Хмельницький національний університет
Факультет інформаційних технології
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi
Назва теми

КвРКІ.2001136.12.09.01 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Комп'ютерна інженерія та програмування»
Назва

Виконав: студент III курсу, група КІ2с–20–1 _____ М.М. Мевх
Підпис — Ініціали, прізвище

Керівник _____ В.В. Яцків
Підпис, дата — Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата — Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Т.О. Говорущенко
Підпис — Ініціали, прізвище

«01» червня 2023 р.

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"11" 04 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Мевху Максиму Миколайовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi

Керівник проекту (роботи) Яцків В.В., професор кафедри КІІС

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.03.2023 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 07.06.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Концепція кіберфізичних систем та аналіз відомих засобів та рішень

Проєктування кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією

Реалізація кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Креслення сценаріїв пожежної та охоронної сигналізації з фотофіксацією у Node-red

Схема електрична принципова

Монтажна схема

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_11_»_____01_____2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2023	виконан
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2023	виконан
3	Робота над розділом 1 – Концепція кіберфізичних систем та аналіз відомих засобів та рішень	01.03.2023	виконан
4	Робота над розділом 2 – Проєктування кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією	01.04.2023	виконан
5	Робота над розділом 3 – Реалізація кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією	30.04.2023	виконан
6	Оформлення пояснювальної записки згідно вимог	20.05.2023	виконан
7	Попередній захист ВКР	26.05.2023	виконан
8	Захист ВКР на засіданні ЕК	Червень 2023 року	

Студент Підпис Мевх М.М. Ініціали, прізвище

Керівник проекту (роботи) Підпис Яцків В.В. Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ. 2001136.12.09.01ПЗ	Пояснювальна записка	55		
			Графічні матеріали			
2		КвРКІ. 2001136.12.09.01Е8	Креслення сценаріїв	1		
			пожежної та охоронної			
			сигналізації з			
			фотофіксацією у Node-red			
3		КвРКІ. 2001136.12.09.01Е2	Схема електрична	1		
			принципова			
4		КвРКІ. 2001136.12.09.01 Е4	Монтажна схема	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ. 2001136.12.09.01 ПЗ		
Розробив		Мевх М.М.			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Яцків В.В				У	1	1
Н. контр.		Лисенко С.М.				ХНУ, КІ2с-20-1		
Затв.		Говорущенко		02.06				

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi».

Автор роботи: *Мевх Максим Миколайович.*

Керівник роботи: *Яцків Василь Васильович.*

Пояснювальна записка: *55 с.*, 43 *рис.*, 4 *табл.*, 3 *дод.*, 49 *джерел.*

Графічна частина: 3 креслення.

КІБЕРФІЗИЧНА СИСТЕМА, ФОТОФІКСАЦІЯ, ОПОВІЩЕННЯ, СЦЕНАРІЙ.

Мета кваліфікаційної роботи: розробка кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi.

Тема створення кіберфізичної системи охоронної та пожежної сигналізації із фотофіксацією є дуже актуальною в сучасному світі. Зростаюча кількість різних злочинів, крадіжок, пограбувань та пожеж вимагає використання новітніх технологій для забезпечення безпеки майна та життя людей.

Кіберфізична система охоронної та пожежної сигналізації із фотофіксацією поєднує в собі різні технології, такі як інтернет речей, машинне навчання та обробку зображень. Ця система забезпечує постійний моніторинг об'єкта та автоматичне сповіщення про будь-які події, які можуть статися, такі як вторгнення чи пожежа. Інтеграція такої системи із системою повіщення дозволить реалізувати надсилання сигналів тривоги до екстрених служб, що дозволить у найкоротші терміни виявити проблему.

Підпис студента _____ Дата 05.06.2023

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ 4
ВСТУП 5
1 КОНЦЕПЦІЯ КІБЕРФІЗИЧНИХ СИСТЕМ ТА АНАЛІЗ ВІДОМИХ ЗАСОБІВ Й РІШЕНЬ ДЛЯ ОХОРОННОЇ ТА ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ 7
1.1 Концепція та принципи функціонування кіберфізичних систем 7
1.2 MQTT протокол передачі даних у кіберфізичних ситемах та мережах Інтернету речей 10
1.3 Обладнання та засоби охоронної та пожежної сигналізації 12
1.4 Огляд існуючих засобів та систем із функцією охоронної та пожежної сигналізації 15
1.5Постановка задачі 20
2 ПРОЄКТУВАННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ПОЖЕЖНОЇ ТА ОХОРОННОЇ СИГНАЛІЗАЦІЇ ІЗ ФОТОФІКСАЦІЄЮ НА БАЗІ RASPBERRY PI 21
2.1 Вимоги до кіберфізичної системи пожежної та охоронної сигналізації із фото фіксацією на базі Rasperry Pi 21
2.2 Структура кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією на базі Rasperry Pi 22
2.3 Аналіз обраних рішень 25
2.3.1 Аналіз обраних апаратних рішень 26
2.3.2 Аналіз обраних програмних рішень 34
2.4 Висновки до розділу 2 36
3 РЕАЛІЗАЦІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ПОЖЕЖНОЇ ТА ОХОРОННОЇ СИГНАЛІЗАЦІЇ ІЗ ФУНКЦІЄЮ ФОТОФІКСАЦІЇ НА БАЗІ RASPBERRY PI 37
3.1 Встановлення та підготовка середовища Node-RED та брокера mosquitto 37
3.2 Монтажна схема кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією 39

3.3 Принципова схема і схема розведення провідників на макетній платі 41
3.4 Реалізація сценаріїв пожежної та охоронної сигналізації із реалізацією функції фотофіксації у Node red 43
3.4.1 Сценарій ідентифікації проникнення у приміщення із фотофіксацією та ропізнаванням 43
3.4.2 Сценарій пожежної сигналізації із фотофіксацією 52
3.5 Висновки за розділом 3 58
ВИСНОВКИ 59
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 61
ДОДАТОК А Креслення сценаріїв пожежної та охоронної сигналізації з фотофіксацією у Node-red 67
ДОДАТОК Б Схема електрична принципова 68
ДОДАТОК В Монтажна схема 69

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АЦП – Аналого-цифровий перетворювач

ІТ – Інформаційна технологія

КС – Комп’ютерна система

КФС – Кібер-фізична система

ОПС – Охоронно-пожежна сигналізація

ПЗ – Програмне забезпечення

ЦАП – Цифро-аналоговий перетворювач

MQTT – Message queuing telemetry transport

RPi – Raspbery Pi

ВСТУП

Тема створення кіберфізичної системи охоронної та пожежної сигналізації із фотофіксацією є дуже актуальною в сучасному світі. Зростаюча кількість різних злочинів, крадіжок, пограбувань та пожеж вимагає використання новітніх технологій для забезпечення безпеки майна та життя людей.

Кіберфізична система охоронної та пожежної сигналізації із фотофіксацією поєднує в собі різні технології, такі як інтернет речей, машинне навчання та обробку зображень. Ця система забезпечує постійний моніторинг об'єкта та автоматичне сповіщення про будь-які події, які можуть статися, такі як вторгнення чи пожежа. Інтеграція такої системи із системою повіщення дозволить реалізувати надсилання сигналів тривоги до екстрених служб, що дозволить у найкоротші терміни виявити проблему.

Ключовою частиною кіберфізичної системи охоронної та пожежної сигналізації є реалізація функції фотофіксації, оскільки вона дозволяє збирати та аналізувати зображення з об'єкта, що підлягає охороні. Фотофіксація, яка є частиною системи, дозволяє фіксувати зображення об'єкту та подій, що відбуваються на ньому. Це дозволяє оперативно реагувати на будь-які випадки та швидко встановлювати винних. Окрім того дозволяє збирати зображення з об’єкта та відстежувати будь-які незвичайні події, які можуть бути пов'язані з вторгненням або крадіжкою. Це допомагає оперативно виявляти злочинців та діяти відповідним чином.

Окрім охоронної сигналізації фотофіксація дозволяє виявляти пожежу на ранніх стадіях та оперативно реагувати на неї. Збір зображень із об’єкта дозволяє визначити точне місце та масштаб пожежі, а також стан пожежогасіння. І нарешті фотофіксація забезпечує зберігання доказів про будь-які небезпечні події або злочини, які можуть відбутися на об’єкті спостереження, що може допомогти у подальшому при розслідуванні інцидентів.

Отже, створення кіберфізичної системи охоронної та пожежної сигналізації із фотофіксацією є дуже актуальним зараз, коли безпека майна та життя стає все більш важливою темою для багатьох людей.

