма, будь-коли та всюди.

2.2.3. Сенсор руху, як тригер активації GSM-сигналізації

Датчик виявлення руху є електронним пристроєм, який здатний оцінювати рівень освітленості, що створюється об'єктами в його полі зору [2]. Сенсор руху (PIR-датчик) може виявляти наявність руху загалом, але не може визначити точний об'єкт, тому їх називають детективними датчиками. Важливість камер у системах безпеки починається власне

відсутності можливості фіксувати за допомогою датчику руху самого об'єкту. Зазвичай, люди думають, що камери просто знімають будь-які об'єкти в їхньому діапазоні одразу після того, як їх бачить об'єктив. Реальність полягає в тому, що датчики руху виявляють, а потім запускають камеру, щоб зафіксувати виявлений об'єкт.

PIR-датчики використовуються для виявлення присутності зломисників або потенційних загроз у певній зоні. Вони є важливим компонентом систем безпеки, оскільки забезпечують безконтактний засіб виявлення руху або зміни температури.

PIR-датчики працюють, випромінюючи інфрачервоне випромінювання та аналізуючи випромінювання, яке відбивається від об'єктів у полі їхнього зору [2].

Кількість відбитого випромінювання можна використовувати для розрахунку як температури об'єкта, так і кількості простору, що відокремлює PIR-датчик від об'єкта. Наприклад, система безпеки може використовувати сенсор руху для виявлення присутності зломисника, а потім активувати камеру для зйомки відеозапису зломисника.

PIR-датчики також можна використовувати для моніторингу змін температури в певній зоні, що може бути корисним для виявлення пожеж або інших потенційних небезпек. Наприклад, у системі безпеки розумного будинку інфрачервоні давачі можуть використовуватися для виявлення раптового підвищення температури в кімнаті, що вказує на пожежу чи іншу надзвичайну ситуацію. На рис. 2.6 наведено типовий інфрачервоний сенсор для виявлення руху.

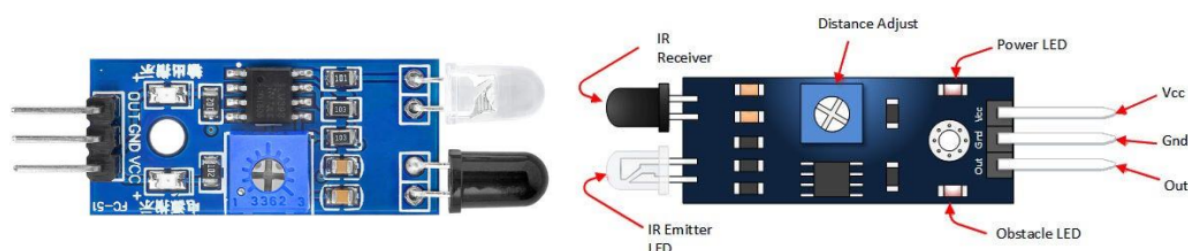


Рис. 2.6. Типовий інфрачервоний сенсор руху

Пасивний інфрачервоний датчик, який показано на рис. 2.6, містить два чутливі елементи для випромінювання та отримання відбитих променів. Датчик PIR325 складається з двох сенсорних компонентів, які об'єднані в конфігурацію компенсації напруги. Ця конфігурація ігнорує сигнали, які надходять від сонячного світла, при зміні температури чи вібрації.

У випадку наявності рухомого об'єкту у радіусі дії датчика спрацюватиме один елемент раніше за інший, тоді як додаткові фактори впливатимуть на обидва елементи одночасно та нейтралізуватимуть один одного. Як правило, інструмент фокусування розміщується перед датчиком. На рис. 2.7 показано принцип функціонування сенсора руху.

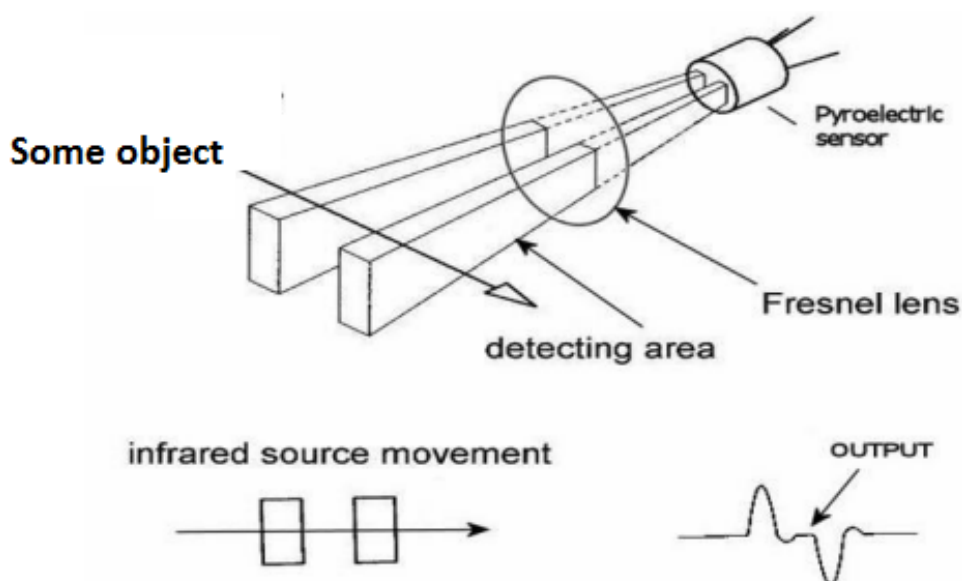


Рис. 2.7. Принцип функціонування сенсора руху

Інфрачервоний датчик направляє свій промінь в широку зону спостереження, і відразу після того, як об'єкт потрапляє в діапазон, сенсор надсилає сигнал камері для зйомки протягом декількох секунд або отримання фото з відповідного сектора.

2.2.4. Сенсор газу як засіб сповіщувач небезпечної ситуації

Датчик газу – це інструмент, який може визначати локалізацію кількох видів газів і видавати попередження або сигнал, коли концентрація газу перевищує встановлений поріг. Щоб захистити людей і майно від витоку газу та інших можливих небезпек, газові датчики дуже важливі, коли мова йде про системи безпеки та автоматику. Залежно від типу та використовуваної технології, характеристики газового датчика можуть відрізнятися. Однак для більшості з них характерні критерії якості, що наведені нижче.

Критерій чутливості датчика газу впливає на те, наскільки ефективно він може виявити його. Датчик має бути унікальним для того типу газу, який він призначений виявляти, і достатньо чутливим, щоб вловлювати навіть дуже низькі його концентрації. Час, який потрібен сенсору для виявлення газу та створення вихідного сигналу є часом відгуку. У таких важливих застосуваннях, як виявлення витоку газу, де миттєва реакція допомагає уникнути шкоди чи попередити небезпеку, короткий час реакції має вирішальне значення.

Точність, як характеристика датчика газу, залежить від того, наскільки коректно він вимірювати концентрацію газу. Вимірювання концентрації газу є точним і надійним завдяки матеріалам з яких він виконаний. Датчик газу вважається стабільним, якщо він може залишатися точним і чутливим з часом. Навіть після багаторазового використання стабільний датчик може забезпечити точні вимірювання.

Селективність датчика газу означає його здатність ідентифікувати газ, не враховуючи інші гази, які можуть бути присутніми в навколишньому повітрі. Вибірковість є ключовим компонентом газових датчиків, які використовуються для відстеження небезпечних речовин. Залежно від потреб і архітектури охоронної системи існує кілька способів підключення датчика газу.

За допомогою дротового або бездротового інтерфейсу сенсор газу, зазвичай, підключається до системи безпеки. Бездротове з'єднання дозволяє йому взаємодіяти з системою безпеки без проводів через радіохвилі на відміну від дротового, яке фізично з'єднує датчик із системою безпеки за допомогою кабелів.

Якщо концентрація газу перевищує порогове значення або є витік, датчик газу надає звіт до бази даних, який буде відображатися в мобільному додатку. Нарешті користувачеві надсилається SMS-повідомлення у формі URL-адреси, щоб домовласник міг вжити необхідних заходів, щоб обмежити будь-яку шкоду чи небезпеку.

На рис. 2.8 показано типовий сенсор газу.

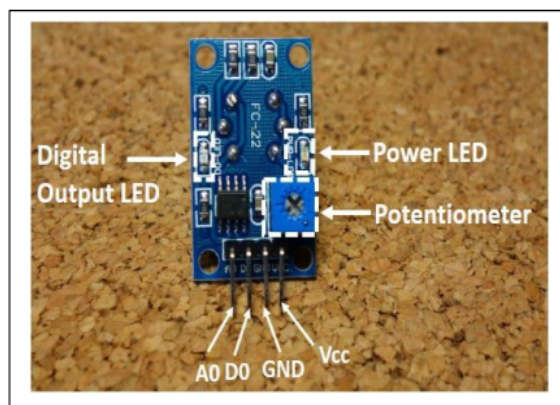


Рис. 2.8. Типовий сенсор газу

Датчик газу містить такі компоненти і виводи: GND, VCC, DO, AO, світлодіод (живлення), потенціометр і світлодіод цифрового виходу. Такий тип сенсора виявляє та сповіщає розумну систему безпеки про наявність газів у навколишньому середовищі.

Опорною напругою у схемі датчика газу є «земля» (GND). Це дає кожному компоненту в схемі єдине заземлення. Напруга живлення позначається як VCC. Датчик газу та інші компоненти ланцюга живляться від цієї напруги номіналом 5 В постійного струму.

D0 є цифровим вихідним контактом датчика газу. Він передає цифровий сигнал, який показує наявність або відсутність газу певного рівня. Вивід D0 видає потужний сигнал, коли виявлено газ, який можна використати для подання сигналу тривоги або ввімкнення світлодіода.

Аналоговий вивід сенсора газу позначається як A0. Він пропускає аналоговий сигнал напруги, обернено пропорційний концентрації рівня газу. Мікроконтролер або інший пристрій може зчитувати аналоговий вихід, щоб визначити концентрацію газу.

Індикатор живлення служить індикатором стану працездатності датчика газу. Він призначений для відображення сигналу про те, що датчик увімкнено та готовий до роботи.

Чутливість датчика газу можна змінити, відрегулювавши потенціометр, який є змінним резистором. Пороговий рівень для виявлення газу можна змінити відповідно до застосування шляхом встановлення потенціометра.

Світлодіод цифрового виходу забезпечує сповіщення блиманням, коли виявлено перевищення порогового рівня концентрації газу.

Датчик газу підключається до мікроконтролера або іншого пристрою в інтелектуальній системі безпеки, щоб він міг зчитувати цифровий або аналоговий вихід і запускати тривогу або виконувати інші операції, наприклад надсилати сповіщення на смартфон або вмикати автоматичну вентиляцію.

Поріг виявлення газу можна встановити за допомогою потенціометра, а світлодіод живлення та світлодіод цифрового виходу показують, чи функціонує датчик газу візуально. Горючі гази, включаючи пропан, бутан і метан, можуть бути знайдені за допомогою каталітичних газових датчиків.

Датчики газу можуть функціонувати як самостійні одиниці або як компонент більшої системи безпеки. У той час як ці, інтегровані в систему безпеки, сенсори подадуть звуковий сигнал, коли концентрація газу

перевищить встановлений поріг, автономні датчики газу, зазвичай, мають цифровий дисплей, який показує рівні концентрації газу та сигнали тривоги. Підсумовуючи, газові датчики є ключовими частинами систем безпеки, оскільки вони забезпечують надійний і точний метод ідентифікації потенційно небезпечних газів у навколишньому середовищі. Сенсори виявлення газів можуть бути інтегровані в системи безпеки, щоб сповіщати власників будинків і співробітників служби безпеки про витік газу, дозволяючи їм вживати негайних заходів, щоб зупинити будь-яку шкоду.

2.2.5. Сенсор вимірювання температури і вологості у системі GSM-сигналізації

У системах безпеки, серед іншого, використовуються датчики температури та вологості типу DHT11. Такий тип сенсора необхідний для забезпечення здатності визначення можливих небезпек, включаючи пожежу або пошкодження водопроводу. Такий функціонал реалізується шляхом відстеження коливань температури та вологості та ввімкненням сигналів тривоги або сповіщень, коли перевищуються задані порогові значення. На рис. 2.9 показано сенсор температури і вологості DHT 11.



Рис. 2.9. Сенсор визначення температури і вологості DHT 11

Датчики DHT 11 програмується на виявлення пожеж у системі виявлення вторгнень. Технологія може оцінити, чи існує ризик пожежі, і вжити заходів для його запобігання, стежачи за температурою в певній зоні. Такий сенсор, наприклад, можна розташувати у кухонних приміщеннях, біля електричних панелей або інших потенційних джерел пожежі в бізнес-структурі. Окрім цього, у будівлях сенсор DHT11 можна розмістити в місцях, потенційного витоку води, наприклад, поблизу труб або підвалів. Якщо вологість підвищується вище певного порогу, система активує сигналізацію та сповістить персонал чи власника будинку.

Дані із усіх сенсорів можна зберігати у базі даних, і у випадку перевищення допустимих показників, виконується негайне оповіщення через SMS-інформування або через мобільний додаток.

2.2.6. Модуль ESP32-CAM та камера OV2640, як апаратна складова інтелектуального розпізнавання облич

З метою організації функції інтелектуального розпізнавання облич у випадку спрацювання сенсора руху у системі захисту фізичних стаціонарних об'єктів GSM-сигналізації запропоновано використання однорідного мікроконтролера ESP32-CAM. Даний контролер реалізований у вигляді модуля в основі якого лежить схема ESP32-S, яка підтримує камеру. Крім порту для підключення нативної камери OV2640 і кількох цифрових виводів цей мікроконтролер підтримує пристрій зберігання даних у вигляді microSD-карти. Це дає змогу зберігати зображення, одержані з камери, з подальшим надсиланням через GSM-модуль або безпроводний маршрутизатор текстового повідомлення про несанкціонований доступ у стаціонарний об'єкт. Структурно ESP32-CAM представлено на рис. 2.10.

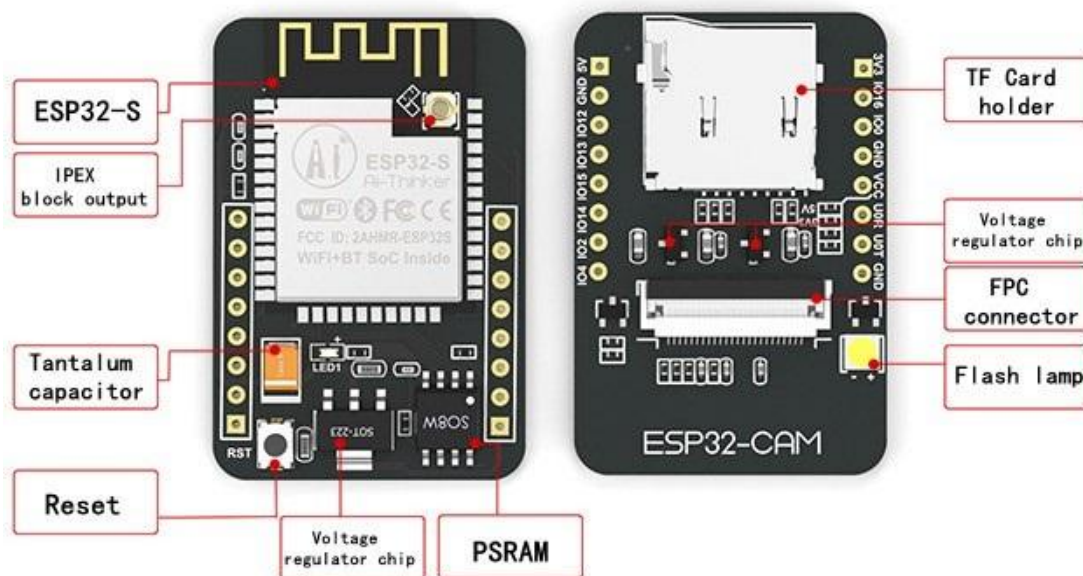


Рис. 2.10. Модуль ESP32-CAM

Технічні характеристики мікроконтролера на базі ESP32-CAM наведено у табл. 2.1.