Метою роботи є розробка кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi.

Об’єктом дослідження є процеси ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням, а також реалізації пожежної сигналізації із фотофіксацією.

Предметом дослідження є кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi.

1 КОНЦЕПЦІЯ КІБЕРФІЗИЧНИХ СИСТЕМ ТА АНАЛІЗ ВІДОМИХ ЗАСОБІВ Й РІШЕНЬ ДЛЯ ОХОРОННОЇ ТА ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ

1.1 Концепція та принципи функціонування кіберфізичних систем

Четверта промислова революція відрила дві основні концепції – «Інтернет речей» та «Кіберфізична система». Ці поняття характеризують тісним зв'язком, де в багатьох випадках чітко розмежувати ці поняття не завжди вдається.

Поняття «кіберфізична система» зазвичай використовується інженерними спільнотами (наприклад, машинобудування, аерокосмічна техніка, аеронавтика), а також інформатиками, що працюють над вбудованими системами та системами тестування та перевірки.

«IoT» або «Інтернет речей» зазвичай використовується телекомунікаційними та мережевими спільнотами, включаючи інформатиків, які працюють у більш широких сферах впровадження та розроблення технології мереж нового покоління.

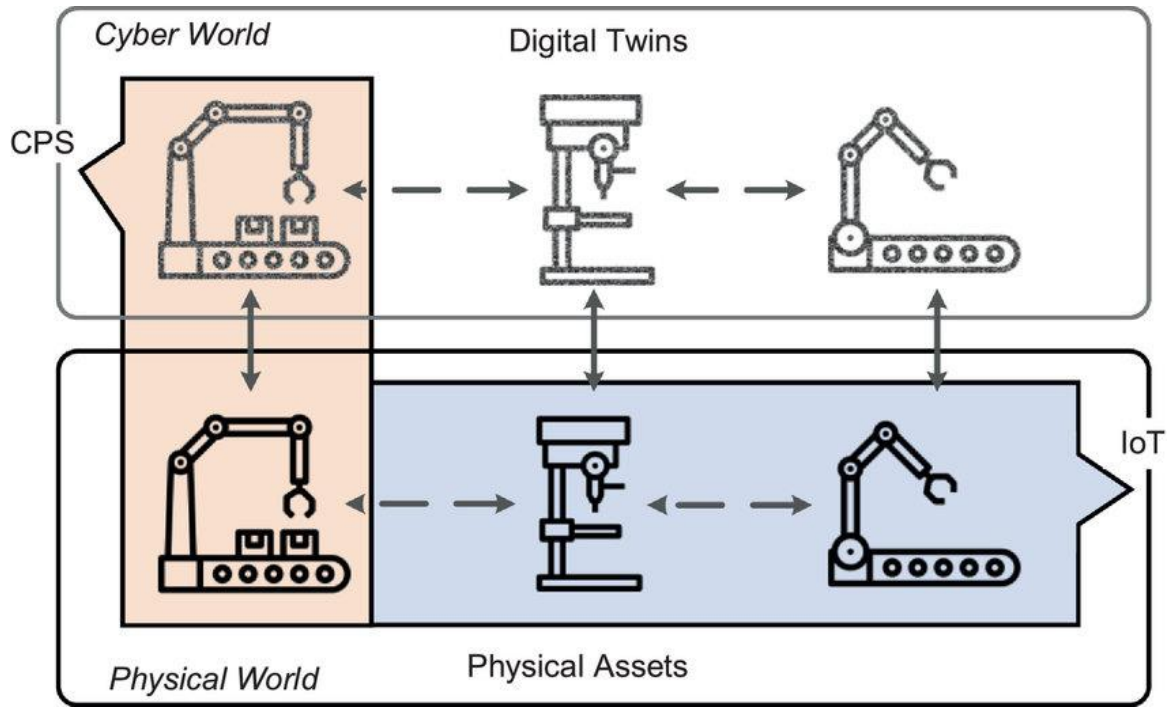


Рисунок 1.1 – Рівні абстракції для IoT та CPS

В більш вузькому понятті IoT розглядається як мережа поєднаних пристроїв, в той час як “кіберфізична система” – це система як дозволяє моніторити та контролювати виробничі процеси, і яка може включати в себе Internet of Things. Можна вважати, що Інтернет речей є одним із екземплярів кіберфізичних систем. Принциповою відмінністю між цими поняттями можна вважати те, що в якості об’єкта прийняття рішення в кіберфізичних системах виступає комп’ютер, в той час як у IoT – людина.

Кіберфізична система – це система, яка інтегрує обчислювальні елементи із фізичними компонентами та процесами. Обчислювальні елементи координують і взаємодіють із датчиками, які контролюють кібер- та фізичні показники, та виконавчими механізмами (або актуаторами), які модифікують кібер- та фізичне середовище (впливають на зовнішнє середовище). Кіберфізичні системи використовують датчики для підключення всього розподіленого інтелекту в навколишньому середовищі, щоб отримати глибші знання про навколишнє середовище, що дає змогу виконувати більш точніші дії та завдання. Іншими словами кіберфізична система це інформаційно-технологічна концепція, що передбачає інтеграцію обчислювальних ресурсів в фізичні сутності будь-якого виду, включаючи біологічні та рукотворні об’єкти. У кіберфізичних системах обчислювальна компонента розподілена по всій фізичній системі, яка є її носієм, і синергетично звя’зана з її складовими елементами, утворюючи одне ціле.

В кіберфізичних системах вбудовані комп’ютери та мережі контролюють і управляють фізичні процеси, включаючи цикли зворотного зв'язку, де фізичні процеси впливають на обчислення і навпаки (рис. 1.2). Отже, проектування таких систем вимагає розуміння спільної динаміки комп’ютерів, програмного забезпечення, мереж та фізичних процесів. Кібер-фізичні системи поєднують в собі кібер- можливості з фізичними можливостями для вирішення проблем, які жодна частина не могла б вирішити поодинці.

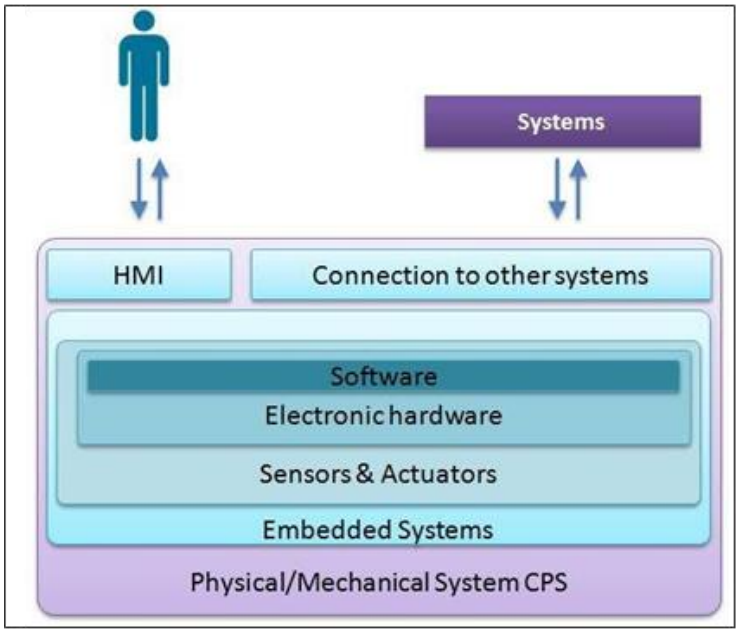


Рисунок 1.2 – Взаємодія людини та машин за посередництва кіберфізичної системи

Кіберфізичні системи, як правило, включають мережу пристроїв, які приймають і виконують фізичні дії, які одночасно контролюються та моніторяться програмним забезпечення КФС. Кіберфізичні системи можна розглядати як інтеграцію вбудованих систем, датчиків, мереж зв'язку та систем управління (рис.1.3). Основна мета використання кіберінфраструктури (включаючи апаратне та програмне забезпечення давачів, обчислювальної техніки та зв'язку) – це моніторинг (від фізичного до кібер світу) та контроль (від кібер до фізичного світу).