Таблиця 2.1

Технічні характеристики ESP32-CAM

№ з/п	Технічна характеристика	Опис
1.	Модуль безпроводного доступу	ESP32-S WiFi 802.11 b/g/n + Bluetooth
2.	Зовнішнє сховище	Слот з підтримкою карт micro- SD з об'ємом до 4 ГБ
3.	Підтримка камер	OV2640 або OV7670
4.	Формат зображення	JPEG (тільки OV2640) BMP Відтінки сірого
5.	Наявність спалаху	Світлодіодний спалах
6.	Контакти	16 з інтерфейсами: – UART, – SPI, – I2C, – PWM
7.	Напруга живлення	5 В
8.	Споживана потужність	Спалах вимкнений - 180 мА Спалах увімкнений – 310 мА Глибокий сон - 6 мА Неглибокий сон - 6,7 мА

9.	Габаритні розміри	40,5 x 27 x 4,5 мм
10.	Температурний діапазон	робочий: 20 – 85 °С зберігання: -40 - 90 °С при 90% відносної вологості

Призначення виводів та їх розташування на платі даного мікроконтролера зображено на рис. 2.11.



Рис. 2.11. Виводи ESP32-CAM

Аналізуючи рис. 2.11 можна побачити, що живлення контролера може забезпечуватися напругою номіналом 3,3 В або 5В, а також наявні 3 виводи для «землі». Цифрові виводи GPIO 1 та GPIO 3 застосовуються при завантаженні програм у контролер. Варто відмітити, що ці інтерфейси є послідовними.

Для того, щоб контролювати можливість спалаху при підключенні камери використовується нульовий цифровий вивід. У випадку, коли даний вивід підключається до виводу «земля», то ESP32-CAM забезпечує режим увімкнення спалаху. Всі інші контакти використовуються при підключенні до схеми зчитування даних з microSD. Призначення виводів для зчитування даних представлені у табл. 2.2.:

Таблиця 2.2

Підключення виводів до microSD

Номер виводу	Призначення
GPIO 14	CLK
GPIO 15	CMD
GPIO 2	Дані 0
GPIO 4	Дані 1 (підключені до світлодіода)
GPIO 12	Дані 2
GPIO 13	Дані 3

Схема підключення виводів ESP32-CAM до камери та microSD-накопичувача проілюстрована у табл. 2.3.

Таблиця 2.3

Схема підключення ESP32-CAM до камери та накопичувача

Камера	ESP32	SD-картка	ESP32
D0	PIN 5	CLK	PIN 14
D1	PIN 18	CMD	PIN 15
D2	PIN 19	DATA0	PIN 2
D3	PIN 21	DATA1/flash	PIN 4
D4	PIN 36	DATA2	PIN 12
D5	PIN 39	DATA3	PIN 13
D6	PIN 34		
D7	PIN 35		
XCLK	PIN 0		
PCLK	PIN 22		
VSYNC	PIN 25		
HREF	PIN 23		
SDA	PIN 26		
SCL	PIN 27		
POWER PIN	PIN 32		

Таким чином, застосування мікроконтролера на базі ESP32-CAM дає можливість на апаратному рівні забезпечити можливість реалізації функції

роботи з камерою і зберігання зображень з неї. Тригером активації камери є сигнал переданий з ESP-32 до ESP32-CAM при спрацюванні сенсора руху.

При виборі камери для фіксації порушення простору необхідно звернути особливу увагу на якість зображення, оскільки від цього залежатиме точність їхнього розпізнавання.

Типовим пристроєм захоплення відео, що постачається у комплекті з ESP32-CAM, є камера OV2640. Даний пристрій дає змогу отримувати відео та зображення, роздільна здатність яких відповідає 2 Мп.

Основними характеристиками камери OV2640 є параметри, що представлені у табл. 2.4.

Таблиця 2.4

Технічні характеристики OV2640

№	Характеристика	Опис
1.	Роздільна здатність	UXGA 1600*1200
2.	Напруга живлення	Основне живлення – 1,3 VDC±5% Аналогове – 2,5-3,0VDC Входу/виходу – 1,7-3,3 V
3.	Споживана потужність у режимі використання	125мВт , 15 fps, UXGA YUV режим 140мВт – для 15 fps, UXGA режим компресії
4.	Споживана потужність (stand by)	600 μA
5.	Основний температурний режим	0-50 C ⁰
6.	Вихідні формати (8-біт)	YUV (422/420)/YCbCr422 RGB565/555 8-бітні стиснуті дані 8/10-бітні Raw RGB дані
7.	Розмір лінзи	1/4"
8.	Основний кут	25 ⁰

9.	Максимальна швидкість передачі зображення	UXGA/ sXGA – 15fps SVGA – 30 fps CIF – 60 fps
10.	Чутливість	0,6 В/Лк-с
11.	Співвідношення сигнал/шум	40дБ
12.	Режим сканування	Прогресивний
13.	Максимальний режим експозиції	1247*trouw
14.	Гамма корекція	Програмована
15.	Розмір пікселів	2,2μм*2,2μм
16.	Фіксований шум	<1%
17.	Площа зображення	3590 μм*2684 μм

Призначення і розташування виводів обраної камери показано на рис. 2.12, а її функціональну схему наведено на рис. 2.13.



Рис. 2.12. Виводи камери OV2640

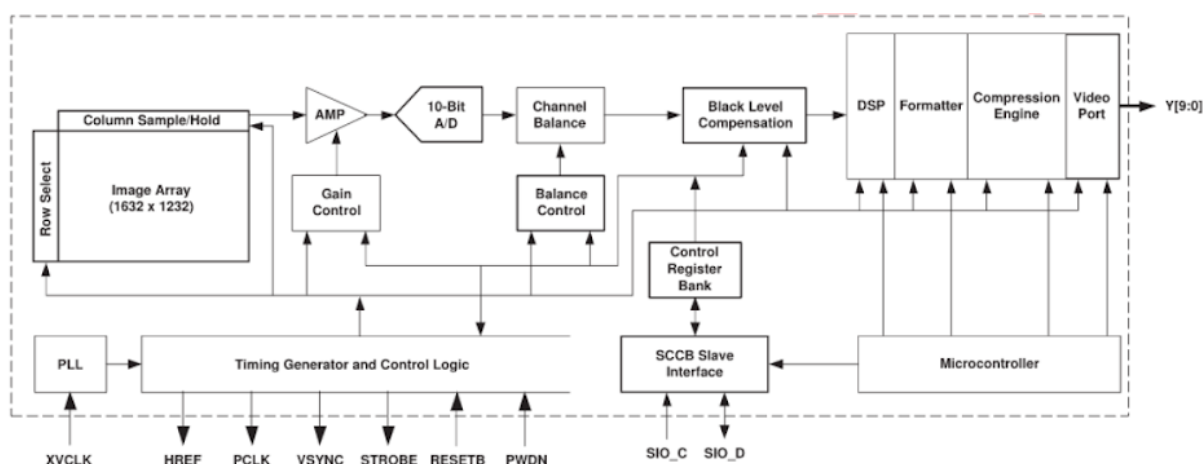


Рис.2.13. Функціональна схема камери OV2640

Відеокамера, функціональну схему якої показано на рис. 2.13, містить у собі мікроконтролер з восьми розрядами та пам'яттю даних розміром 512 Б і пам'яттю для програм 4 КБ. Це дозволяє забезпечити ефективність процесу при декодуванні команд і керування системою.

2.3. Проектування схем з'єднання та інсталяція компонентів системи GSM-сигналізації

Налаштування апаратного забезпечення передбачає підключення плати розробки ESP32, ESP32-CAM, камерb, датчика руху, модуля GSM і макетної плати за допомогою серії кабелів.

Макетна плата стає джерелом енергії для всіх пристроїв. При живленні цієї плати забезпечується також енергією будь-яке, підключене до неї обладнання. Схему з'єднання усіх компонентів системи захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації показано на рис. 2.14.

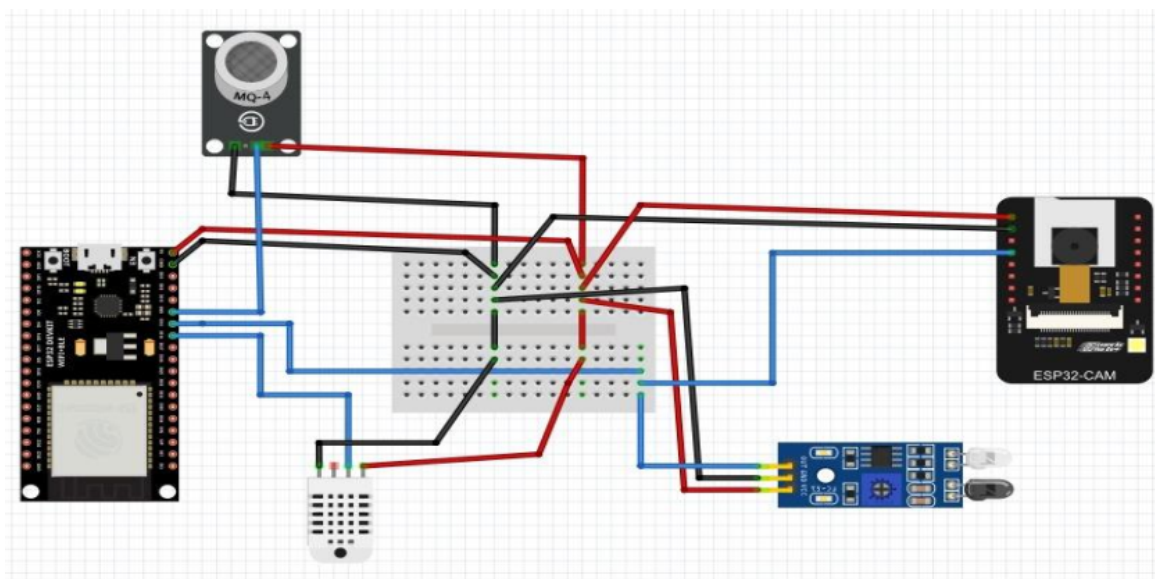


Рис. 2.14. Принципова схема з'єднання елементів системи
GSM-сигналізації

Після того, як принципова схема схеми складена і всі пристрої правильно підключені, починається основна реалізація. Нижче наведено зображення основної схеми, зазначеної на рис. 2.14.

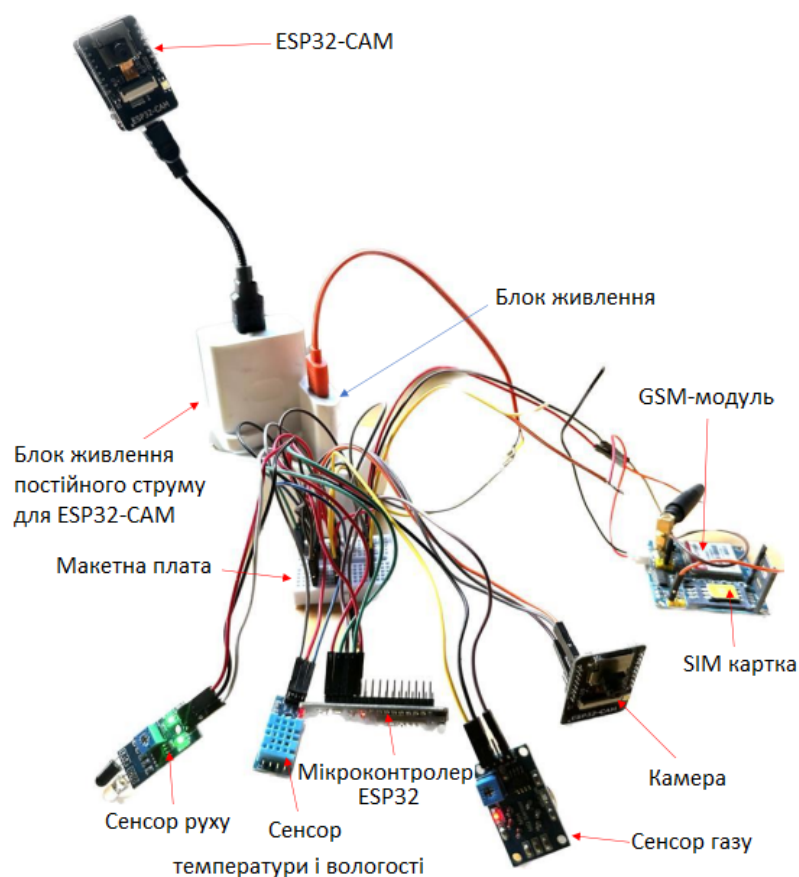


Рис. 2.15. Схема підключення компонентів системи

Для апаратної реалізації підсистеми виявлення та розпізнавання облич у системі захисту стаціонарних об'єктів на основі GSM-сигналізації запропонована і розроблена схема, яка показана на рис. 2.16.

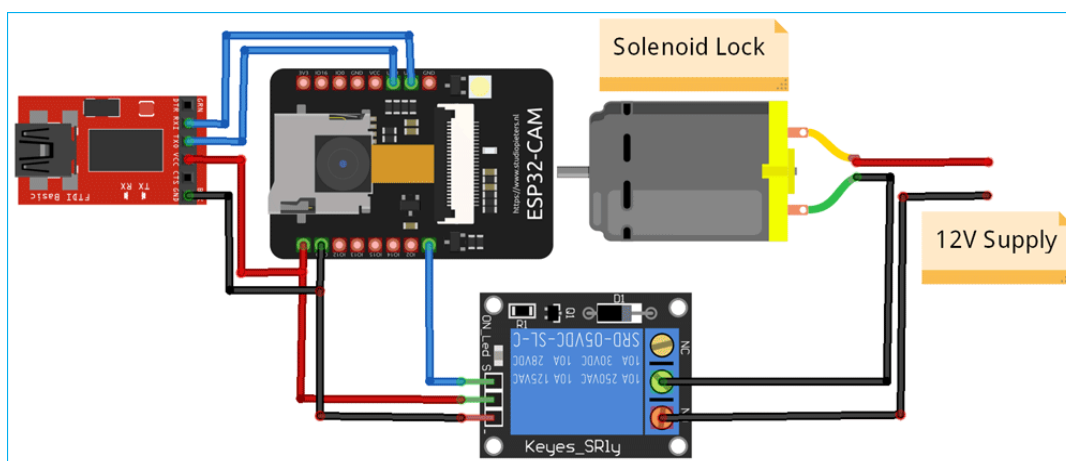


Рис. 2.16. Схема підключення компонентів при організації підсистеми для роботи з камерою

Як видно з рис. 2.16, виконується підключення контролера ESP32-CAM до:

- плати FTDI;
- модуля реле;
- електромагнітного замка (додатково).

Доцільність застосування плати FTDI обумовлена необхідністю запису програми у ESP32-CAM. Це пов'язано з відсутністю у даного мікроконтролера USB-інтерфейсу. Для тестування і, можливо у подальшому, імплементції додаткової функції блокування замків у стаціонарному фізичному об'єкті застосовується модуль реле, що виконує функції увімкнення/вимкнення електромагнітного замка. Схема підключення програматора FTDI до ESP32-CAM показана у табл. 2.5, а підключення реле – у табл. 2.6.

Таблиця 2.5

Схема з'єднання програматора FTDI та ESP32-CAM

ESP32-CAM	FTDI Board
5V	VCC
GND	GND
UOR	TX
UOT	RX

Таблиця 2.9

Схема з'єднання реле та ESP32-CAM

ESP32-CAM	Relay Module
5V	VCC
GND	GND
IO4	IN

ESP32-CAM з підключенням сенсорів газу, температури і вологості, датчика руху і сумісної камери з роздільною здатністю 2Мп, що дало можливість підвищити функціональність системи за рахунок інтеграції програмної моделі інтелектуального розпізнавання облич, яка активується при спрацюванні тригера у вигляді сигналу від сенсора руху з подальшою передачею сповіщення за допомогою GSM-модуля власнику об'єкта.

2. Проаналізовано та обгрунтовано застосування компонентної бази для практичної реалізації системи захисту фізичних стаціонарних об'єктів, що дало можливість забезпечити надійність та визначену функціональність роботи GSM-сигналізації.

3. Спроековано схеми підключення компонентів системи захисту фізичних стаціонарних об'єктів, що дало змогу забезпечити комунікацію всередині системи та оптимально налаштувати взаємодію між пристроями, а отже і забезпечити ефективне функціонування GSM-сигналізації.

4.

РОЗДІЛ 3
ІМПЛЕМЕНТАЦІЯ
ПРОГРАМНОЇ
МОДЕЛІ
РОЗПІЗНАВАННЯ
ОБРАЗІВ ТА
СИСТЕМНОГО
ПРОГРАМНОГО
ЗАБЕЗПЕЧЕННЯ
GSM-СИГНАЛІЗАЦІЇ

3.1. Нейронна мережа для ідентифікації зображення з камери системи GSM-сигналізації

Реалізацію функції відеозахоплення, фіксації та захоплення обличчя людини у комп'ютерній системі захисту стаціонарних фізичних об'єктів з використанням GSM-сигналізації запропоновано виконати із застосуванням методу штучного інтелекту, зокрема, згорткових нейронних мереж.

Основне застосування згорткових нейромереж пов'язано із розв'язком задач комп'ютерного зору, де вони показали високу ефективність. До таких задач належить класифікація і пошук зображень, а також виявлення ознак досліджуваних об'єктів. Глибокі нейронні мережі на основі операції згортки зменшують розміри візуального об'єкту на вході, але збільшують їх у прихованих та вихідному шарі, що дає змогу отримувати ознаки зображення у просторі меншого розміру. У зв'язку з тим, що існує розподіл вагових коефіцієнтів, тобто кількість нейронів і відповідних параметрів зменшується, згорткові нейромережі швидше і легше піддаються навчанню.

В якості прикладу можна розглянути примітивну згорткову нейронну мережу у двовимірному просторі. У цьому випадку операцію згортки представляють у вигляді деякого вікна з певними розмірами та випадково заданими ваговими коефіцієнтами, що пересувається по зображенню. При цьому виконується поелементне множення над даними, які потрапили у даний момент у площу вікна і лише після цієї операції виконується додавання усіх отриманих значень в єдиний піксель, що є виходом вікна. Вікно, або по-іншому ядро, рухається по зображенню і формує перетворення матриці вхідних ознак в іншу матрицю нових властивостей.

Усі вихідні ознаки в процесі ковзання ядра можна представити як зважену суму ознак входу. Розміщення характеристик зображення знаходиться доволі близько до тієї локації, у якій розміщений останній піксель вхідного шару.

Слід відмітити, що входження вхідної характеристики абсолютно не залежить від локації пікселя, оскільки він залежить від розташування у межах вікна. В якості прикладу приведемо випадок, коли вхідний набір ознак має розмір 5×5 , тобто існує 25 пікселів, а на виході потрібно отримати набір, який містить 9 ознак, тобто 3×3 пікселі. При цьому кожен повнозв'язний шар нейронної мережі буде містити матрицю 25×9 , компонентами якої є вагові коефіцієнти параметрів, а кожна ознака на виході буде представлятися як зважена сума наявних ознак у вхідному шарі. Операція згортки застосовується по 9-ти параметрах. На рис. 3.1 наведено структуру нейронної мережі, яка забезпечує класифікацію зображення.

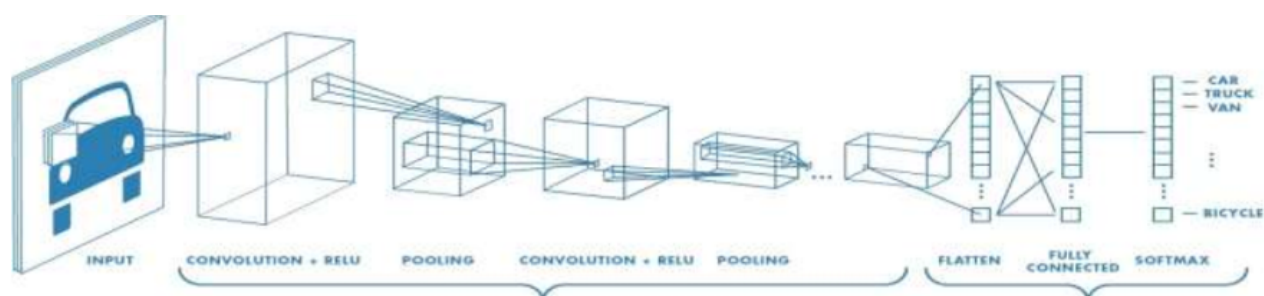


Рис. 3.1. Приклад структури згорткової нейронної мережі в режимі класифікатора

Коли вікно рухається по зображенню, по-іншому – по карті ознак, крайні пікселі зображення не враховуються і відбувається перехід від матриці ознак з розміром 5×5 до матриці з меншою кількістю ознак – 3×3 . Візуальне представлення операції згортки проілюстровано на рис. 3.2.

Варто зауважити, що при такому підході пікселі, які знаходяться на краю зображень ніколи не будуть потрапляти у центр вікна, а це знижує інформативність, оскільки розмір ознак вихідного шару повинен бути ідентичним до розміру ознак вхідного зображення.

Для ефективного застосування підходу згорткових нейронних мереж можна використовувати два підходи:

- Padding – підхід, що передбачає додавання до карти ознак додаткових пікселів, тим самим забезпечуючи рух вікна з врахуванням крайніх пікселів зображення;
- Striding – передбачає встановлення деякого інкременту, що виконує зміщення вікна пропускаючи при цьому деякі пікселі.

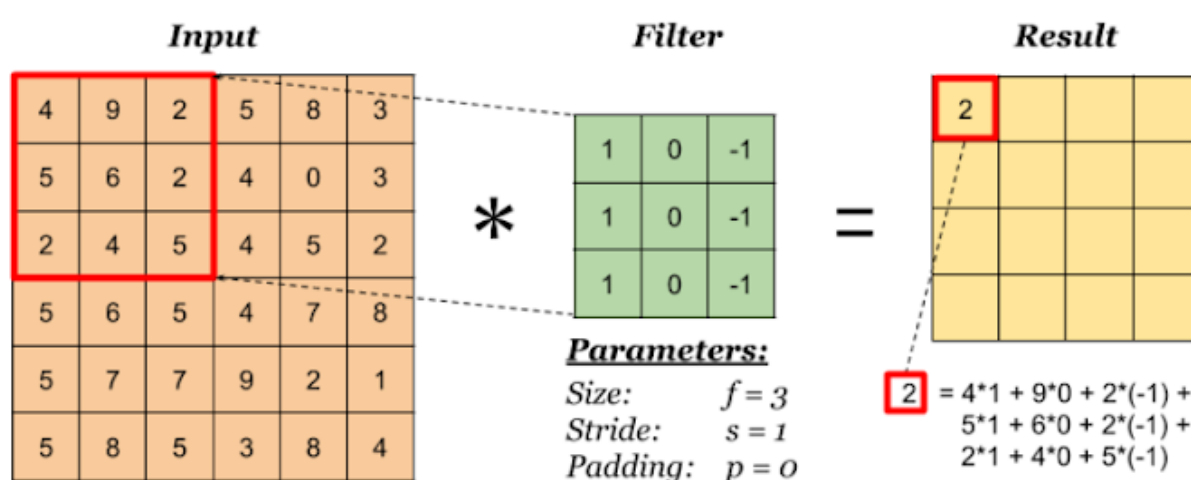


Рис. 3.2. Операція згортки

Застосування технології Padding передбачає створення фейкових пікселів і дає змогу оригінальним пікселям бути проаналізованим ядром, що рухається по зображенню.

Доволі частим завданням при застосуванні згорткових шарів є зниження розмірності вихідних даних у порівнянні з вхідними, тобто виникає необхідність стиснення зображення. Це передбачає зменшення кількості просторових розмірів з одночасним зростанням числа каналів. Для розв'язання такої задачі можна скористатися додаванням шарів pooling. Одним з варіантів є використання середнього або максимального значення кожної ділянки площею 2×2 для зменшення усіх просторових розмірів удвічі. На рис. 3.3 наведено приклад застосування різних видів pooling, зокрема, функцій мінімізації, максимізації та середнього значення.

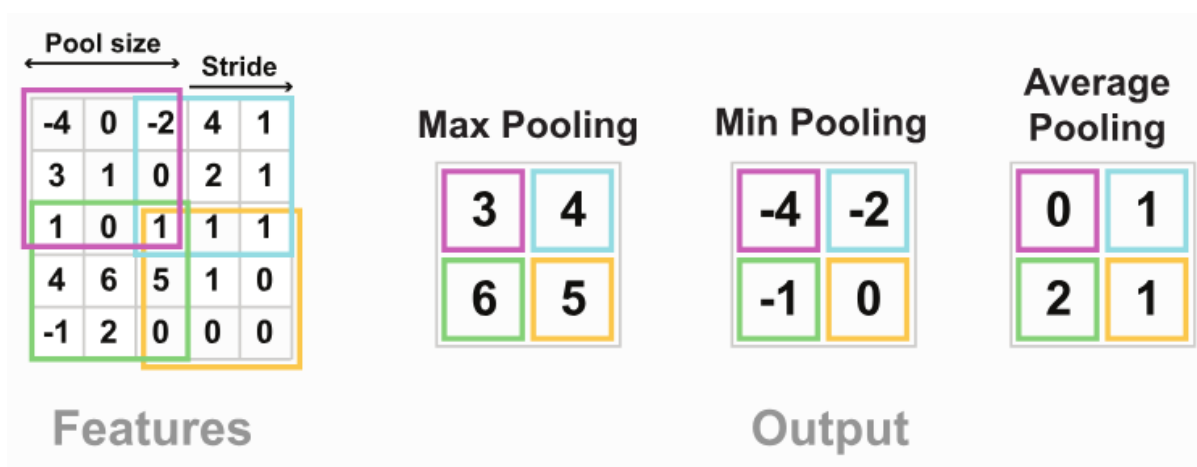


Рис. 3.3. Типи pooling-шару

Альтернативним варіантом для стиснення зображення є використання stride, основна ідея якого реалізується шляхом пропуску деяких областей при переміщенні ядра по зображенню.

Якщо задати значення stride рівним одиниці, то у вікно будуть потрапляти пікселі через один. У випадку, коли значення буде рівним 2, то ядро буде формуватися з пропуском двох пікселів. Сьогодні сучасні

нейромережі інтенсивно використовують архітектуру ResNet, тим самим відмовляючись від pooling-шарів.

Уявімо собі ситуацію, коли на вхід згорткового шару надходить графічний об'єкт з розміром 4×4 , і поставлена задача забезпечити його перетворення у мапу ознак з удвічі меншим розміром.

Якщо для цього застосовувати нейронну мережу прямого поширення, то необхідно виконати перетворення вхідної матриці 4×4 у вектор в шістнадцяти вимірному просторі. Далі його потрібно подати на повно зв'язний шар. Кількість входів якого становить 16, а виходів – 4. Формально, матриця, що описує синаптичні ваги представляється як:

$$\begin{bmatrix} w_{1,1} & \dots & w_{1,16} & \dots & \dots & \dots & w_{4,16} & \dots & \dots & w_{4,16} \end{bmatrix}, \quad (3.1)$$

$w_{i,j}$ – інтерпретують вагові коефіцієнти пікселів, які отримуються у результаті множення матриць інтенсивності пікселів і ядра, $i = 1..4, j = 1..16$.

Будь-які операції згортки над ядрами представляють собою лінійні перетворення над відповідною матрицею переходу. Для прикладу, при застосуванні деякого вікна K шириною і висотою у три пікселі та вході розміром 4×4 одержати вихід розміром 2×2 можливе при використанні матриці наступного вигляду:

$$\begin{bmatrix} k_{1,1} & k_{1,2} & k_{1,3} & 0 & k_{2,1} & k_{2,2} & k_{2,3} & 0 & k_{3,1} & k_{3,2} & k_{3,3} & 0 & 0 & 0 & 0 & 0 \\ 0 & k_{1,1} & k_{1,2} & k_{1,3} & 0 & k_{2,1} & k_{2,2} & k_{2,3} & 0 & k_{3,1} & k_{3,2} & k_{3,3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & k_{1,1} & k_{1,2} & k_{1,3} & 0 & k_{2,1} & k_{2,2} & k_{2,3} & 0 & k_{3,1} & k_{3,2} & k_{3,3} & 0 \\ 0 & 0 & 0 & 0 & 0 & k_{1,1} & k_{1,2} & k_{1,3} & 0 & k_{2,1} & k_{2,2} & k_{2,3} & 0 & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} \quad (3.2)$$

У матриці еквівалентностей розміром 4×16 , яка сформована з 64 елементів даних, визначальними є тільки дев'ять параметрів. Ці параметри застосовуються по кілька разів. Для кожного вихідного вузла визначена лише наперед встановлена кількість входів. При цьому відсутня будь-яка взаємодія з іншими входами, оскільки вагові коефіцієнти дорівнюють нулю.

У випадку, коли передбачено застосування попередньо навченої моделі для розв'язку задач класифікації графічних об'єктів, то доцільно встановити параметри нейронної мережі як пріоритетні. Це означає, що буде відбуватися добування образів в останньому повнозв'язному шарі. Для загального випадку, архітектура нейронної мережі з операцією згортки представлена на рис. 3.4.

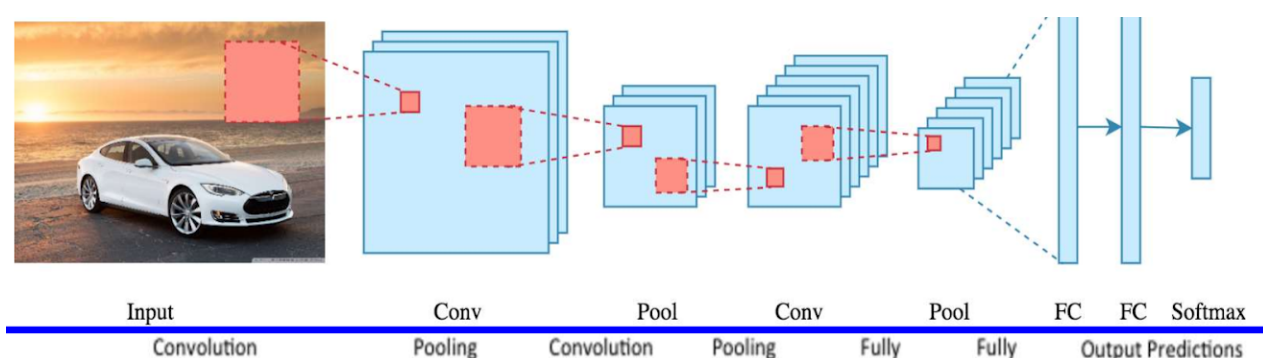


Рис. 3.4. Типова структура нейронної мережі за шарами

На рис. 3.4 показано, що зображення у початковому своєму вигляді поступає на вхід згорткового шару. Якщо зображення кольорове, то його пікселі генерують 3 мапи ознак у цьому шарі. Ці ознаки інтерпретуються як інтенсивність червоного, зеленого та синього кольорів.

Наступним після згорткового іде pooling-шар, який забезпечує визначення важливих ознак на зображенні та зниження розмірності мапи ознак. Створення даного шару може використовувати предикати максимізації або використовувати середнє значення інтенсивності пікселів у фільтрі.

Наступний етап передбачає повторення процедури у відповідності до архітектури згорткової нейронної мережі. Типовою архітектурою згорткової нейромережі, окрім розглянутих раніше шарів, передбачено шар Flatten. Основна функція цього шару полягає у трансформації матриці ознак у вектор. Принцип за яким функціонує шар Flatten проілюстровано на рис. 3.5.