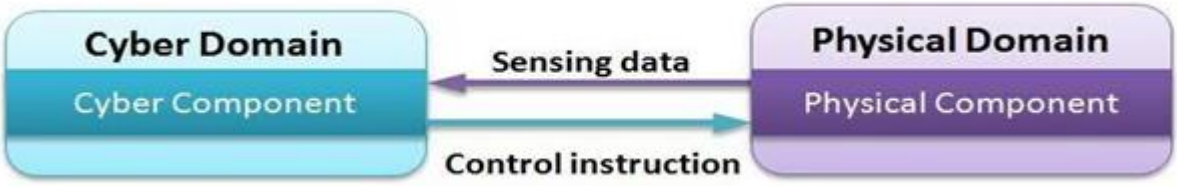


Рисунок 1.3 – Процес взаємодії фізичної та кібер складової в КФС

Кіберфізичні системи можуть бути використані в різних сферах, включаючи автомобільну промисловість, медицину, енергетику, транспорт, сільське господарство, виробництво та інші.

Такі системи можуть забезпечувати автоматизацію процесів, зменшення витрат, підвищення продуктивності та ефективності, а також поліпшення безпеки і зниження ризику виникнення аварійних ситуацій. Однією з важливих характеристик кіберфізичних систем є їх здатність до взаємодії з користувачами та іншими системами в режимі реального часу.

Як підсумок можна відзначити, що залучення кіберфізичних систем у існуючі технологічні процеси має наступні переваги:

– Ефективність: КФС дозволяють забезпечити автоматизацію та оптимізацію фізичних процесів, що призводить до зниження витрат на енергію та матеріали.

– Надійність: КФС можуть виявляти та локалізувати помилки та несправності у системах, що дозволяє вчасно їх виправити та запобігти аваріям.

– Безпека: КФС дозволяють стежити за процесами, що відбуваються в системах та реагувати на загрози в режимі реального часу.

– Гнучкість: КФС можуть бути змінені та адаптовані до змінних умов роботи, що дозволяє швидко реагувати на зміни в середовищі.

– Інновації: КФС відкривають нові можливості для розробки нових продуктів та послуг, що раніше були неможливі.

Усі ці переваги дозволяють підвищити ефективність та якість роботи систем, знизити витрати, автоматизувати процес функціонування та забезпечити безпеку працівників та споживачів.

1.2 MQTT протокол передачі даних у кіберфізичних ситемах та мережах Інтернету речей

MQTT протокол широко використовується в кіберфізичних системах для забезпечення зв'язку між різними пристроями, такими як датчики, контролери та інші елементи системи. Цей протокол дозволяє забезпечити масштабовану та надійну передачу даних між пристроями, що допомагає забезпечити ефективну та безперебійну роботу кіберфізичних систем.

У кіберфізичних системах MQTT протокол може використовуватись для передачі різних типів даних, таких як температура, вологість, тиск, рівень сигналу та інші параметри, що вимірюються датчиками. Цей протокол також може використовуватись для керування пристроями та виконання різних команд.

MQTT протокол був розроблений для забезпечення ефективної та надійної передачі повідомлень в мережах з низькою пропускною здатністю та незначною затримкою. Цей протокол дозволяє пристроям відправляти та отримувати повідомлення з мінімальними витратами ресурсів та енергії.

Спочатку MQTT був розроблений у 1999 році, який в основному використовувався в нафтовій і газовій промисловості. Однак до сьогодні він широко використовувався в багатьох програмах, таких як домашня автоматизація та Facebook Messenger. MQTT – це протокол зв'язку «багато-до-багатьох», що забезпечує обмін інформацією між кількома клієнтами. Крім того, MQTT підходить для обмежених середовищ, таких як обмежена пропускна здатність, обмежені обчислювальні можливості та низьке енергоспоживання. Таким чином, він підходить для впровадження на пристроях, які працюють від батареї. В концепції MQTT існує кілька важливих понять, зокрема: видавець, клієнт, брокер, підписник і тема (або топік).

На рис. 1.2 приведено модель зв'язку для протоколу MQTT.

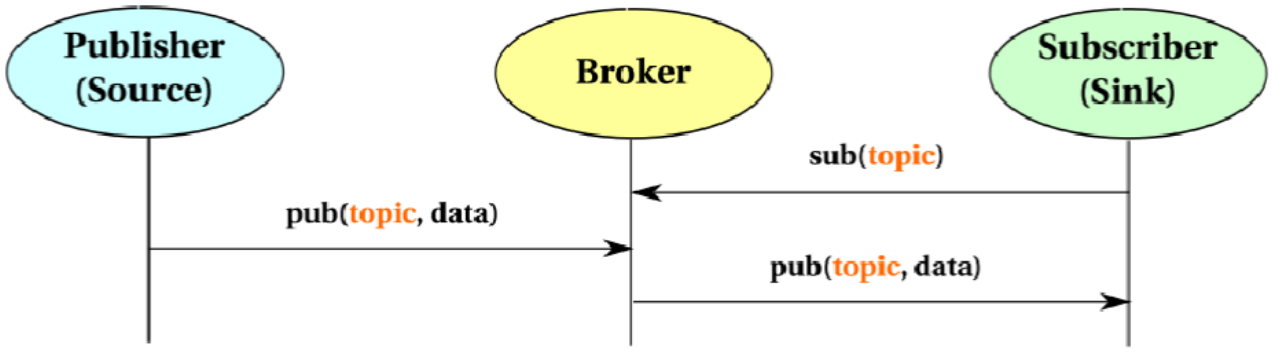


Рисунок 1.4 – Модель процесу обміну даними через MQTT протокол

І видавець, і підписники називаються клієнтами MQTT. Видавець відноситься до клієнта, який публікує повідомлення або інформацію брокеру. Абонент відноситься до клієнта який підписаний на тему, щоб отримати повідомлення. Клієнтом MQTT можуть бути будь-які пристрої, за умови, що вони можуть підключитися до брокера MQTT. В концепції «підписка-публікація» не має прямого спілкування чи зв'язку між клієнтами. Усі повідомлення будуть опубліковані й відправлені від брокера. Брокер MQTT – це програмне забезпечення, функцією якого є отримання всієї інформації та повідомлень від клієнтів. Він фільтруватиме повідомлення та надсилатиме інформацію клієнтам, які підписалися. Брокер є центром системи обміну даними. HiveMQ, AWS IoT, Mosquitto та Mosca – це деякі приклади брокерів MQTT. Наприклад, пристрій А хоче отримувати повідомлення із пристрою В. Тепер пристрій В є клієнтом публікації, а пристрій А є клієнтом підписки. Для успішної передачі інформації пристрої В і пристрої А повинні бути підписані на одну тему.

1.3 Обладнання та засоби охоронної та пожежної сигналізації

Охоронно-пожежна сигналізація (ОПС) – є складним комплексом технічного обладнання, службовця для виявлення виникнення пожежі та несанкціонованого доступу на територію, що охороняється. Для більшої ефективності ОПС об'єднують в комплекс, який складається з систем безпеки та інженерно-технічних споруд, що дозволяють забезпечити достовірною інформацією системи пожежогасіння, оповіщення, димовидалення, контролю проходу та інші. З'єднання пожежної та охоронної сигналізації в єдиний комплекс відбувається на рівні централізованого управління. При цьому ці системи управляються автономними постами управління, що зберігають свою незалежність у складі загальної системи сигналізації. Залежно від виконуваних завдань, у складі сигналізації може складатися устаткування трьох основних категорій: система пожежної сигналізації призначається для своєчасного

виявлення місця спалаху та генерації сигналів для систем сповіщення про пожежу, й включення установок автоматичного пожежогасіння, димовидалення; система охоронної сигналізації реалізує завдання оповіщення співробітників служби охорони про факт, або спроби проникнення сторонніх на об'єкт охорони з фіксуванням дати, часу й місця події порушення; для оповіщення про нештатну ситуацію на об'єкті в обладнання охоронно-пожежної сигналізації включені сповіщувачі. Вони відрізняються типом контрольованих параметрів, принципом функціонування чутливого елемента, способами передачі сигналу тривоги на централізований пульт управління.

Рисунок 1.5 – Датчик газу від Xiaomi

За принципами формування сигналу про проникнення в охоронну зону, або загоряння сповіщувачі сигналізації поділяються на активні та пасивні. Широко поширені такі типи охоронних сповіщувачів як: пасивні інфрачервоні, датчики розбиття скла, магнітоконтактні датчики, периметральні датчики, а також комбіновані активні сповіщувачі.

За принципами формування сигналу про проникнення в охоронну зону, або загоряння сповіщувачі сигналізації діляться на активні та пасивні. Широко

поширені такі типи охоронних сповіщувачів, як пасивні інфрачервоні, датчики розбиття скла, магнітоконтактні датчики, периметральні датчики, а також комбіновані активні сповіщувачі.