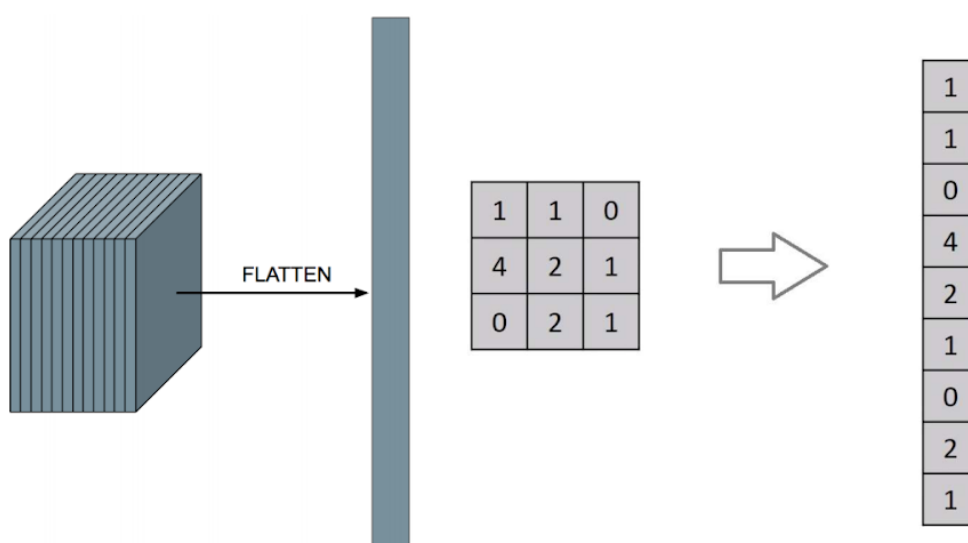


Рис. 3.5. Шар Flatten

Часткове добування ознак із зображення реалізується на етапах починаючи від вхідного шару і завершуючи шаром Flatten. Результати роботи такої послідовності організації шарів у подальшому можна передавати на MLP чи іншу реалізацію класифікатора чи регресора. Структурно та операційно один шар згортки наведено на рис. 3.6.

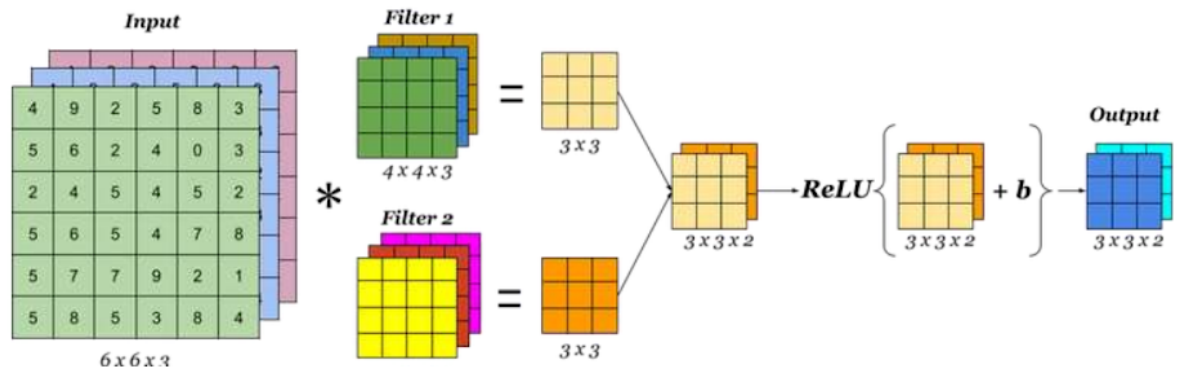


Рис. 3.6. Структура згорткового шару нейронної мережі

Послідовність опрацювання графічного об'єкту згортковою нейронною мережею з відповідними результатами після кожного з шарів проілюстровано на рис. 3.7.

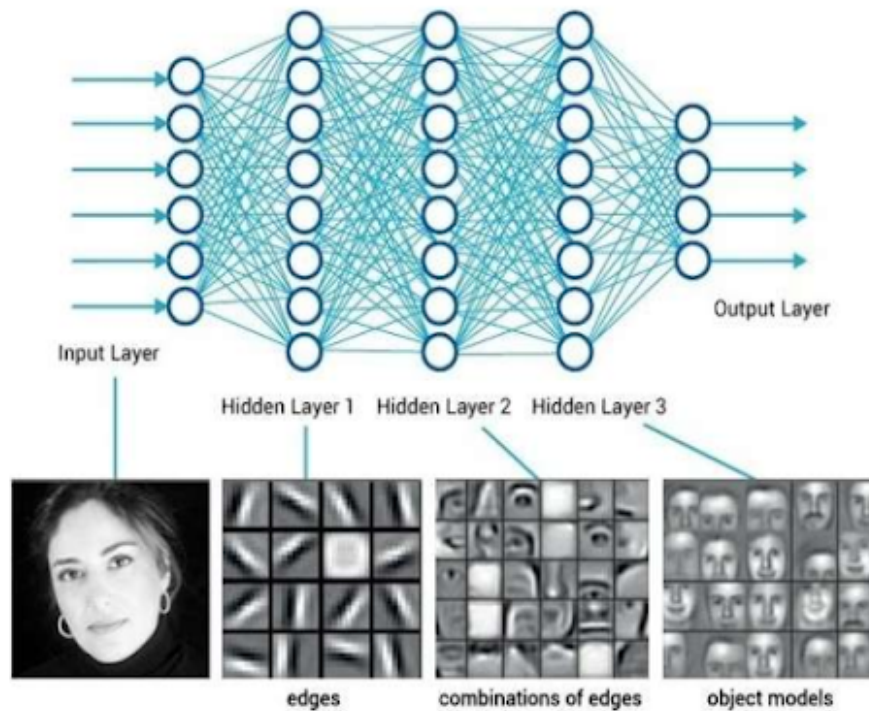


Рис. 3.7. Результати опрацювання зображення шарами згорткової нейронної мережі

Варто відмітити той факт, що процедура створення вхідних даних для мереж і реалізація алгоритмів навчання нейронних мереж на основі операції згортки передбачає значні часові і фінансові витрати.

Оптимізацію цих процесів можна забезпечити шляхом використання уже існуючих архітектур, які показали хороші результати при розпізнаванні зображень. Зазвичай, існуючі архітектури наявні у вільному доступі від таких ІТ-компаній, як Google, Microsoft, OpenAI, IBM та інші. Підхід використання готових архітектур нейромереж або їх компонентів для розв'язання задач окремого конкретного домену називають Transfer Learning. В основному він передбачає передачу вже набутих знань новому об'єкту (рис. 3.8).



Рис. 3.8. Принцип Transfer Learning

Ідея, концепція якої наведена на рис. 3.8, передбачає повторне використання існуючої архітектури попередньо навченої нейромережі. Саму суть передачі знань у порівнянні з традиційним навчанням нейромережі проілюстровано на рис. 3.9.

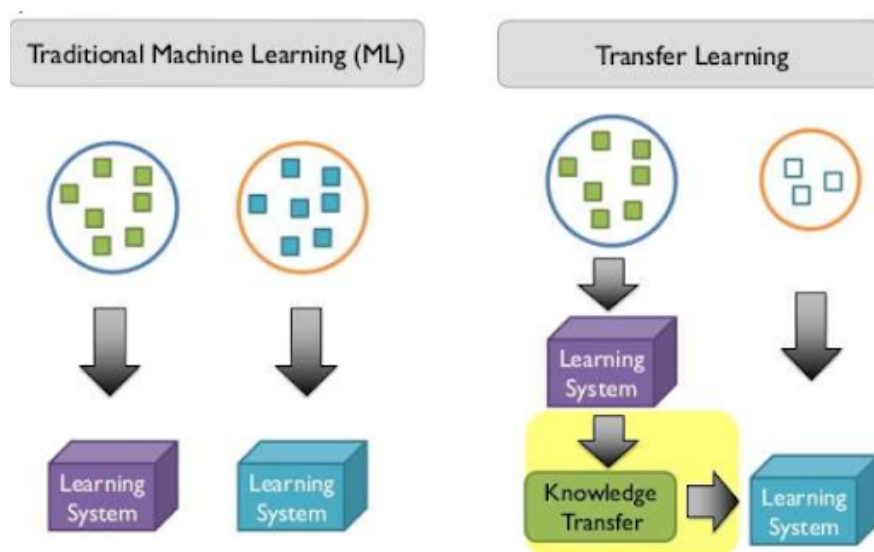


Рис. 3.9. Порівняння традиційного машинного навчання з Transfer Learning

При підході transfer learning передбачено можливість застосування одного з трьох варіантів навчання, які використовують:

- лише синаптичні ваги;
- лише вхідний набір даних;
- синаптичні ваги і вхідний набір зображень.

Враховуючи переваги застосування підходу передачі знань та згорткових нейронних мереж, пропонується їх використання при захопленні та аналізі зображень з камери у випадку спрацювання GSM-сигналізації.

3.2. Проектування топології нейронної мережі для реалізації функції розпізнавання обличчя системи GSM-сигналізації

Побудова топології нейронної мережі є однією з найважливіших стадій імплементації системи захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації. При обґрунтованому виборі топології необхідно виконати ряд послідовних кроків:

- визначитися з типом і класом задачі – у даному випадку необхідно класифікувати обличчя, віднісши його до одного з класів: наявне в базі даних зареєстрованих користувачів або ні;
- задати критерії продуктивності щодо швидкості і точності розпізнавання;
- проаналізувати параметри вхідних даних відносно джерела їх генерації: відеозображення, аудіопотік, фото, розмір та формат.

При реалізації системи захисту на базі GSM-сигналізації встановлено наступні типи обмежень::

- швидкість відгуку системи не повинна перевищувати 1 с;
- точність виявлення та аналізу обличчя на рівні не менше, ніж 75%.

Враховуючи висунуті вимоги та обмеження щодо реалізації підсистеми розпізнавання облич, топологію нейромережі запропоновано реалізувати у вигляді, як показано на рис. 3.10.

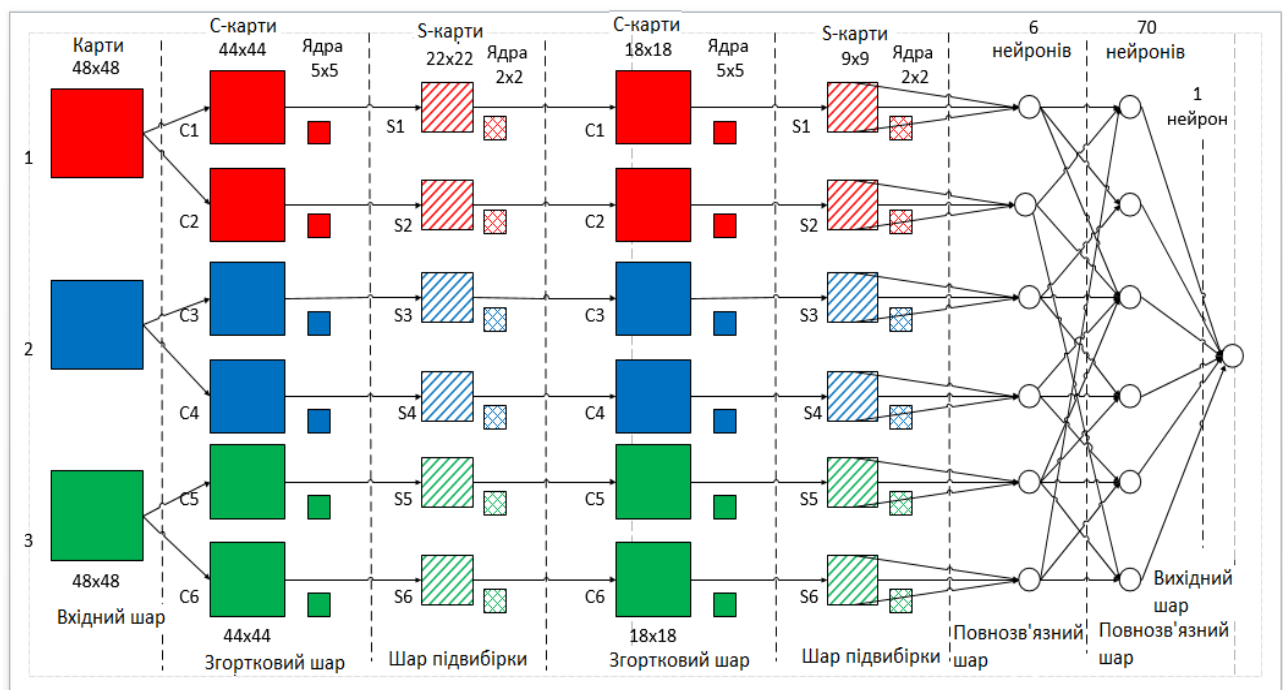


Рис. 3.10. Топологія спроектованої нейромережі

На вхідний шар нейронної мережі подаються зображення, отримані з камери, у форматі RGB розміром 48*48 пікселів. При цьому одне зображення представляється у вигляді трьох у відповідності до каналів кольоропередачі.

Для представлення згорткового шару формується карта ознак на яких у подальшому буде накладатися фільтр. З метою забезпечення надзвичайно високої точності виявлення необхідних об'єктів необхідні значні апаратні ресурси, оскільки це забезпечується за рахунок великої кількості карт ознак.

У випадку функціонування нейронної мережі на мікроконтролері ESP32-CAM необхідно враховувати його потужність і знайти компроміс між точністю і продуктивністю.

При аналізі наукових публікацій, зокрема [13,15], встановлено, що оптимальним варіантом при реалізації функції розпізнавання обличчя є співвідношення один до двох, тобто будь-яка карта ознак з попереднього шару має зв'язок з 2 картами ознак у згортковому шарі. Реалізації такого співвідношення проілюстровано на рис. 3.11.

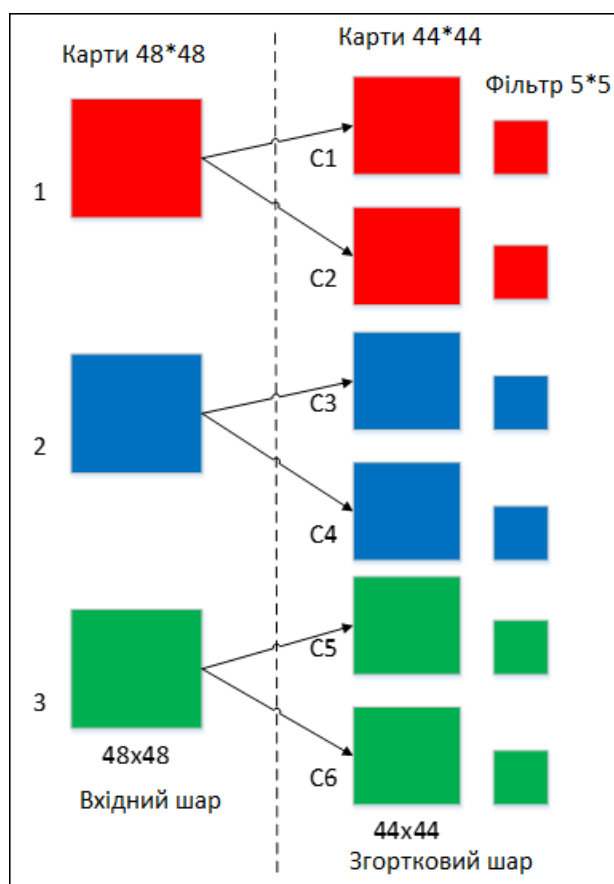


Рис. 3.11. Зв'язок 1 до 2 між шарами ЗНМ

В якості прикладу наведемо попередньо навчену згорткову нейронну мережу на наборі зображень людей. При цьому один фільтр в процесі навчання може забезпечувати виявлення ознак обличчя.

Всі інші шари по типу Pooling та повнозв'язних виконують функції, які описано у попередньому підрозділі кваліфікаційної роботи.

Що стосується кількості нейронів у вихідному шарі, то їх кількість повинна відповідати кількості класів зображень. При організації системи захисту фізичних стаціонарних об'єктів доцільно реалізувати класифікацію облич за двома класами (бінарна класифікація), тобто ідентифікації особи, яка є у визначеному списку дозволів, або її немає.

Окрім цього, оптимізацію ресурсів системи пропонується виконати за рахунок зменшення кількості зв'язків у нейронній мережі, тобто застосовувати тільки один нейрон вихідного шару, що відповідає за клас приналежності особи до списку дозволених.

3.3. Розробка алгоритму роботи системи захисту стаціонарних об'єктів на основі GSM-сигналізації

У загальному випадку, принцип функціонування систем захисту на основі GSM-модулів передбачає аналіз показників з використовуваних пристроїв вимірювання і виконання дій зі сповіщення при перевищенні верхніх порогових значень.

Виходячи із структури системи, що запропонована у попередньому розділі, загальний алгоритм можна вербально описати наступним чином:

1. Вимірювання і передача показників із сенсорів температури і вологості, сенсора газу, сенсора руху до ESP32.
2. У випадку перевищення порогового значення одного з показників виконується активація GSM-модуля і відбувається відправлення SMS-повідомлення власнику стаціонарного об'єкту і/або довіреним особам;
3. У випадку спрацювання сенсора руху повинна активуватися камера та модуль ESP32-CAM.
4. Виконується захоплення камерою певної області.
5. Визначаються кадри, які містять обличчя людини.
6. Виконується запропонований у попередньому підрозділі алгоритм для розпізнавання обличчя і результати порівнюються з наявним списком осіб, яким дозволено перебування у стаціонарному об'єкті.
7. Якщо результат розпізнавання відповідає образу людини, котрій дозволений доступ до об'єкту, то система переходить в стан очікування.
8. Якщо результат розпізнавання відмінний від фото, збережених у базі даних, то активується GSM-модуль і відправляється сповіщення власнику об'єкту і/або довіреним особам, а також зберігається фото на SD-карту та за наявності інтернет-з'єднання пересилається у віддалене місце зберігання.

Загальний алгоритм роботи системи безпеки фізичних стаціонарних об'єктів на основі GSM-сигналізації при зчитуванні даних із сенсорів по типу газу, температури і вологості представлений на рис. 3.12.

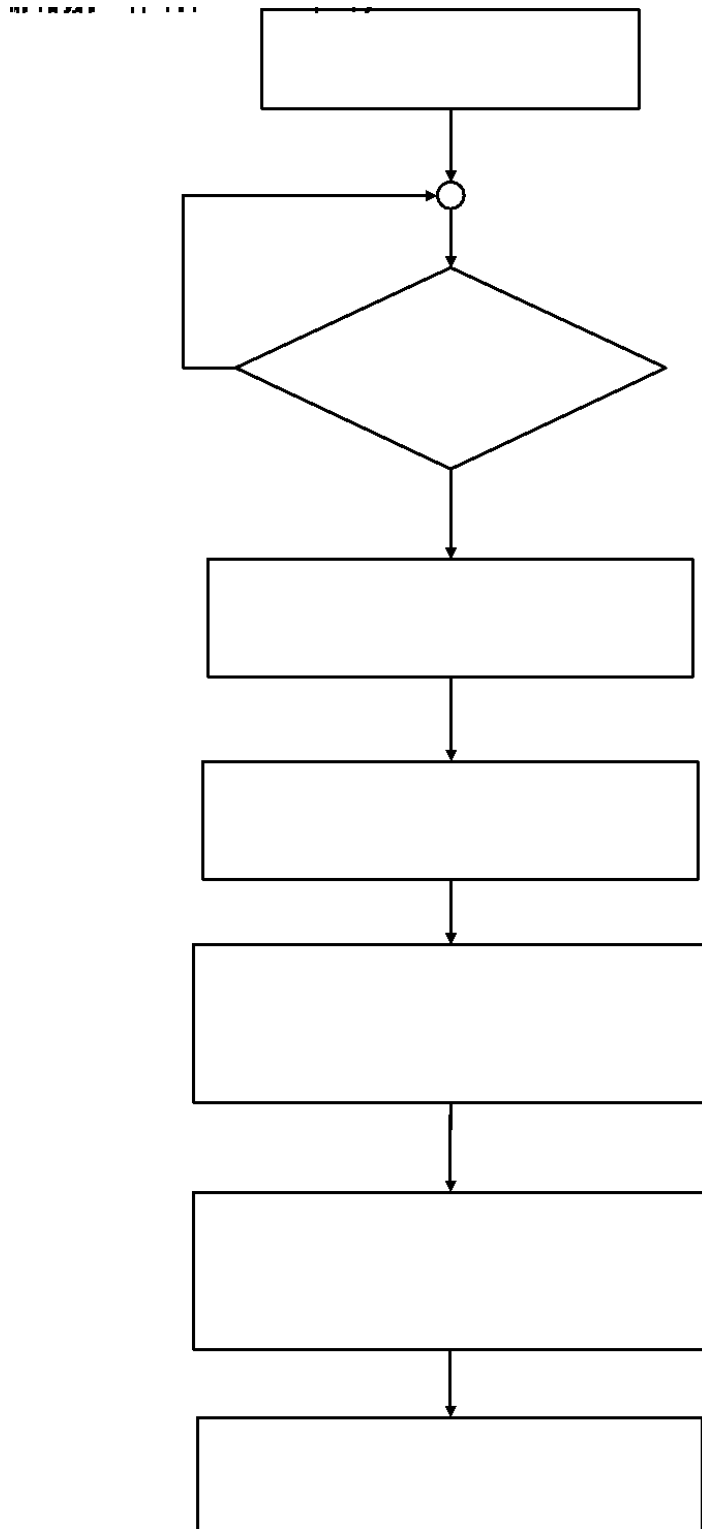


Рис. 3.12. Алгоритму функціонування системи GSM-сигналізації при перевищенні порогових значень сенсорів газу, температури і вологості

Алгоритм роботи системи безпеки у випадку активації сенсора руху представлено на рис. 3.13.

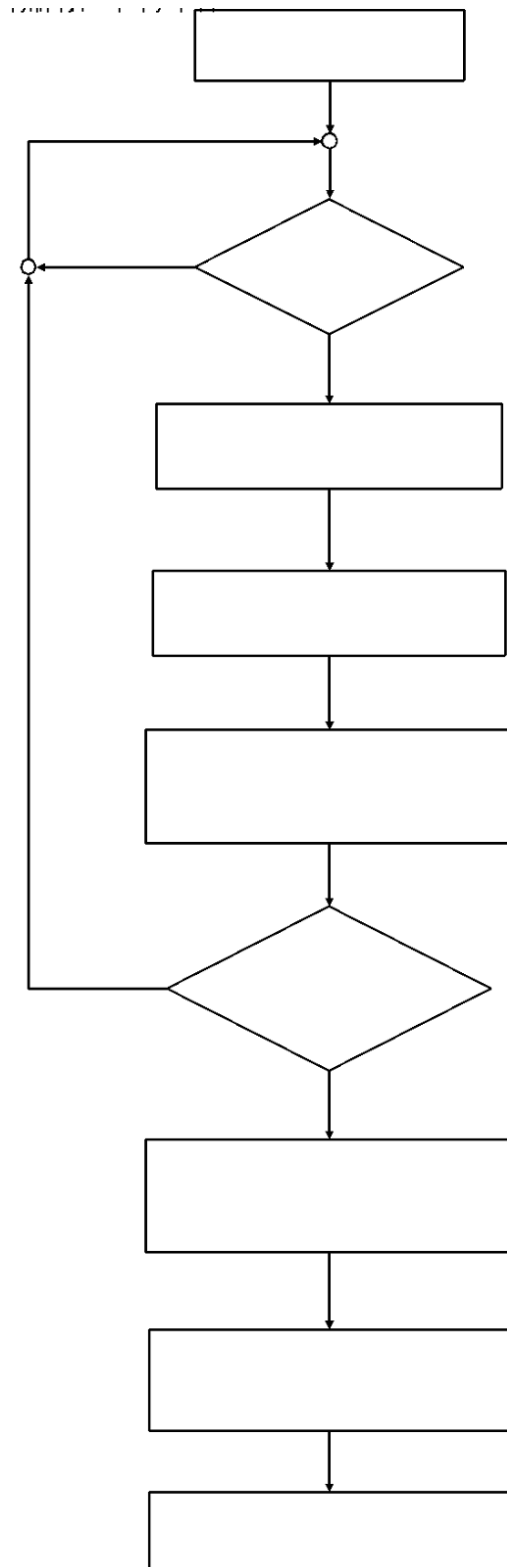


Рис. 3.13. Алгоритм роботи системи у випадку спрацювання сенсора руху

Розробивши теоретичне підґрунтя системи безпеки фізичних стаціонарних об'єктів на основі GSM-сигналізації далі необхідно перейти до встановлення і налаштування програмного забезпечення.

3.4. Встановлення та налаштування бібліотек ESP32-CAM

Насамперед, при встановленні та налаштуванні параметрів системного ПЗ для забезпечення ефективного функціонування мікроконтролера на базі ESP32 та ESP32-CAM, необхідно підключити потрібні модулі у середовищі Arduino IDE. Першим кроком є виконання дій, показаних на рис. 3.14 .

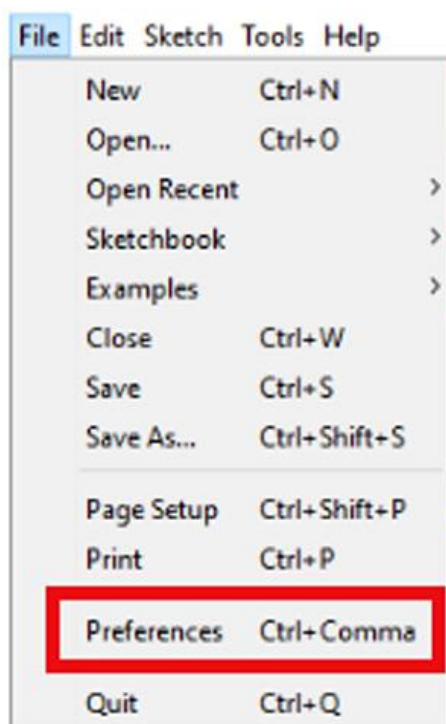


Рис. 3.14. Вибір меню налаштувань

Далі, обравши пункт вибору додаткових макетних плат потрібно вказати адресу з якої виконати завантаження бібліотеки (рис. 3.15).

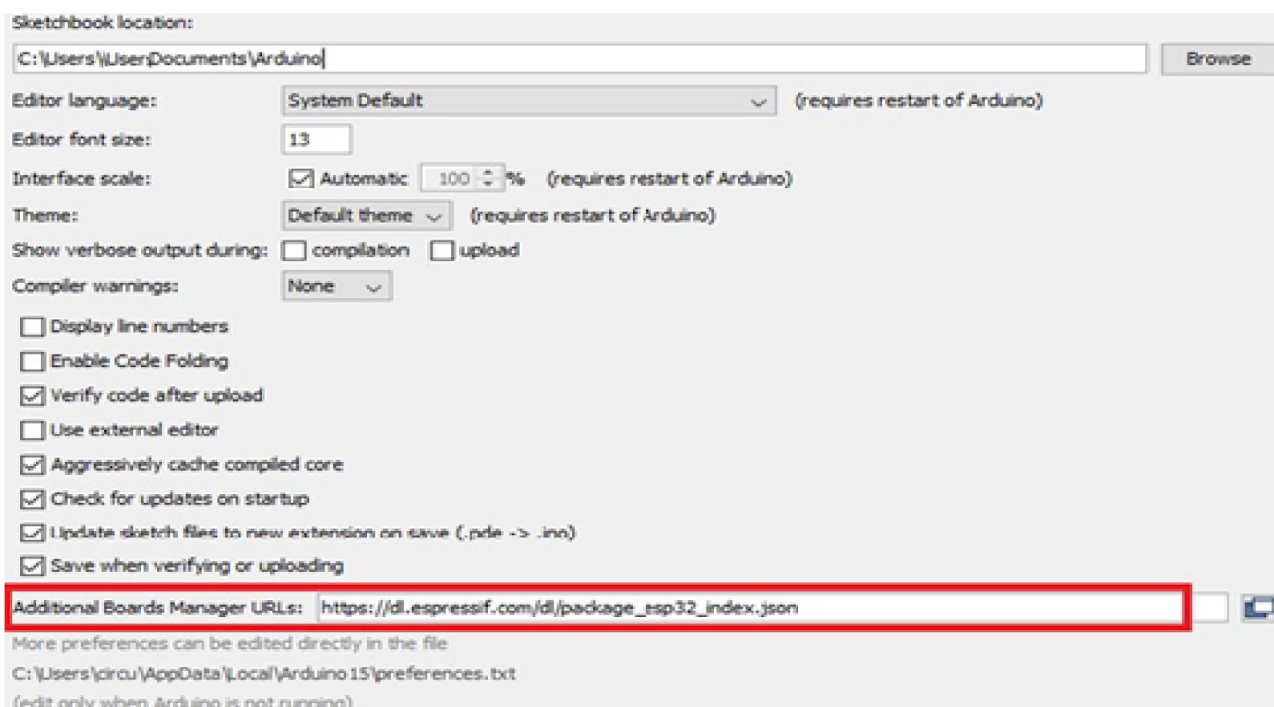


Рис. 3.15. Завантаження бібліотеки ESP32-CAM

Для підтвердження обраної дії натискається кнопка «Ок». Наступний крок передбачає вибір менеджера для управління макетними платами, як показано на рис. 3.16.

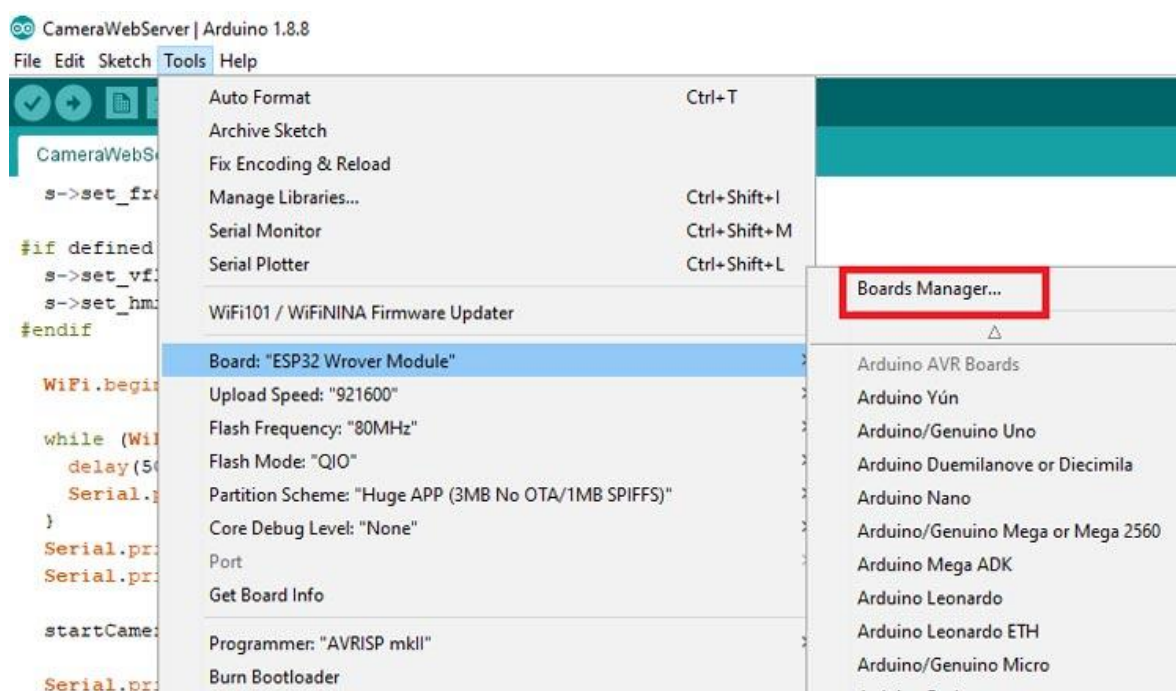


Рис 3.16. Підключення бібліотеки ESP32-CAM з Arduino IDE

Безпосереднє встановлення бібліотеки для роботи з ESP32 із середовища Arduino IDE показано на рис. 3.17.