У системах пожежної сигналізації використовують такі засоби охоронно-пожежної сигналізації як димові, теплові, іонізаційні, світлові, комбіновані ручні сповіщувачі.

Для обробки одержуваних сигналів в охоронно-пожежної сигналізації використовуються різні типи контрольного обладнання: контрольні панелі, центральні станції, приймально-контрольні прилади. Ця апаратна частина володіє різною інформаційної ємністю – числом шлейфів сигналізації, ступенем функцій оповіщення та управління. Все обладнання охоронно-пожежної сигналізації повинно бути забезпечено безперебійним електроживленням. Згідно державним нормам пожежної безпеки, сигналізація повинна функціонувати у разі зникнення електроживлення на об'єкті не менше доби в черговому режимі та до 3-х годин у тривожному режимі. Тому, для проходження цій вимозі, сигналізація повинна мати джерела запасного електроживлення.

На сьогоднішній день на ринку існує багато компаній, які виробляють інтелектуальне обладнання для охоронної та пожежної сигналізації. Деякі з найвідоміших компаній цього ринку:

– Honeywell - компанія, що пропонує інтелектуальні системи безпеки для підприємств та домогосподарств.

– Bosch Security and Safety Systems - компанія, що пропонує інтелектуальні системи безпеки для офісів, магазинів та інших приміщень.

– Siemens Building Technologies - компанія, що пропонує інтелектуальні системи безпеки для будівель та інфраструктури;.

– Tyco Security Products - компанія, що пропонує інтелектуальні системи безпеки для промислових та комерційних об'єктів.

– Hikvision - компанія, що пропонує інтелектуальні системи відеоспостереження та безпеки для різноманітних об'єктів.

– Johnson Controls - компанія, що пропонує інтелектуальні системи безпеки для промисловості, комерції та житлового будівництва.

– Xiaomi - компанія, що спеціалізується на виробництві побутової техніки та інтелектуальних пристроїв.

– ADT - компанія, що пропонує інтелектуальні системи безпеки для домогосподарств та бізнесу.

Ці компанії мають широкий асортимент продуктів та послуг, що дозволяє задовольнити потреби клієнтів з різних галузей.

1.4 Огляд існуючих засобів та систем із функцією охоронної та пожежної сигналізації

Огляд досліджень [1-16] показав, що основним компонентом, на базі якого здійснюється проектування недорогих систем із функцією охоронної та пожежної сигналізації є одноплатна комп'ютерна система Raspberry Pi. На це є декілька актуальних причин:

– Покращення безпеки: така система дозволяє відстежувати події та захищати приміщення від злочинів та пожеж.

– Економія коштів: Raspberry Pi є дешевим та компактним пристроєм, який може бути використаний для створення невеликих систем за низькою ціною.

– Легкість у використанні: Raspberry Pi має простий інтерфейс та підтримує безліч додатків та бібліотек, що робить його ідеальним вибором для розробки кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією.

– Гнучкість: Raspberry Pi дозволяє розширювати та налаштовувати систему залежно від потреб користувача. Це дозволяє створювати спеціалізовані системи, які відповідають конкретним потребам та завданням.

– Можливості обробки зображень: Raspberry Pi має вбудовану можливість обробки зображень, що дозволяє реалізувати фотофіксацію високої якості, що допомагає ідентифікувати та відстежувати події.

Розглянемо детальніше деякі запропоновані підходи.

У роботі [1] запропоновано веб-систему відеоспостереження на основі Raspberry Pi. Окрім Raspberry Pi система складалась із камери Pi, датчика руху PIR, ультразвукового датчика, веб-додатків і мобільних додатків. Використання Raspberry Pi надало можливість керувати детекторами руху, відстанню до зловмисників і відеокамерами для дистанційного зондування та спостереження. Камери автоматично транслюють відео в реальному часі, а пристрій Raspberry Pi надсилав сповіщення електронною поштою та SMS на комп'ютер або мобільний пристрій власника веб-систему відеоспостереження. Запропоноване рішення є економічно ефективним у порівнянні з іншими продуктами комерційних систем відеоспостереження, такими як CCTV, IP-камери тощо. Проте, дана система не здатна реагувати та сповіщати користувачів на появу осердку вогнища.

Інтелектуальна система відеоспостереження, що використовує мережу датчиків PIR та gsm модулів була представлена у роботі [2]. Система використовувала датчик PIR та відеокамеру на базі PIC контролера. PIC є недорогим, простим у програмуванні та може контролювати всі компоненти з невеликими обчислювальними вимогами.

У роботі [3] запропоновано система пожежної сигналізації , що функціонує в режимі реального часу та яка виявляє наявність диму в повітрі спричененого пожежою та фіксує зображення за допомогою камери, встановленої всередині приміщення, коли виникає пожежа. Для розробки цієї системи використані вбудовані системи Raspberry Pi та Arduino Uno. Особливістю системи є можливість дистанційного сповіщення при виявленні пожежі. Коли буде виявлено наявність диму, система відобразить зображення стану приміщення на веб-сторінці. Системі знадобиться підтвердження

користувача, щоб повідомити про подію пожежникам за допомогою служби коротких повідомлень (SMS).

У роботі [4] автори запропоновували роботизовану систему відстеження появи пожежі. Основними апаратними компонентами, що були задіяні для розробки системи були raspberry pi3 та Arduino mega, GSM модуль для надсилання повідомлень, датчики полум'я та газу використовуються для виявлення полум'я та диму або газу в прилеглих областях, модуль Bluetooth і драйвер двигуна L298N з двома двигунами постійного струму. Робот має можливість рухатись залежно від голосової команди, які створюються за допомогою інвертора додатків MIT, у той же час програмне забезпечення є флеш-програмним забезпеченням для керування роботом на основі IOT та ОС raspbion для raspberry pi. Нарешті, робот може рухатися залежно від заданого напрямку, щоб виявити пожежу та витік газу та надсилати повідомлення, подаваи звуковий сигнал, а також виводити на дисплей поточне значення стану та датчиків роботизовано системи.

У роботі [5] запропоновано систему виявлення диму та осередку вогню на основі одноплатної комп'ютерної системи Raspberry Pi. До складу системи увійшли такі компоненти як давач диму, вогню, температури, а також модуль відтворення звуку. Для обміну даними було використано брокер Mosquitto, що встановлювався на Raspberry Pi. Запропонована система показала високу ефективність виявлення газу та вогню, проте у даній системі відсутні функції охоронної сигналізації, а також відсутній процес розпізнавання зображень, що може призвести до високого рівня помилкових спрацювань.

Таким чином проведений огляд засобів і систем із функціями охоронної та пожежної сигналізації продемонстрував, що сучасні системи досить ефективно вирішують покладені на них завдання, проте головним недоліком таких систем є відсутність розпізнавання створених зображень.

Також на риснку існують комерційні засоби пожежної та охоронної сигналізації.

Зокрема фірмою Ajax представлено комплект бездротової сигналізації Ajax StarterKit Cam Plus white (рис. 1.6). Цей комплект призначений для сигналізації та забезпечення безпеки будинку та офісу з фотоверифікацією тривог, що працює за бездротовою технологією Jeweller/Wings із підтримкою 5 каналів зв'язку – Wi-Fi, Ethernet, 2G, 3G, LTE. Інтелектуальна централь сигналізації Ajax Hub 2 Plus акумулює всі можливості кожного датчика в єдину систему. Доступ через мобільні програми з будь-якої точки світу дозволяє контролювати стан охоронної системи (постановку/зняття, мікроклімат тощо).

Бездротова технологія Jeweller дозволяє розкинути мережу на відстані до 2000 метрів на відкритому просторі або на декількох поверхах бізнес-центру. Протокол зв'язку Wings за наявності загроз надішле фотографії з датчиків руху MotionCam і викличе охорону. Для підвищення надійності система працює відразу на 5 каналах зв'язку – Wi-Fi, Ethernet, 2G, 3G, LTE. Охоронну систему можна підключити до пульту охоронної компанії. Даний пристрій підтримує підключення до 200 датчиків та до 100 камер, а також забезпечує можливість підключення до моніторингу системи до 200 користувачів.

Рисунок 1.6 – Комплект бездротової сигналізації Ajax StarterKit Cam Plus (8EU) UA white з фотоверифікацією тривог та підтримкою LTE

Ще одним коменрційним пристроєм пожежної сигналізації є Mi Smart Home Fire Detector Honeywell. Даний пристрій є бездротовим датчиком виявлення пожежі, розроблений спільно компанією Xiaomi і Honeywell. Його призначення полягає в ранньому виявленні пожежі в будинку або офісі, що дозволяє швидко ухвалити відповідні заходи для запобігання поширенню вогню та захисту майна та життя.

Основні можливості Mi Smart Home Fire Detector Honeywell включають:

– Виявлення пожежі: Датчик використовує спеціальні алгоритми та сенсори для виявлення пожежі в ранній стадії. Він реагує на зміну температури, підвищення рівня диму або наявність вогню у приміщенні.

– Звуковий сигнал: Якщо датчик виявляє загрозу пожежі, він активує вбудований звуковий сигнал, щоб попередити присутніх про небезпеку. Звуковий сигнал може досягати достатньо гучності, щоб пробудити сплячих людей або привернути увагу у віддаленому місці.

– Оповіщення через смартфон: Датчик може бути підключений до мережі Wi-Fi і спільно працювати зі смартфоном через мобільний додаток Mi Home. Користувач отримує сповіщення на свій смартфон у разі виявлення пожежі, навіть якщо він знаходиться далеко від дому.

– Підключення до інших пристроїв Mi Smart Home: Можливе інтегрування датчика пожежі з іншими пристроями Mi Smart Home, такими як розумні дзеркала, освітлення, дзвінки дверного замка тощо. Це дозволяє автоматизувати дії, наприклад, увімкнути освітлення або відкрити двері у разі виявлення пожежі.

Таким чином проведений огляд комерційних засобів пожежної та охоронної сигналізації показав, що відомі рішення володіють досить широким спектром можливостей, проте головним їх недоліком є перш за все висока вартість.

1.5 Постановка задачі

Тема створення кіберфізичної системи охоронної та пожежної сигналізації із фотофіксацією є дуже актуальною в сучасному світі. Зростаюча кількість різних злочинів, крадіжок, пограбувань та пожеж вимагає використання новітніх технологій для забезпечення безпеки майна та життя людей. Тому створення кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi є актуальним завданням.

Вирішення поставленого завдання передбачає виконання наступних етапів:

1. аналіз відомих систем та засобів, що реалізують функції пожежної та охоронної сигналізації з фотофіксацією;
2. складання вимог до кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi;
3. проєктування структури кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi;
4. проєктування монтажної схеми та схеми розведення провідників на друкованій платі для кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi;
5. реалізація сценаріїв пожежної та охоронної сигналізації із фотофіксацією у Node-Red.

2 ПРОЄКТУВАННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ПОЖЕЖНОЇ ТА ОХОРОННОЇ СИГНАЛІЗАЦІЇ ІЗ ФОТОФІКСАЦІЄЮ НА БАЗІ RASPBERRY PI

2.1 Вимоги до кіберфізичної системи пожежної та охоронної сигналізації із фото фіксацією на базі Rasperry Pi

Визначення функціональних вимог є дуже важливим етапом проєктування будь-якого програмного забезпечення або системи. Функціональні вимоги визначають, які функції повинні бути реалізовані у системі або програмному забезпеченні, тобто які задачі вони повинні виконувати. Чітко виписані вимоги дозволяють покращити ефективність та якість розробки системи.

У проєктованій кіберфізичній системі пожежної та охоронної сигналізації із фотофіксацією на базі одноплатної комп'ютерної системи Rasperry Pi повинні бути реалізовані наступні функції:

1. Ідентифікація проникнення у приміщення із фотофіксацією та ропізнаванням зображення. У випадку наявності руху у приміщенні система повинна зробити фото та виконати процес його розпізнавання. Якщо буде визначено, що на фото зображена людина, надіслати повідомлення із прикріпленим фото на електронну пошту користувача. У випадку, якщо у процесі розпізнавання зображення буде визначено інший об'єкт, наприклад, домашню тварину, оповіщення на електронну пошту надходити не повинно.

2. Ідентифікація задимленості та наявності осередку вогню із фотофіксацією. У випадку наявності задимленості, що проявляється у підвищенні рівня концентрації вуглекислого газу у повітрі, або підвищенні температури у приміщенні, кіберфізична система повинна увімкнути оповіщення, зробити фото та надіслати повідомлення із прикріпленим зображенням на електронну пошту користувача.

Також, разом із функційними вимогами, виділяють нефункційні вимоги, що описують такі характеристики системи як надійність, безпека, масштабованість, сумісність тощо.

Виділимо основні нефункційні вимоги до проєктованої кіберфізичної системи:

– Здатність до стабільного й безперебійного функціонування в умовах нормального використання (тобто умовах, що означені для складових, з яких складається кіберфізична система).

– Здатність працювати швидко та ефективно із врахуванням обсягу даних та ресурсів, які необхідні для її роботи.

– Зручність користування.

– Здатність до оновлення.

– доступність, тобто система повинна бути доступною для користувачів з різними потребами та можливостями.

– Низька вартість комплектуючих.

– Придатність до масштабованості відповідно до зростаючих потреб користувачів та обсягів даних.

Таким чином, визначені функційні та нефункційні вимоги дозволяють зрозуміти, якими функціями та характеристиками повинна володіти проєктована кіберфізична система для задоволення потреб та очікування користувачів цієї системи.

2.2 Структура кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією на базі Rasperry Pi

Для реалізації поставлених вимог до кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією на базі одноплатної комп’ютерної системи Rasperry Pi запропоновано структуру цієї системи, структурна схема якої наведена на рис. 2.1.

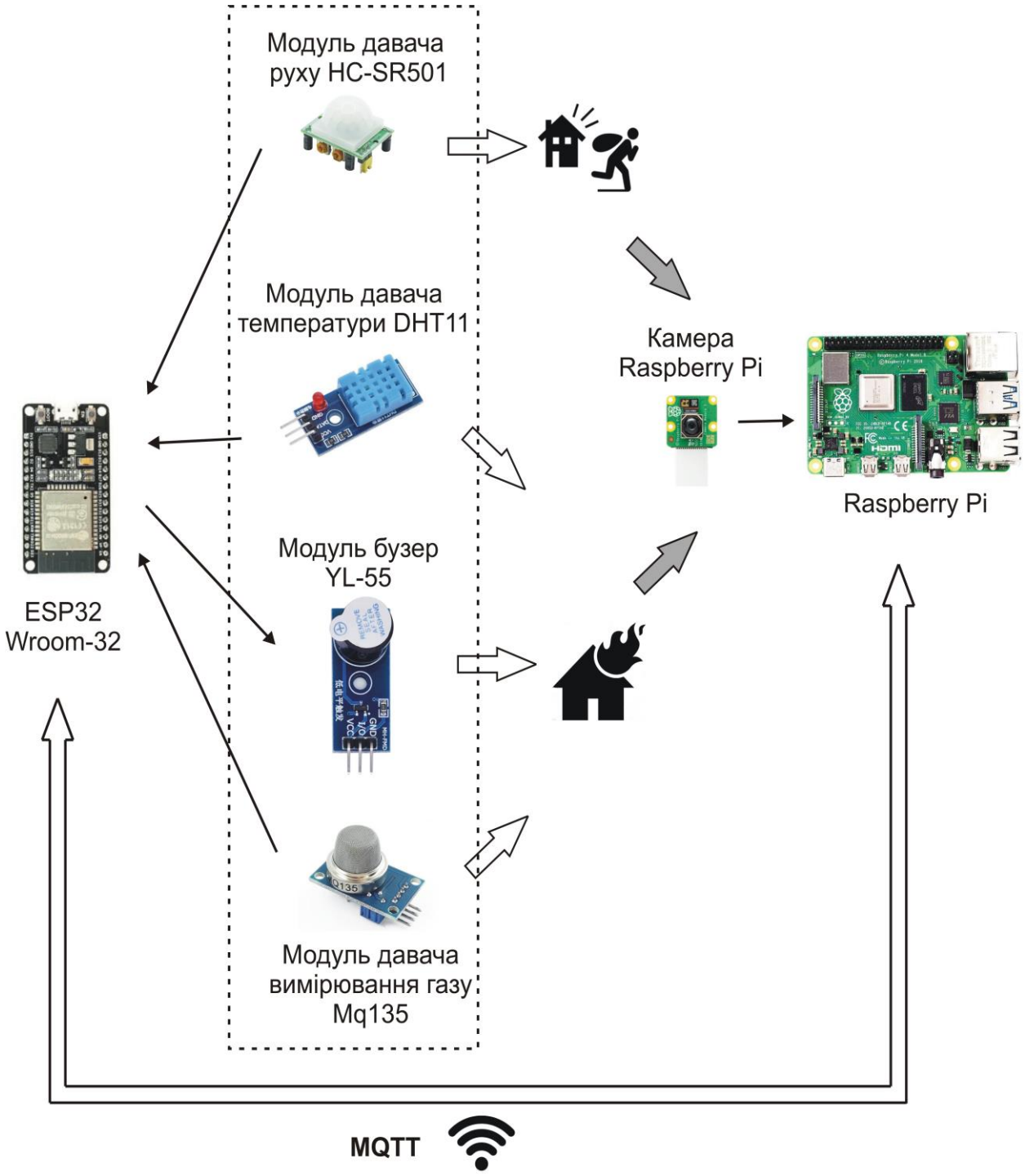


Рисунок 2.1 – Структурна схема кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi