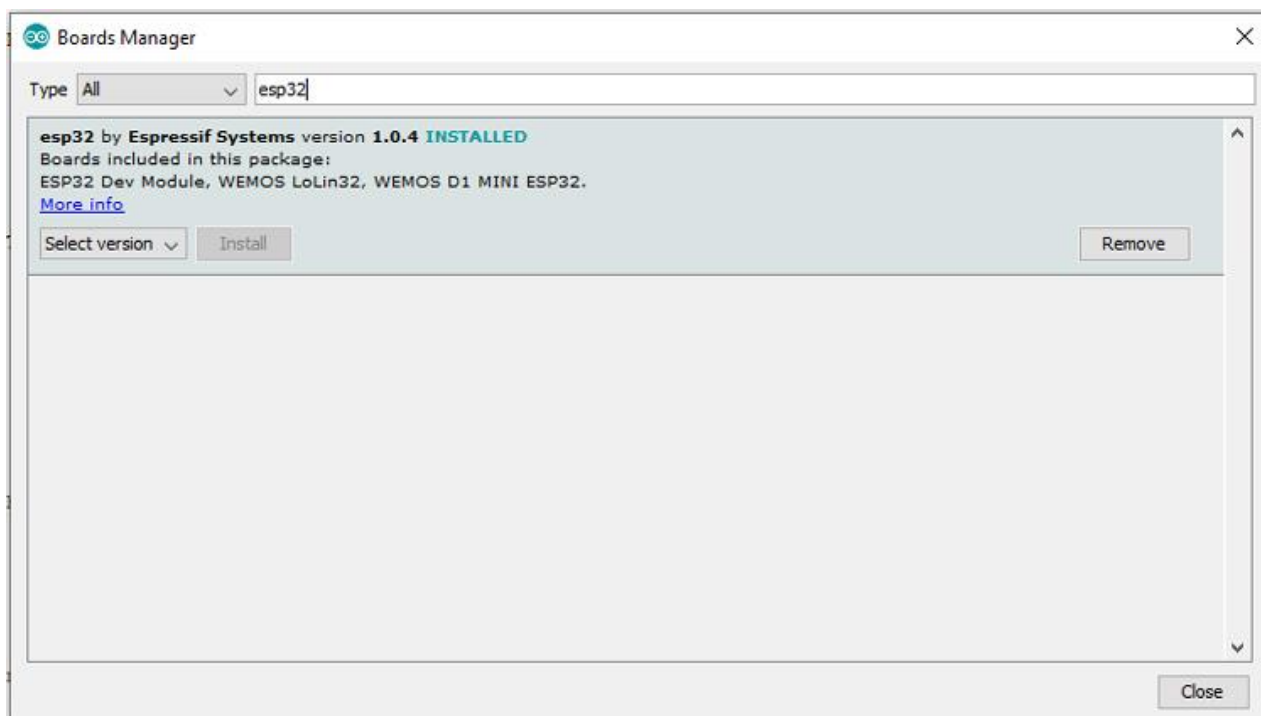


Рис. 3.17. Інсталяція “ESP32 by Espressif Systems”

Налаштування бібліотек необхідних для роботи визначених відбувається подібним чином. Підключивши необхідні бібліотеки можна приступити до написання системного ПЗ для управління GSM-сигналізацією. Фрагмент коду підключення програмних модулів для роботи з ESP32 та комунікації через WiFi показано на рис. 3.18.

```
#include "esp_camera.h"
#include <WiFi.h>
#include "camera_pins.h"
```

Рис. 3.18. Фрагмент підключення бібліотек

При виборі типу камери для захоплення зображення із

контрольованих зон стаціонарного об'єкту потрібно видалити або описати у вигляді коментарів стрічки коду, які показані на рис. 3.19.

```
//#define CAMERA_MODEL_WROVER_KIT
//#define CAMERA_MODEL_ESP_EYE
//#define CAMERA_MODEL_M5STACK_PSRAM
//#define CAMERA_MODEL_M5STACK_WIDE
#define CAMERA_MODEL_AI_THINKER
```

Рис. 3.18. Підключення камери «CAMERA_MODEL_AI_THINKER»

За замовчуванням може використовуватися 5 різних типів камер, проте у проекті застосовується лише одна – не закоментована константа.

Забезпечення доступу до наявної безпроводної мережі передачі даних реалізується шляхом початкового налаштування з вказанням назви мережі та сигнатури автентифікації, як показано на рис. 3.19.

```
const char* ssid = "Wi-Fi Name";
const char* password = "Wi-Fi password";
```

Рис. 3.19. Оголошення змінних для доступу до мережі

Далі необхідно програмно визначити вивід, що відповідатиме за взаємодію з модулем реле. Реалізація функції «`millis ()`», яка показана на рис. 3.20, забезпечує встановлення початкового стану механізму замка після того, як відбулось успішне розпізнавання обличчя. Задана затримка рівна 5 с.

```
#define relay 4
long prevMillis = 0;
int interval = 5000;
```

Рис. 3.20. Оголошення виводу реле та інтервалу блокування замка

Функція `setup()` передбачає ініціалізацію послідовного монітора із заданою швидкістю 115200 для переходу до режиму налаштувань. Решта програмного коду, представленого на рис. 3.21, задає режим роботи реле.

```
void setup() {
  Serial.begin(115200);
  pinMode(relay, OUTPUT);
  digitalWrite(relay, LOW);
}
```

Рис. 3.21. Ініціалізація функції `setup()`

Імплементація алгоритму розпізнавання обличчя реалізується шляхом виклику функції перевірки обличчя, яка інтегрована в іншій функції – `loop()`. Така реалізація забезпечує порівняння зображення одержаного з камери та тих, які зберігаються у базі даних. На рис. 3.22 продемонстровано алгоритм перевірки схожості виявленого обличчя і тих, котрі наявні у БД.

```
void loop() {
  if (matchFace == true && activeRelay == false){
    activeRelay = true;
    digitalWrite (relay, HIGH);
    prevMillis = millis();
  }
  if(activeRelay == true && millis()- prevMillis > interval){
    activeRelay = false;
    matchFace = false;
    digitalWrite(relay, LOW);
  }
}
```

Рис. 3.22. Виклик функції ідентифікації обличчя

Прямий доступ до ESP32-CAM забезпечується через стрічку адресу у якій прописується його IP-адреса ESP. Ввівши адресу, з'являється вікно,

яке показано на рис. 3.23.

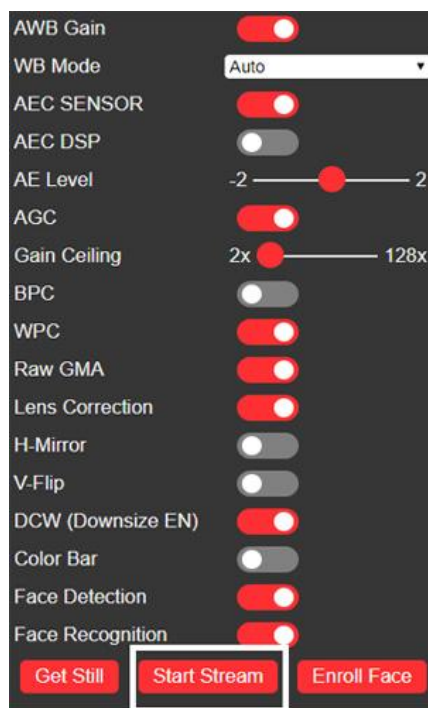


Рис. 3.23. Вікно налаштування відеотрансляції

Натиснення кнопки початку відеотрансляції активує вивід зображень, які потрапляють в об'єктив камери. Для того, щоб зареєструвати користувачів, яким дозволено доступ до фізичного стаціонарного об'єкту та активувати програму виявлення і розпізнавання облич можна скористатися варіантом, який показаний на рис. 3.24.

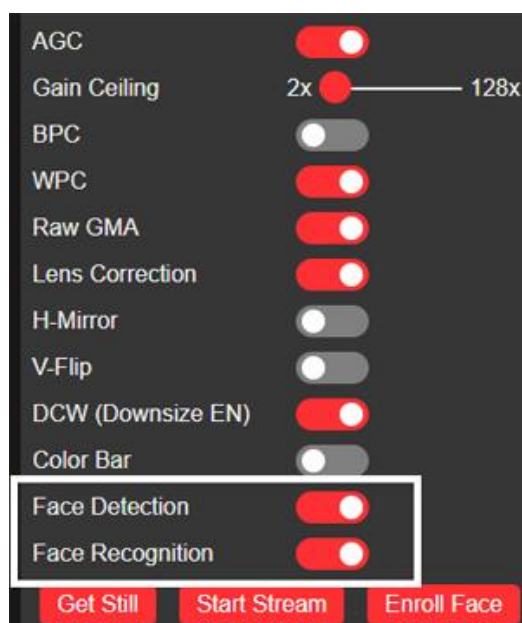


Рис. 3.24. Налаштування розпізнавання та реєстрації обличчя

Натиснувши на кнопку реєстрації (додавання) облич, будуть збережені налаштування щодо їх виявлення та розпізнавання. Таку процедуру виконують декілька разів з метою одержання більш повної множини облич зареєстрованих користувачів.

Проте можна скористатися й іншим шляхом – ручним завантаженням зображень на сервер із вказанням читабельних назв, які будуть відображатися при успішному розпізнаванні. Результат успішної ідентифікації особи, чиї дані збережені у БД, приведено на рис. 3.25.

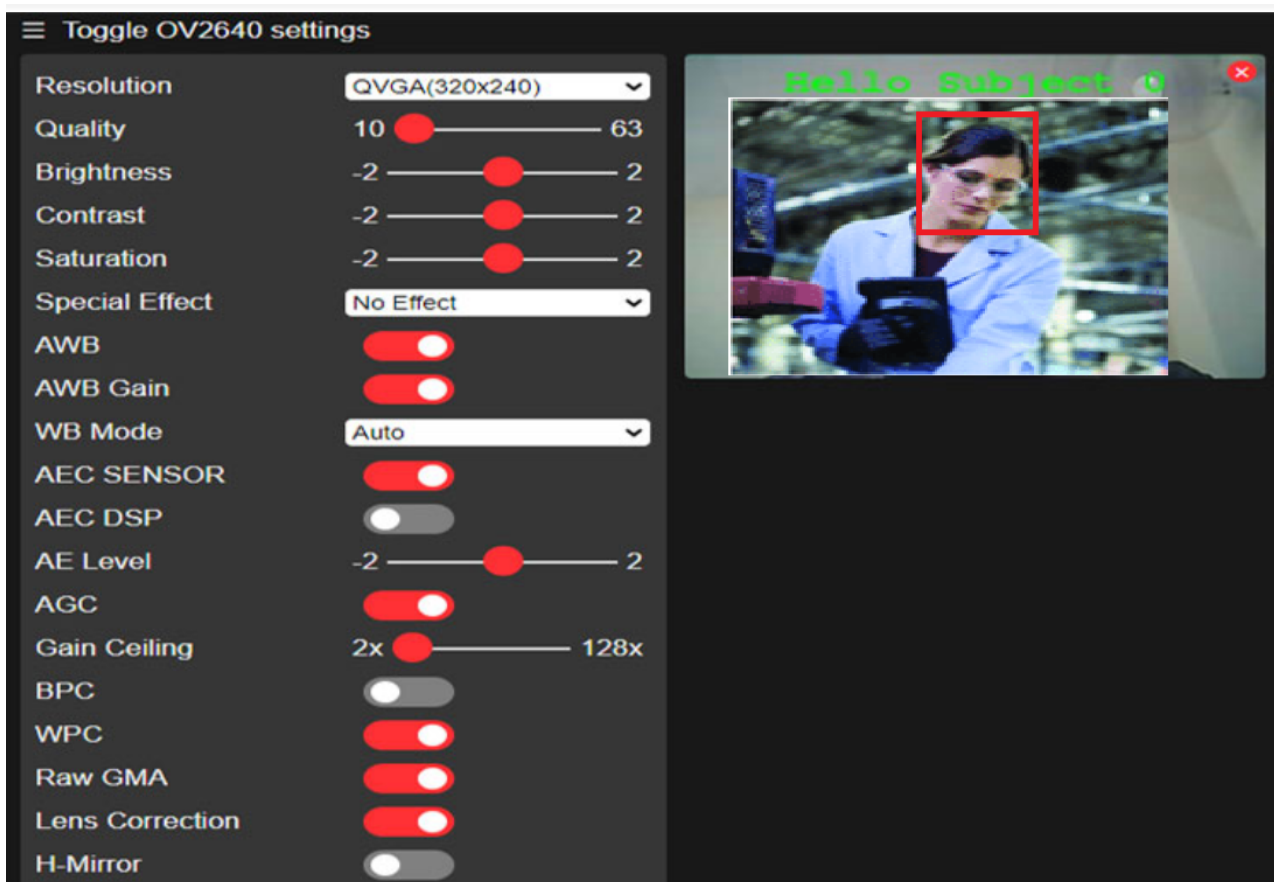


Рис. 3.25. Результат розпізнавання обличчя

Таким чином у кваліфікаційній роботі запропоновано і практично імплементовано систему захисту фізичних стаціонарних об'єктів, яка використовує сенсори температури та вологості, датчик газу, сенсор руху і підсистему розпізнавання облич, а в якості передавача сповіщень застосовується GSM-модуль.

3.5. Висновки до розділу

Основні результати даного розділу полягають в наступному:

1. Проаналізовано принципи організації та архітектури згорткових нейронних мереж і встановлено, що вони є найбільш ефективним засобом при розв'язку задач комп'ютерного зору, зокрема при виявленні і розпізнаванні облич, що дало змогу обґрунтувати їх застосування у системах GSM-сигналізацій.

2. Запропоновано архітектуру нейромережі для забезпечення функції розпізнавання облич, що використовує топологію згорткової нейронної мережі і дає змогу оптимізувати використання апаратних ресурсів за рахунок використання лише одного нейрону у вихідному шарі.

3. Розроблено загальний і частковий алгоритми роботи комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації, де визначено послідовність виконання дій при зчитуванні даних із сенсорів та їх опрацювання мікроконтролерами, а також функціонування підсистеми розпізнавання облич.

4. Проведено налаштування параметрів для функціонування мікроконтролерів ESP32 та ESP32-CAM при управлінні системою формування сповіщень GSM-модуля.

РОЗДІЛ 4

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

У кваліфікаційній роботі магістра проведено дослідження методів і засобів організації комп'ютерних систем захисту фізичних стаціонарних об'єктів та запропоновано власне рішення щодо їх побудови. Оскільки, проектування комп'ютерної системи захисту стаціонарних об'єктів виконується з використанням ПК та IoT пристроїв, то важливо забезпечити дотримання вимог і правил техніки безпеки та охорони праці для розробника.

Діючим основним нормативним документом, який визначає і регламентує норми і правила експлуатації електронно-обчислювальної техніки є НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» [23]. Правила встановлюють вимоги безпеки до обладнання робочих місць операторів ЕОМ.

НПАОП 0.00-7.15-18 є обов'язковим для виконання роботодавцями, операторами електронно-обчислювальних машин, операторами комп'ютерного набору, операторами комп'ютерної верстки та працівників інших професій, які у своїй роботі застосовують ЕОМ з ВДТ і ПП [23].

Згідно НПАОП 0.00-7.15-18 електронно-обчислювальні засоби повинні відповідати вимогам чинних в Україні стандартів і пройти державну санітарно-епідеміологічну експертизу у Порядку проведення державної санітарно-епідеміологічної експертизи.

З метою забезпечення електробезпеки користувачів ПК при проектуванні комп'ютерної системи захисту фізичних стаціонарних

об'єктів з використанням GSM-сигналізації необхідно, щоб комп'ютери і периферійні пристрої відповідали I-му класу захисту, або були заземленими відповідно до вимог НПАОП 40.1-1.32-01.

Неприпустимим є використання клем функціонального заземлення для підключення захисного заземлення [24].

При організації робочих місць користувачів комп'ютерних систем необхідно забезпечити дотримання вимог щодо їх розташування, зокрема відстань робочого місця від стіни повинна складати 1 м, а відстань між робочими місцями повинна становити 1,7 м. Площа, яка виділяється на одне робоче місце, обладнане ПК становить – $\geq 6.0 \text{ м}^2$, а об'єм – $\geq 20 \text{ м}^3$ [24].

При виборі кімнат для розміщення робочих місць ПК враховано ступінь відбиття світла на екранах дисплеїв, яке проходить через вікна і яке може викликати значне осліплення в тих, хто сидить перед ними, особливо влітку та в сонячні дні. Тому, ПК і оргтехніка розміщені біля стін, які не знаходяться біля вікон або навпроти них [24].

Оскільки, при незадовільному освітленні знижується продуктивність праці користувачів ПК, і можливі негативні впливи на здоров'я такі, як короткозорість, швидка втомленість, тому всі приміщення, які облаштовані робочими місцями з ПК, мають природне і штучне освітлення. Не допускається розташування робочих місць з ПК в підвальних приміщеннях [24].

Робочі місця з ПК при виконанні творчої роботи, яка потребує значної розумової концентрації, зокрема при реалізації алгоритмів машинного навчання для перетворення тексту в аудіопотік, ізолювано одне від одного перегородкою висотою 1,6 м [23]. Поверхня підлоги у приміщеннях повинна бути оздоблена керамічною плиткою і бути рівною та зручною для очищення та вологого прибирання.

Штучне освітлення у приміщеннях повинно бути виконано у вигляді комбінованої системи освітлення з використанням люмінесцентних джерел світла у світильниках загального освітлення, які розташовувати над

робочими поверхнями у рівномірно-прямокутному порядку. Штучне освітлення забезпечує на робочих місцях з ПК освітленість 300 – 500 Лк [23].

Для запобігання засвітленню екранів ПК прямими світловими потоками лінії світильників розташовані з достатнім бічним зміщенням відносно рядів робочих місць, а також паралельно до світлових отворів. При цьому кожне вікно повинно мати світлорозсіюючі штори з коефіцієнтом відбивання 0,7 [22].

У приміщенні також необхідно забезпечити і природнє освітлення, при цьому на кожному вікні закріплені жалюзі з вертикальними ламелями, що регулюються для зменшення прямого попадання сонячного світла на екран комп'ютерів.

З метою запобігання нещасним випадкам та організації охорони праці на виробництві розробляються інструкції з охорони праці і техніки безпеки при використанні комп'ютерної техніки. Дія інструкції поширюється на всі структурні підрозділи установи [25].

До роботи на ПК допускаються особи, які пройшли спеціальне навчання, медичне обстеження, вступний інструктаж з охорони праці, інструктаж на робочому місці та інструктаж з пожежної безпеки [25].

З ергономічної точки зору, при розташуванні елементів робочого місця враховано наступні фактори [25]:

- простір для розміщення користувача;
- можливість огляду елементів робочого місця;
- можливість огляду простору за межами робочого місця;
- можливість робити записи, розміщення документації і матеріалів, які використовує користувач.

При дослідженні методів і засобів організації комп'ютерних систем захисту фізичних стаціонарних об'єктів з використанням GSM-сигналізації проведено аналітичний огляд чинних вимог з охорони праці і техніки безпеки та відповідно враховано їх, що дозволило забезпечити зручні

умови для ефективної роботи користувачів спроектованої комп'ютерної системи.

4.2. Засоби захисту персоналу від уражень радіації

Враховуючи необхідність проведення державних заходів захисту населення від надзвичайних ситуацій прийнято Закон "Про цивільну оборону України". Згідно із Законом кожен громадянин має право на захист свого життя і здоров'я від наслідків аварій, катастроф, пожеж, стихійного лиха та має право на надання гарантій забезпечення реалізації цього права від Кабінету Міністрів України, міністерств та інших центральних органів місцевого самоврядування, керівництва підприємств, установ і організації незалежно від форм власності й підпорядкування. Як гарант цього права держава створила систему цивільної оборони.

З метою забезпечення стійкості роботи важливих виробничих підприємств (об'єктів) в надзвичайних ситуаціях мирного і воєнного часу завчасно проводиться комплекс організаційних і інженерно-технічних заходів цивільної оборони, спрямованих на забезпечення захисту населення і зменшення руйнувань, на підвищення стійкості роботи об'єкту, на утворення необхідних умов для проведення РіІНР [25].

Основними вимогами до проектування й побудови промислових підприємств (об'єктів) є забезпечення стійкості інженерно-технічного комплексу об'єкту.

Згідно [24], будівлі і споруди на об'єкті необхідно розміщувати розосереджено, при цьому відстань між будівлями повинна забезпечувати протипожежні розриви.

Пожежні розриви між будівлями повинні бути проєктовані таким чином, щоб виключити можливість перенесення вогню з однієї будівлі на іншу. В загальному випадку, ширина протипожежного розриву L_p , м, визначається за формулою: $L_p = H_1 + H_2 + 15$ м, де H_1 і H_2 – висота сусідніх будинків. Будівлі адміністративно-господарського і

обслуговуючого призначення повинні розміщуватись окремо від основних цехів.

Виходячи з того, що важливі виробничі споруди будують заглибленими або пониженої висоти, і вони, зазвичай, прямокутної форми, то виробничі цехи повинні бути спроектовані у відповідності до цих вимог. Це дозволяє зменшити парусність будівлі і збільшити її опір при ударній хвилі будь-якого вибуху. Висока стійкість до дії ударної хвилі властива залізобетонній будівлі з металевими каркасами в бетонній опалубці.

Для підвищення стійкості до пожеж необхідно застосовувати вогнестійкі конструкції та проведення вогнезахисної обробки горючих елементів будівлі. У цехах, які збудовано з каменю перекриття виготовляється з бетонних плит.

У технічних заходах пожежного захисту повинно передбачатися 4 виходи, ширина коридорів у приміщеннях повинна складати 2,6 м. Усі будівлі підприємств повинні використовувати систему протидимового захисту, пожежного зв'язку і сигналізації, а будівельні роботи повинні бути виконані з вогнетривких матеріалів. Усі приміщення повинні бути обладнані засобами пожежогасіння.

Організаційні заходи проектування на підприємствах реалізуються шляхом навчання працюючих правилам пожежної безпеки, розробки інструкцій про правила роботи з пожежонебезпечними матеріалами та про дії персоналу під час пожежі.

У ряді випадків при проектуванні і будівництві промислових будівель і споруд повинна бути передбачена можливість герметизації приміщень від проникнення радіоактивного порошу. Це особливо важливо для підприємств харчової промисловості і продовольчих складів.

Деякі унікальні види технологічного устаткування потрібно розміщувати в більш міцних спорудах (підвалах, підземних спорудах) або будівлях з легких незгорюючих конструкцій павільйонного типу, під

навісами або відкрито. Це обумовлюється тим, що в багатьох випадках устаткування може витримати набагато більший надлишковий тиск ударної хвилі, ніж будівля, в якій воно знаходиться. При зруйнуванні будівлі внаслідок падіння конструкцій розміщене в них устаткування буде виходити з ладу.

Дороги на території підприємств повинні мати тверде покриття і забезпечувати зручний шлях руху між сусідніми будівлями; кількість в'їздів на територію даного підприємства об'єкту – два у різних напрямках. Системи побутової і виробничої каналізації повинні мати два випуски у міську каналізаційну мережу.

Електрозабезпечення є основою будь-якого виробництва. Порушення нормальної подачі електроенергії на об'єкт або окремі ділянки виробництва може призвести до повної зупинки роботи об'єкту.

Для надійного електрозабезпечення підприємстві в умовах надзвичайних ситуації при її проектуванні і будівництві повинні бути враховані основні вимоги, які впливають із завдань цивільної оборони. Електрозабезпечення підприємств повинно здійснюватися від енергосистем міста, до складу яких входять електростанції, що працюють на різних видах палива. При електропостачанні об'єкту від одного джерела передбачено два вводи з різних напрямів. Електроенергію на ділянках виробництва подають по належних електрокабелях, прокладених в землі на глибині 1 м.

Крім цього, на території підприємств необхідно передбачити створення автономних резервних джерел електропостачання у вигляді автономних генераторів на дизельному паливі.

Для підвищення стійкості постачання об'єктів водою необхідно, щоб система водопостачання здійснювалась не менше, ніж від двох незалежних джерел, одне з яких бажано влаштовувати підземним.

Стійкість мережі водопостачання підвищується при заглибленні в ґрунт всіх ліній водопроводу і розташування належних гідрантів і

відключаючих пристроїв на території, яка не може бути заваленою, а також пристроїв перемичок, які дозволяють відключити пошкоджені ланки і споруди.

На багатьох виробничих об'єктах газ використовується як паливо, а на хімічних підприємствах - і як вихідна сировина. При порушенні мережі, газ може стати причиною вибуху, пожежі. Для більш надійного постачання газ повинен подаватися в місто і на промислові об'єкти по двох незалежних газопроводах. Газорозподільчі станції повинні бути розташованими за межами міста. Газова мережа за кільцюється і прокладається під землею на глибині 0,6-1,7 м. На газовій мережі у визначених місцях встановлюються автоматичні відключаючі пристрої, які спрацьовують від надлишкового тиску ударної хвилі.

Крім того, на газопроводах встановлюють відключаючу апаратуру з дистанційним управлінням і крани, які автоматично перекривають подачу газу при розриві труб, що дозволяє відключити газові мережі певних ділянок і районів міста.

ВИСНОВКИ

Основні наукові та практичні результати полягають в наступному.

1. Проведено аналіз принципів і технології організації GSM-зв'язку, у результаті якого визначено переваги і недоліки їх застосування у системах на основі мікроконтролерів та IoT-пристроїв. Обгрунтовано доцільність їх застосування при організації систем захист фізичних стаціонарних об'єктів.

2. Проаналізовано особливості проектування та імплементації систем захисту фізичних стаціонарних об'єктів на основі GSM-сигналізацій, що дало змогу визначити їх мінімальну необхідну функціональність та запропонувати шляхи вдосконалення шляхом імплементації у мікроконтролери моделей розпізнавання облич при спрацюванні сенсору руху.

3. Спроековано архітектуру комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі мікроконтролерів ESP32 та ESP32-CAM з підключенням сенсорів газу, температури і вологості, датчика руху і сумісної камери з роздільною здатністю 2Мп, що дало можливість підвищити функціональність системи за рахунок інтеграції програмної моделі інтелектуального розпізнавання облич, яка активується при спрацюванні тригера у вигляді сигналу від сенсора руху з подальшою передачею сповіщення за допомогою GSM-модуля власнику об'єкта.

4. Проаналізовано та обгрунтовано застосування компонентної бази для практичної реалізації системи захисту фізичних стаціонарних об'єктів, що дало можливість забезпечити надійність та визначену функціональність роботи GSM-сигналізації.

5. Спроековано схеми підключення компонентів системи захисту фізичних стаціонарних об'єктів, що дало змогу забезпечити комунікацію всередині системи та оптимально налаштувати взаємодію між пристроями, а отже і забезпечити ефективне функціонування GSM-сигналізації.

6. Проаналізовано принципи організації та архітектури згорткових нейронних мереж і встановлено, що вони є найбільш ефективним засобом при розв'язку задач комп'ютерного зору, зокрема при виявленні і розпізнаванні облич, що дало змогу обґрунтувати їх застосування у системах GSM-сигналізацій.

7. Запропоновано архітектуру нейромережі для забезпечення функції розпізнавання облич, що використовує топологію згорткової нейронної мережі і дає змогу оптимізувати використання апаратних ресурсів за рахунок використання лише одного нейрону у вихідному шарі.

8. Розроблено загальний і частковий алгоритми роботи комп'ютерної системи захисту фізичних стаціонарних об'єктів на основі GSM-сигналізації, де визначено послідовність виконання дій при зчитуванні даних із сенсорів та їх опрацювання мікроконтролерами, а також функціонування підсистеми розпізнавання облич.

9. Проведено налаштування параметрів для функціонування мікроконтролерів ESP32 та ESP32-CAM при управлінні системою формування сповіщень GSM-модуля.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ESP32-CAM Video Streaming Web Server (works with Home Assistant). URL: <https://randomnerdtutorials.com/esp32-cam-video-streaming-web-server-camera-home-assistant/> (дата звернення 14.11.2024 р.)
2. Nemchak O., Luhovych O., Kobzar S. Study of identification methods for access of vehicles to closed object. V All Ukrainian Scientific and Practical Conference “Current trends in young scientists’ researches”, April 12, 2018. Zhytomyr: ZHDTU, 2018. С.92-95.
3. Beginner’s Guide to Object Detection Algorithms. URL: <https://medium.com/analytics-vidhya/beginners-guide-to-object-detectionalgorithms-6620fb31c375> (дата звернення 16.11.2024).
4. Офіційна сторінка Open CV. URL: <https://opencv.org/about/> (дата звернення 20.11.2024).
5. ESP8266:Примеры/Веб-сервер с помощью ESP8266 и IDE Arduino. URL: http://wikihandbk.com/wiki/ESP8266:%D0%9F%D1%80%D0%B8%D0%BC%D0%B5%D1%80%D1%8B/%D0%92%D0%B5%D0%B1-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80_%D1%81_%D0%BF%D0%BE%D0%BC%D0%BE%D1%89%D1%8C%D1%8E_ESP8266_%D0%B8_IDE_Arduino (дата звернення 28.11.2024 р.)
6. IoT: від «розумних» лампочок до передових технологій виробництва / Новини / IT українською URL: <http://it-ua.info/news/2016/06/21/iot-vd-rozumnih-lampochok-do-peredovih-tehnology-virobnictva.html> (дата звернення 26.11.2024р.).
7. Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Програма та методичні рекомендації з проходження практики за тематикою кваліфікаційної роботи для студентів спеціальності 123 «Комп’ютерна

інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. ТНТУ. 2024. 45 с.

8. Луцик Н. С., Луцків А. М., Осухівська Г. М., Тиш Є. В. Методичні рекомендації до виконання кваліфікаційної роботи магістра для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль. ТНТУ. 2024. 44 с.

9. Варавін А.В., Лецишин Ю.З., Чайковський А.В. Методичні вказівки до виконання курсового проєкту з дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» для здобувачів другого (магістерського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль. ТНТУ, 2024. 32 с.

10. Жаровський Р.О., Іваницький В.А. GSM-сигналізації як спосіб розширення функціональності розумних будинків та підвищення безпеки об'єктів нерухомості. Матеріали XII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (18-19 грудня 2024 року). Тернопіль: ТНТУ. 2024. С. 124.

11. Жаровський Р.О., Іваницький В.А. Організація захисту стаціонарного об'єкту нерухомості на основі GSM-сигналізації та мікроконтролера Raspberry Pi. Матеріали XII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (18-19 грудня 2024 року). Тернопіль: ТНТУ. 2024. С. 125.

12. Cerence/Nuance TTS Ukrainian. URL: <https://nextup.com/cerence/> (дата звернення: 08.12.2024).

13. Yasniy O., Pastukh O., Didych I., Yatsyshyn V., Chykhira I. Application of machine learning for modeling of 6061-T651 aluminum alloy stress–strain diagram. *Procedia Structural Integrity*. 48. 2023. pp. 183–189.

14. Yatsyshyn V., Pastukh O., Palamar A., Zharovskyi R. Technology of relational database management systems performance evaluation during computer systems design. *Scientific Journal of TNTU (Tern.)*. Vol. 109. No 1. 2023. pp. 54–65.
15. Pastukh O., Yatsyshyn V. Development of software for neuromarketing based on artificial intelligence and data science using high-performance computing and parallel programming technologies. *Scientific Journal of TNTU. Tern.: TNTU*, 2024. Vol 113. No 1. P. 143–149.
16. Griffin-Lim Algorithm. URL: <https://paperswithcode.com/method/griffin-lim-algorithm> (дата звернення: 10.12.2024).
17. Information Processing Systems. URL: <https://proceedings.neurips.cc/paper/2019/file/f63f65b503e22cb970527f23c9ad7db1-Paper.pdf> (дата звернення: 11.11.2024).
18. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп'ютеризованих вимірювальних систем і комплексів. Навчальний посібник. Тернопіль: ТНТУ. 2019. 150 с.
19. Погребенник В. Д., Клим Г. І., Бордун І. М., Пташник В. В., Паламар А. М. Системи оперативного контролю інтегральних параметрів водного середовища. Т. 2. Елементи комп'ютерних систем оперативного контролю: колективна монографія. Житомир: Видавничий дім «Бук-Друк», 2021. 180 с.
20. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Київ. 2018.
21. Жидецький В.Ц. Охорона праці користувачів комп'ютерів. Львів: Афіша, 2011. 176 с.
22. Желібо Е.Н. Безпека життєдіяльності: Навчальний посібник/ За редакцією Е.П. Желібо, В.М. Львів: «Новий світ - 2000», 2011. 320с.