Запропонована кіберфізичні система включає в себе такі програмні та апаратні компоненти:

– Одноплатна комп’ютерна система Raspberry Pi 3 Model B, що використовуватиметься для прийняття рішення щодо реагування на

надзвичайну ситуацію, що склалась через проникнення у приміщення або наявність осередку вогню. Конфігурація Raspberry Pi передбачала додаткове встановлення програмного забезпечення для розробки рішень Інтернету речей. Для цього було встановлено інструмент розробки Node-RED, який працює на основі потоків, а також брокер повідомлень mosquitto. Одноплатна комп'ютерна система Raspberry Pi з'єднується із системою на кристалі ESP32 через бездротовий зв'язок Wi-Fi за участю протоколу MQTT (message queuing telemetry transport). Брокер mosquitto топіки, у які здійснюється публікація даних від давачів. Для вирішення поставленого завдання у системі задіяно чотири топіки:

– home/pir – для публікації даних від давача руху.

– home/temperature – для публікації даних про температуру у приміщенні.

– home/smog – для публікації даних від давача рівня вуглекислого газу.

– home/buzzer – для публікації повідомлень, призначених для відтворення звуку модулем п'єзодинаміку.

– Давач температури буде використаний для вимірювання температури у приміщенні. Публікує дані у топік home/temperature. Публікація температури здійснюється один раз на хвилину.

– Давач вимірювання вуглекислого газу публікує дані у топік home/smog (одиниця вимірювання цієї величини ppm). Як і у випадку із температурою дані публікуються один раз на хвилину, причому вимірювання цих величин синхронізовано таким чином, щоб вони публікувались одночасно.

– Давач руху використовуватиметься для реалізації сценарію ідентифікації проникнення у приміщення із фотофіксаціює та розпізнаванням. Даний давач виконує публікацію повідомлення «on» у топік home/pir, у випадку якщо руху виявлено та «off», якщо протягом 3-х секунд руху не було виявлено.

– Модуль п'єзодинаміку буде використаний для відтворення звуку у випадку наявності осередку полум'я та/або вуглекислого газу. Кіберфізична система виконує публікацію у у топік home/buzzer повідомлення «0», якщо

відсутні ознаки пожежі, і «1» – в іншому виадку. Отримавши таке повідомлення модуль п’єзодинаміку буде або монототонно відтворювати звуу із заданою частотою або звук буде відсутній.

– Камера для Raspberry Pi використовуватиметься для отримання зображення у випадку проникнення у приміщення або якщо буде виявлено пожежу.

– Система на кристалі ESP 32 Wroom-32 буде використана як концентратор для всіх давачів. Використання цієї системи продиктовано його малим енергоспоживанням та наявністю модуля Wi-Fi. Всі давачі під’єднані до ESP32 через провідне з’єднання, в той час як ESP32 комунікує із Raspberry Pi через бездротову мережу Wi-Fi. Безпровідна комунікація між ESP32 та Raspberry Pi дозволяє організувати процес моніторингу у декількох приміщеннях та залучити декілька ESP32.

– Середовище розробки на основі потоків Node red, яке встановлено на Raspberry Pi. Використовується для реалізації сценаріїв ідентифікації проникнення у приміщення із фотофіксацією та ропізнаванням, а також пожежної сигналізації із фотофіксацією.

Таким чином визначені компоненти та зв’язки між ними у неведеній структурі кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi дозволяють реалізувати поставлені вимоги до проектованої системи.

2.3 Аналіз обраних рішень

Після проєктування структури та визначення принців функціонування кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією, наступним етапом є відбір та оцінка можливостей апаратного та програмного забезпечення, що будуть задіяні у запропонованій системі.

2.3.1 Аналіз обраних апаратних рішень

Пропонована кіберфізичні система пожежної та охоронної сигналізації із реалізацією функції фотофіксації складається із наступних апаратних компонентів: одноплатної комп’ютерної системи Rasperry Pi, давачів вимірювання рівня газу у повітрі, температури, руху, модуля п’єзодинаміка для відтворення звуку, камери для Raspberry Pi, а також системи на кристалі ESP32 Wroom-32.

Однією із головних вимог, що ставляться до систем пожежної та охоронної сигналізації є наявність пристрою, що генерує звуковий сигнал у випадку наявності небезпечної ситуації. В пропонованій кіберфізичні системі пожежної та охоронної сигналізації із фотофіксацією в якості такого пристрою використано модуль п’єзодинаміка YL-44 (рис. 2.2).

Підключення п’єзодинаміка YL-44 є типовим для давачів, що включає у себе під’єднання живлення, заземлення, а також сигналу керування. П’єзодинамік видає такий самий звук, як динамік ініціалізації в системному блоці комп'ютера. П’єзодинамік керується Arduino контролером або іншим керуючим мікропроцесорним пристроєм за допомогою спеціальних програм і бібліотеки «TONE». Даний модуль можна використовувати із будь-якими мікропроцесорними та мікроконтролерними системами, зокрема MCU/ARM/PIC/AVR/STM32MCU/ ARM/PIC/AVR/MSP430/PLC/STM32/Arduino, тощо.

Рисунок 2.2 – Модуль п’єзодинаміка YL-44

П’єзодинамік конструктивно представлений металевою пластиною з нанесеним на неї напиленням із струмопровідної кераміки. Пластина та напилення виступають у ролі контактів. Пристрій полярний, та має власні «+» та «-». Принцип дії зумера заснований п’єзоелектричному ефекті. Згідно із ним, при подачі електрики на зумер він починає деформуватися. При цьому відбуваються удари об металеву платівку, яка і робить «шум» потрібної частоти.

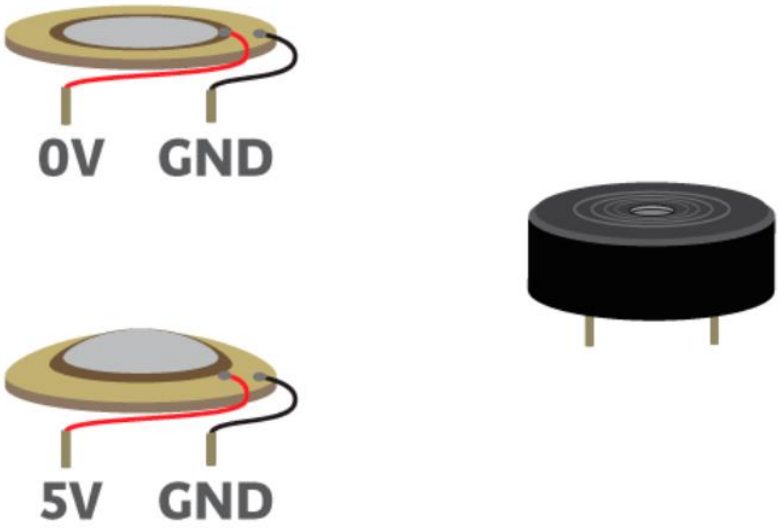


Рисунок 2.3 – Принцип роботи п’єзодинаміка

Слід також відзначити, що бузер буває двох видів: активний та пасивний. Принцип дії у них однаковий, проте в активному немає можливості змінювати частоту звучання, хоча сам звук гучніший і підключення його є дещо простішим.

Бузер модуля звука YL-44 володіє має наступні характеристиками:

– Модель: FC-07.

– Тип зумера: пасивний.

– Звук, що відтворюється: такий як у динаміка ініціалізації в системному блоці комп'ютера.

– Отвір для закріплення на плоскій поверхні.

– Напруга живлення: 3,3 - 5 В.

– Розмір: 33 х 13 х 12 мм.

– Вага: 6 г.