23. Стадник І.Я., Зварич Н.М. Оцінка хімічної обстановки при аваріях на хімічно небезпечних об'єктах викидом (виливом) небезпечних хімічних речовин та застосуванні хімічної зброї. ТНТУ. 2020. 36 С.

24. Стадник І.Я., Зварич Н.М. Оцінка хімічної обстановки при аваріях на хімічно небезпечних об'єктах викидом (виливом) небезпечних хімічних речовин та застосуванні хімічної зброї. ТНТУ. 2020. 36 С.

25. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання «Безпека в надзвичайних ситуаціях» / В.С. Стручок –Тернопіль: ФОП Паляниця В. А.156 с.

26.

Додаток А

Текст наукових публікацій кваліфікаційної роботи магістра

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

**XIII Міжнародної науково-практичної
конференції молодих учених та студентів**
11-12 грудня 2024 року



УКРАЇНА
ТЕРНОПІЛЬ – 2024

В. Бражніков, Г. Осухівська ВПЛИВ ПЕРСОНАЛІЗАЦІЇ КЛІЄНТСЬКИХ ВЗАЄМОВІДНОСИН НА ЕФЕКТИВНІСТЬ CRM-СИСТЕМ У ЛОГІСТИЦІ V. Brazhnikov, H. Osukhivska THE IMPACT OF CUSTOMER RELATIONSHIP PERSONALIZATION ON THE EFFICIENCY OF CRM SYSTEMS IN LOGISTICS	114
А. М. Паламар, Р. О. Жаровський, Ю. С. Гарбів СИСТЕМА МОНІТОРИНГУ АТМОСФЕРНОГО ТИСКУ ЗА ДОПОМОГОЮ IOT-ТЕХНОЛОГІЙ A. M. Palamar, R. O. Zharovskiy, Y. S. Harbich SYSTEM FOR MONITORING ATMOSPHERIC PRESSURE USING IOT TECHNOLOGIES	115
С. Вінтонів, Є. Туш ОПТИМІЗАЦІЯ КІЛЬКОСТІ ЗАПИТІВ ДО БАЗИ ДАНИХ ДЛЯ GRAPHQL-API З ВИКОРИСТАННЯМ DATALOADER S. Vintoniv, Ye. Tysh OPTIMIZING THE NUMBER OF DATABASE QUERIES FOR GRAPHQL-API USING DATALOADER	116
А. М. Паламар, Ю. С. Гарбів КОМП'ЮТЕРИЗОВАНА СИСТЕМА ДЛЯ IOT-МОНІТОРИНГУ АТМОСФЕРНОГО ТИСКУ A. M. Palamar, Y. S. Harbich COMPUTERIZED SYSTEM FOR IOT MONITORING OF ATMOSPHERIC PRESSURE	117
Н. О. Гладовський ПРОГРАМНІ РІШЕННЯ МОНІТОРИНГУ СИСТЕМ ТА МЕРЕЖ N. M. Holovetskyi SYSTEM AND NETWORK MONITORING SOFTWARE SOLUTIONS	118
Н. О. Гладовський ВИЯВЛЕННЯ НЕСПРАВНИХ ПАРАМЕТРІВ У ХОДІ МОНІТОРИНГУ МЕРЕЖІ N. M. Holovetskyi DETECTION OF FAULTY PARAMETERS DURING NETWORK MONITORING	119
Н. М. Головецький УПРАВЛІННЯ ПРИСТРОЯМИ В ЛОКАЛЬНИЙ M2M МЕРЕЖІ N. M. Holovetskyi DEVICE MANAGEMENT IN A LOCAL M2M NETWORK	120
Л. П. Дмитроца, О. Т. Старицький ОПТИМІЗАЦІЯ ПРОДУКТИВНОСТІ ТА SEO ПРИ МАСШТАБУВАННІ ПРОЄКТІВ НА ОСНОВІ REACT I NEXT.JS L. P. Dmytrotsa, O. T. Starytskyi OPTIMIZING PERFORMANCE AND SEO WHEN SCALING PROJECTS BASED ON REACT AND NEXT.JS	121
М. В. Дрогобицький, А. І. Фіалка, Н. С. Луцьк МЕТОДИ ВИКОРИСТАННЯ МЕРЕЖ MICROGRID ДЛЯ ДИНАМІЧНОГО БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ЗАГАЛЬНИХ ЕЛЕКТРИЧНИХ МЕРЕЖ M. V. Drohobytzkyi, A. I. Fialka, N. S. Lutsyk METHODS OF USING MICROGRID NETWORKS FOR DYNAMIC LOAD BALANCING OF GENERAL ELECTRICAL GRIDS	123
Р. О. Жаровський, В. А. Іваницький GSM-СИГНАЛІЗАЦІЯ ЯК СПОСІБ РОЗШИРЕННЯ ФУНКЦІОНАЛЬНОСТІ РОЗУМНИХ БУДИНКІВ ТА ПІДВИЩЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ НЕРУХОМОСТІ R. O. Zharovskiy, V. A. Ivanytskyi GSM-ALARM AS A WAY OF SMART HOUSE FUNCTIONALITY EXTENDING AND PROPERTY'S SAFETY INCREASING	124

УДК 004.3

Жаровський Р.О. канд. техн. наук, Іваницький В.А.

Тернопільський національний технічний університет імені Івана Пулюя

GSM-СИГНАЛІЗАЦІЯ ЯК СПОСІБ РОЗШИРЕННЯ ФУНКЦІОНАЛЬНОСТІ РОЗУМНИХ БУДИНКІВ ТА ПІДВИЩЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ НЕРУХОМОСТІ

Zharovskiy R.O. PhD., Ivanytskyi V.A.

GSM-ALARM AS A WAY OF SMART HOUSE FUNCTIONALITY EXTENDING AND PROPERTY'S SAFETY INCREASING

GSM -сигналізація відноситься до класу охоронних систем та базується на використанні мобільного зв'язу. У таких системах передбачається надсилання сигналу-сповіщення на смартфон з метою попередження власника фізичного стаціонарного об'єкту про виникнення небезпечних подій. Передача даних від GSM-сигналізації відбувається на основі цифрового стандарту стільникового зв'язу.

Типова структура при організації GSM-сигналізації передбачає використання центрального блоку управління, який може бути реалізований за допомогою Raspberry PI, Arduino чи інших мікроконтролерів, GSM-модуля і сенсорів руху. Окрім цього, до пристрою керування GSM-сигналізацією можуть підключатися бездротові датчики газу та диму, сенсори розбиття скла чи відкриття дверей. Зазвичай, класичні системи безпеки подають сигнал тривоги у форматі SMS-повідомлення безпосередньо на мобільний телефон власника стаціонарного фізичного об'єкту.

Системи на базі GSM-технологій володіють і забезпечують гнучкість налаштування параметрів. Зокрема, можна реалізовувати режим оповіщення про пожежу у приміщенні, пожежу рухомих об'єктів, витік газу. Важливою також є функція одночасного надсилання повідомлень на мобільні телефони кількох адресатів, список яких налаштовується власником GSM-сигналізації. Інтеграція GSM-сигналізації у проєктах розумного будинку дає можливість значно підвищити функціональність, комфорт та безпеку таких рішень. Одна охоронна система на основі технології GSM може забезпечити контроль різних зон у квартирі чи будинку з ідентифікацією того, який конкретно компонент системи надіслав сигнал про порушення простору.

Для віддаленого керування систем, базованих на GSM-технології, використовуються додатки, які можна встановлювати на смартфон, а при реалізації охоронних систем важливо враховувати фактор розміру фізичного об'єкта, оскільки потрібно визначити кількість необхідних сенсорів.

Сучасні технології дозволяють GSM-системі функціонувати у наступних режимах:

- сповіщення власників – режим при якому передається повідомлення усім абонентам, які наявні у списку користувачів сигналізації
- локальне масове сповіщення – режим, який налаштовується у випадку виникнення пожежі або диму з додатковою комунікацією з системою сирен або підсвітки евакуаційних виходів;
- увімкнення заданих і додаткових систем – охоронна система на основі GSM-технології може паралельно працювати з системою вентиляції, пожежогасіння, газопостачання та водопостачання і керуватися GSM-сигналізацією.

Враховуючи високі функціональні можливості GSM базованих інструментів можна забезпечити повний захист будь-якої нерухомості.

Р. О. Жаровський, В. А. Іваницький ОРГАНІЗАЦІЯ ЗАХИСТУ СТАЦІОНАРНОГО ОБ'ЄКТУ НЕРУХОМОСТІ НА ОСНОВІ GSM-СИГНАЛІЗАЦІЇ ТА МІКРОКОНТРОЛЕРА RASPBERRY PI R. O. Zharovskyi, V. A. Ivanytskyi ORGANIZATION OF SAFETY OF A STATIONARY PROPERTY OBJECT BASED ON GSM-SIGNALIZATION AND RASPBERRY PI	125
Р. О. Жаровський, І. П. Цірка ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ ПРИ РЕАЛІЗАЦІЇ МЕРЕЖІ ЗБОРУ, ПЕРЕДАЧІ ТА АНАЛІЗУ ДАНИХ ВОДОСПОЖИВАННЯ R. O. Zharovskyi, I. P. Tsirka DATA TRANSMISSION TECHNOLOGIES IN THE IMPLEMENTATION OF A NETWORK FOR COLLECTION, TRANSMISSION AND ANALYSIS OF WATER CONSUMPTION DATA	126
Р. О. Жаровський, І. В. Марценюк, А. М. Паламар СТРУКТУРА АВТОМАТИЗОВАНОЇ ІОТ-СИСТЕМИ ДЛЯ МОНІТОРИНГУ КОНЦЕНТРАЦІЇ МЕТАНУ В ШАХТАХ R. O. Zharovskyi, I. V. Martseniuk, A. M. Palamar STRUCTURE OF AN AUTOMATED IOT SYSTEM FOR MONITORING METHANE CONCENTRATION IN MINES	127
Д. Ключко, Ю. Лещишин, Р. Жаровський КОМП'ЮТЕРНА СИСТЕМА МОНІТОРИНГУ СЕЙСМІЧНОЇ АКТИВНОСТІ ЗЕМНОЇ КОРИ D. Klochko, Y. Leshchyshyn, R. Zharovskyi COMPUTER SYSTEM FOR MONITORING SEISMIC ACTIVITY OF THE EARTH'S CRUST	128
Д. М. Козак, Н. Б. Стадник ДОСЛІДЖЕННЯ СТАНДАРТІВ ФІЗИЧНОГО РІВНЯ WI-FI D. M. Kozak, N. B. Stadnyk RESEARCH OF WI-FI PHYSICAL LAYER STANDARDS	129
Д. М. Козак, Н. Б. Стадник МЕТОДИ МАНІПУЛЯЦІЇ СИГНАЛОМ У БЕЗДРОТОВОМУ ЗВ'ЯЗКУ D. M. Kozak, N. B. Stadnyk KEYING METHODS OF SYGNAL IN WIRELESS COMMUNICATION	130
М. В. Козачок, С. В. Марценко ДОСЛІДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНКЛЮЗИВНОЇ ОСВІТИ M. V. Kozachok, S. V. Martsenko RESEARCH OF TELECOMMUNICATION TECHNOLOGIES FOR INCLUSIVE EDUCATION	131
О. В. Крайник ВИМОГИ ДО БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ O. V. Krainyk REQUIREMENTS FOR WIRELESS SENSOR NETWORKS	132
О. В. Крайник ZIGBEE GREEN POWER O. V. Krainyk ZIGBEE GREEN POWER	133
І. О. Кухар, Г. М. Осухівська ІНТЕГРАЦІЯ СОЛЯЧНИХ ЕЛЕКТРОСТАНЦІЙ У SMART GRID: СУЧАСНІ РІШЕННЯ ТА ГЛОБАЛЬНІ ТРЕНДИ I. O. Kukhar, H. Osukhivska INTEGRATION OF SOLAR POWER PLANTS INTO SMART GRIDS: MODERN SOLUTIONS AND GLOBAL TRENDS	134

УДК 004.3

Жаровський Р.О. канд. техн. наук, Іванницький В.А.

Тернопільський національний технічний університет імені Івана Пулюя

ОРГАНІЗАЦІЯ ЗАХИСТУ СТАЦІОНАРНОГО ОБ'ЄКТУ НЕРУХОМОСТІ НА ОСНОВІ GSM-СИГНАЛІЗАЦІЇ ТА МІКРОКОНТРОЛЕРА RASPBERRY PI

Zharovskiy R. PhD., Ivanytskyi V.

ORGANIZATION OF SAFETY OF A STATIONARY PROPERTY OBJECT BASED ON GSM-SIGNALIZATION AND RASPBERRY PI

Розвиток ІТ-технологій, окрім благородної мети, може вносити у суспільство багато нових загроз. У зв'язку з цим доцільно постійно вдосконалювати розумні комп'ютерні системи, орієнтовані на підвищення рівня безпеки кожної людини шляхом довіри і підтвердження надійності нових технологій.

Одним із таких способів є організація автоматизованих систем безпеки та охоронної сигналізації під керуванням GSM. Система блокування дверей з сервоприводом, що дозволяє блокувати входи/виходи всередині приміщення, є додатковою перевагою. Як тільки датчик розмикається, власник отримує дзвінок і через кілька хвилин всі двері в будинку будуть замкнені на окремий замок. Така система функціонує надійно, оскільки завжди наявний доступ до Інтернету.

Система розумного будинку на базі GSM і Bluetooth забезпечує визначену функціональність за низькою ціною і водночас не ставить під загрозу безпеку. Основним контролером управління у таких системах є Arduino. Проте точність передачі даних є не надто високою, а її складна інтеграція при підключенні аудіодинаміків споживає величезну енергію. Щоб уникнути цього, пропонується альтернативна система сповіщення на основі Raspberry Pi. На рис. 1 показано архітектуру пропонуваного рішення.

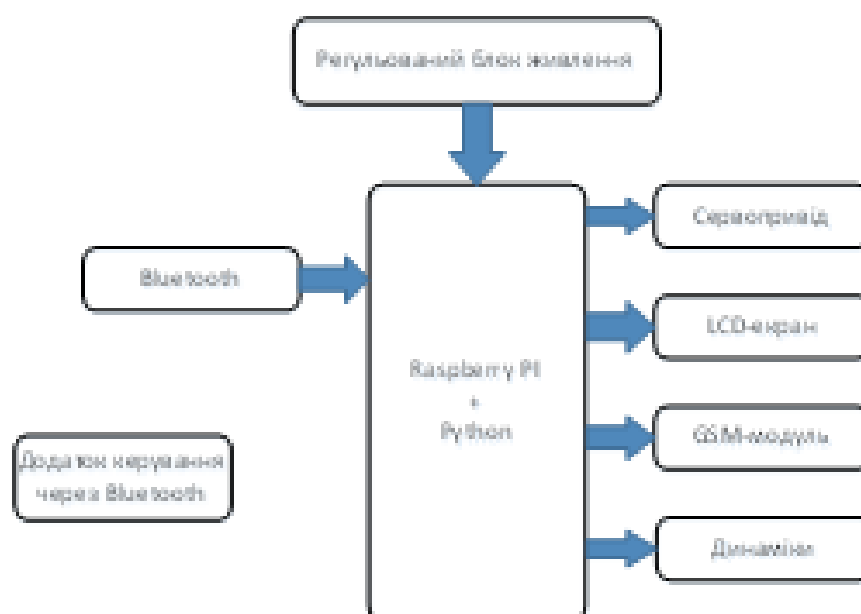


Рис. 1. Архітектура системи захисту стаціонарних об'єктів на основі Raspberry Pi