Таблиця 2.1 – Призначення контактів модуля п’єзодинаміка YL-44

Вивід		Опис
1	VCC	Напруга живлення
2	GND	GND
3	I/O	Керуючий сигнал

В якості давача для вимірювання температури у проектованій кіберфізичній системі було обрано DHT11 (рис. 2.3). Давач DHT11 призначений для вимірювання температури та вологості повітря. Передача даних здійснюється через один провідник на основі використанням власного протоколу. Може бути використаний у пристроях Arduino, AVR, PIC, ARM та ін. Складається з ємнісного датчика вологості та термістора. Також давач містить в собі аналогово-цифровий перетворювач для перетворення аналогових значень вологості та температури.

Давач DHT11 володіє наступними характеристиками:

- Модель виробника: ASAIR DHT11.
- Визначення вологості: 5 – 95% RH ± 5% (макс.).
- Визначення температури: -20 ~ +60 ºC ± 2% (макс.).
- Живлення: 3.5-5.5 В.
- Частота опитування: ~1 Гц.
- Розміри 15.5 х 12 х 5.5 мм.

Таблиця 2.2 – Призначення контактів модуля п’єзодинаміка DHT11

Вивід		Опис
1	VCC	Напруга живлення
2	GND	GND
3	Data Out	Керуючий сигнал
4	NC	Не використовується

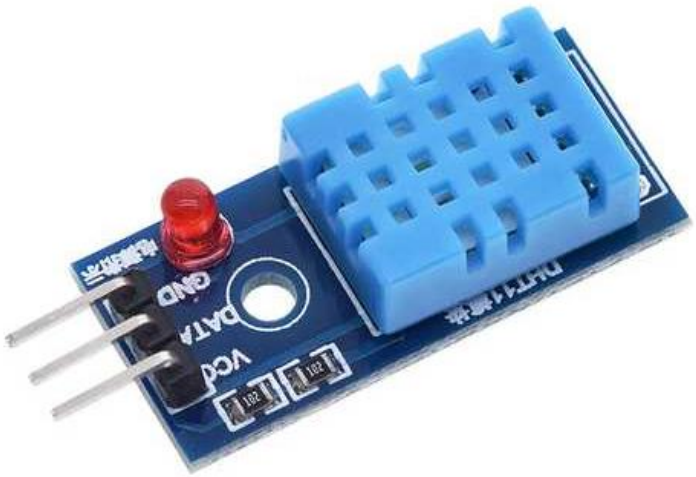


Рисунок 2.4 – Модуль давача вимірювання температури DHT11

У проекті було використано датчик руху HC-SR501, який працює на основі вимірювання інфрачервоного випромінювання. Він дозволяє виявляти рух об’єктів на відстані до 7 метрів і має два входи живлення та один цифровий вихід, яким можна знімати дані. Якщо датчик виявляє рух об'єкта, то на його виході буде високий рівень, а якщо немає – низький. Датчик також має перемичку, яка впливає на його роботу: якщо перемичка встановлена в положенні H, то на виході буде високий рівень, поки датчик буде виявляти рух, якщо перемичка в положенні L, то стан виходу буде перемикатися з високого на низький і назад приблизно раз у секунду. Для більшості проектів положення H є переважаючим, але для керування пристроєм, що перемикається по фронту сигналу, кращим рішенням буде положення L.

Датчик HC-SR501 має наступні характеристики:

- Дальність виявлення: 0 - 7 м.
- Кут спрацьовування: 110° (на дистанції до 7 м).
- Вихідна напруга логічного рівня: 0 - 3.3 В.
- Напруга живлення (рекомендована): 4.5 - 12 В.
- Максимальний вихідний струм: 65 мА.
- Час затримки: 0.3 – 300 секунд.
- Режими перемикання: L – неповторюване, H – повторюване.
- Діапазон робочої температури: -20° - +50°.

Таблиця 2.3– Призначення контактів давача HC-SR501

Вивід		Опис
1	VCC	Живлення
2	GND	Земля
3	Data	High/Low output

Рисунок 2.5– Датчик HC-SR501

В якості давача, що вимірює рівень вуглекислого газу у повітрі було обрано MQ-135. Датчик газу MQ-135 Gas Sensor реагує на наявність у повітрі шкідливих газів і їх сумішей, що дозволяє оцінити його якість. Датчик реагує на наступні гази:

– Вуглекислий газ (CO2).
– Аміак (NH3).
– Окиси азоту (NOx).
– Етиловий спирт.
– Бензин.
– Дим.

Давач має два виходи – аналоговий й дискретний TTL. Напруга на аналоговому виході змінюється в залежності від концентрації домішок у повітрі, і

складає діапазон 0-5 В. Порог обробки датчика газу MQ135 по дискретному виходу налаштовується потенціометром на корпусі.

Перед першим використанням давач слід його прогріти протягом 24-х годин, після чого відкалібрувати на свіжому повітрі (для отримання еталонних значень).

Давач MQ-135 має наступні характеристики:

– Тип технології: Напівпровідниковий.

– Тип детектируемого газу: угарний газ CO, пари спирту, бензин, алкоголь та ін.

– Час обробки: 10 с.

– Час відновлення: 30 с.

– Потужність нагрівача: 900 мВт.

– Робоча температура -10...50 °C.

– Напруга живлення: 5 В.

– Вихідний сигнал High/Low і аналоговий.

– Використовуваний компаратор: LM393.

– Габаритні розміри: 32x22x30 мм.

Таблиця 2.4– Призначення контактів давача MQ-135

Вивід		Опис
1	VCC	Живлення
2	GND	Земля
3	AOUT	Аналоговий вихід
4	DOUT	Цифровий вихід

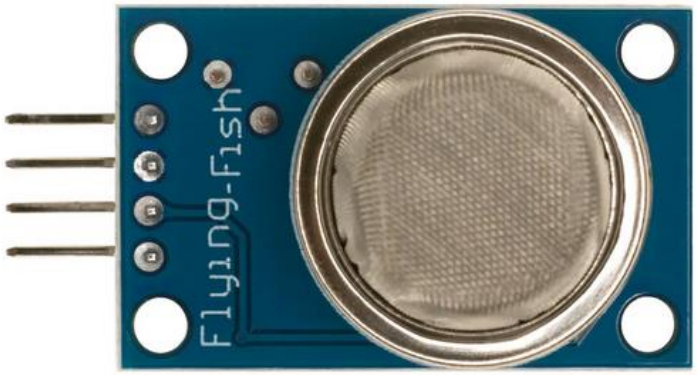


Рисунок 2.6 – Давач визначення рівня вуглекислого газу MQ-135

В якості концентратора, до якого під’єднуються всі давачі у системі використано систему на кристалі ESP32 WROOM32. ESP32 - це мікроконтролер з вбудованим Wi-Fi та Bluetooth, розроблений компанією Espressif Systems. Його призначення полягає в забезпеченні бездротового зв'язку та обробки даних в різноманітних застосуваннях Інтернету речей (IoT), мобільних пристроях, сенсорах, різноманітних додатках та інших проектах.

В якості системи на кристалі, до якої під’єднуються всі давачі було обрано ESP32. ESP32 – серія недорогих мікросхем з малим енергоспоживанням компанії Espressif Systems [19]. Представляє собою систему на кристалі з інтегрованими контролерами радіозв'язку Wi-Fi, Bluetooth і Thread. У серіях ESP32 і ESP32-S використовуються процесорні ядра з архітектурою компанії Tensilica, а в серіях ESP32-C і ESP32-H – ядра з відкритою архітектурою RISC-V.

Одним із представників серії ESP32 є модуль ESP-32 DevKit V1 (рис. 2.7).

Модуль розробника DEVKITV1 30-pin побудований на мікромодулі ESP-WROOM-32 - новому мініатюрному високопродуктивному поєднанні Wi-Fi + BT + BLE модулем, призначеним для широкого спектра застосувань, починаючи від мікропотужних мережевих датчиків до найскладніших програм, наприклад, таких як кодування голосу, потокова передача музики та MP3 кодування. На модулі зібрана вся необхідна мінімальна периферія, достатня для швидкого і комфортного старту роботи з ESP-WROOM-32.

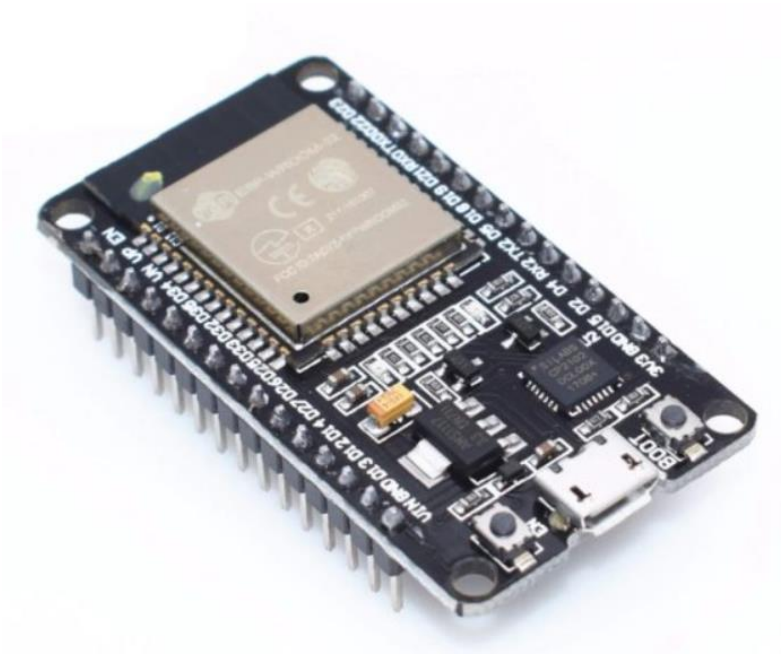


Рисунок 2.7 – Модуль ESP-32 DevKit V1

ESP-WROOM-32 виконаний на базі популярного двоядерного чіпсета ESP32, із змінною тактовою частотою від 80 МГц до 240 МГц, можливістю індивідуального управління і живлення.

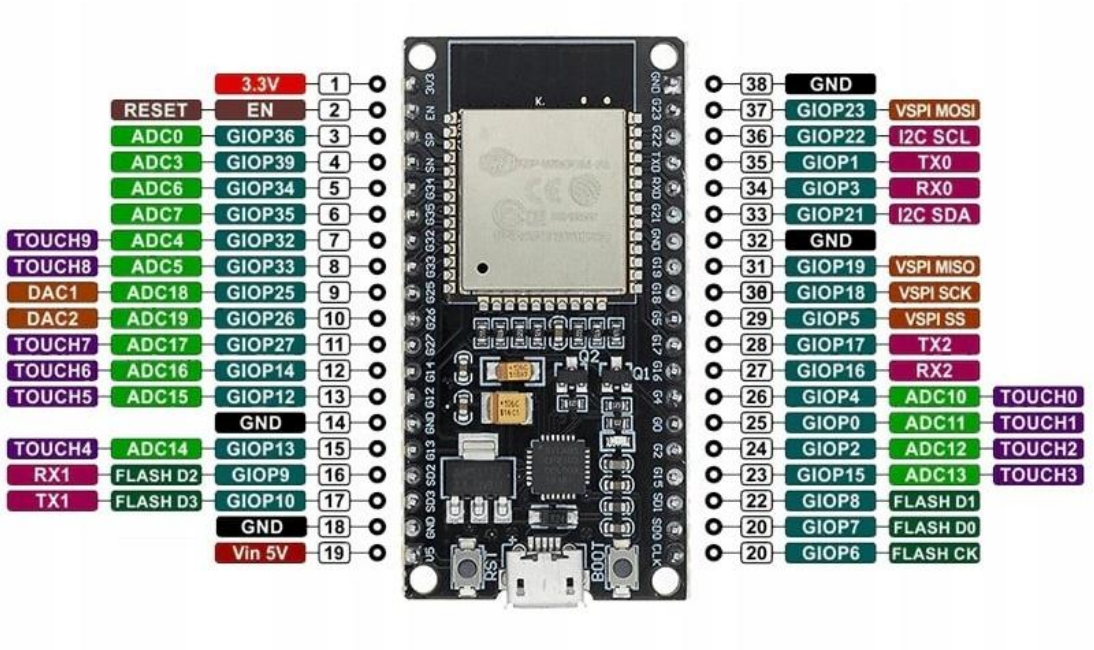


Рисунок 2.8 – Призначення контактів ESP-WROOM-32

Модуль розроблений для переносної і автономної електроніки та додатків інтернет-речей, виконаний в мініатюрному корпусі 25,5 мм х 18 мм, обладнаний

Flash пам'яттю, кварц 40 МГц і PCB антеною, що забезпечує відмінні RF характеристики.

ESP-WROOM-32 має досить багату периферію, що включає в себе такі інтерфейси як I2C, UART, SPI, I2S, роз'єм для SD карти, інфрачервоний порт, інтерфейс для підключення ємнісної сенсорної панелі.

Однією з особливостей модуля є наднизьке електроспоживання і гнучкий вибір «сплячих» режимів (споживання до 20мкА в режимі deep sleep mode).

Модуль підтримує весь стек протоколів стандартів WiFi 802.11n і BT4.2, забезпечуючи даний функціонал через інтерфейси SPI/SDIO або I2C/UART.

Основні властивості системи на кристалі ESP32:

– USB-UART конвертер: CP2102.

– Напруга живлення: 5В.

– Максимальний струм стабілізатора напруги: 800мА.

– Wi-Fi Стандарти: FCC/CE/IC/TELEC/KCC/SRRC/NCC.

– Протоколи: 802.11 b/g/n/d/e/i/k/r (802.11n до 150 Мбіт/с).

– A-MPDU і A-MSDU підтримка та підтримка захисного інтервалу в 0.4 сек.

– Частотний діапазон: ГГц 2.4 ~ 2.5.

– Bluetooth Протоколи: Bluetooth v4.2 BR/EDR і BLE specification.

– Радіо NZIF приймач з чутливістю: -98 dBm.

– Передавач: Class-1, class-2 і class-3 AFH.

– Аудіо: CVSD і SBC.

– Апаратні засоби та інтерфейси: SD, UART, SPI, SDIO, I2C, LED PWM, Motor PWM, I2S, IR.

GPIO, сенсорний датчик, ADC, DAC, LNA перед підсилювач.

2.3.2 Аналіз обраних програмних рішень

З метою реалізації сценаріїв охоронної та пожежної сигналізації та аналізу даних отриманих від давачів та камери, на Raspberry Pi встановлено програмне

забезпечення Node-RED. Node-RED є відкритим веб-інтерфейсом на основі потоків, що дозволяє швидко створювати програми для Інтернету речей (IoT) та автоматизації процесів, використовуючи зручний графічний інтерфейс.

Node-RED пропонує візуальну відповідь на складність створення потоків даних та забезпечує зручну візуалізацію та маніпулювання потоками даних. Він має бібліотеку вбудованих вузлів, що дозволяє виконувати різноманітні завдання, такі як обробка даних, комунікація з різними API, інтеграція з базами даних та іншими службами, а також збереження та обробка даних IoT-датчиків.

Node-RED має відкритий інтерфейс, тому його можна легко розширити за допомогою сторонніх вузлів та плагінів. Це дозволяє розробникам швидко та ефективно створювати складні програмні рішення для IoT та інших додатків Інтернету.

З точки зору реалізації проєктованої кіберфізичної системи важливою функцією є процес розпізнавання зображення. Таку функцію можна реалізувати за допомогою TensorFlow, відкритого програмного забезпечення з відкритим кодом для машинного навчання та глибинного навчання, що розроблене компанією Google. TensorFlow надає фреймворк для створення та навчання штучних нейронних мереж.

Node-RED підтримує TensorFlow через використання сторонніх вузлів, таких як node-red-contrib-tensorflow та node-red-contrib-tf-model. Ці вузли дозволяють користувачам створювати та навчати нейронні мережі, а також використовувати навчені моделі в потоках даних Node-RED. За допомогою вузлів node-red-contrib-tensorflow та node-red-contrib-tf-model користувачі можуть завантажувати навчені моделі TensorFlow та використовувати їх у своїх потоках даних Node-RED. Також ці вузли надають засоби для навчання моделей за допомогою даних, які надходять в потік даних Node-RED.

Окрім Node-RED на Raspberry Pi потрібно встановити брокер Mosquitto повідомлень, для організації обміну даними по MQTT протоколу. Mosquitto – це відкрите програмне забезпечення з відкритим кодом, яке є брокером повідомлень, розробленим для протоколу MQTT (Message Queuing Telemetry Transport). Брокер

MQTT дозволяє взаємодіяти з додатками Інтернету речей (IoT), обмінюючись повідомленнями між клієнтами.

Mosquitto є популярним брокером MQTT і зазвичай використовується для побудови масштабованих систем Інтернету речей (IoT), в тому числі для збору даних з сенсорів, контролю за пристроями та системами контролю віддаленого доступу. Mosquitto дозволяє клієнтам підключатися до брокера, надсилати та отримувати повідомлення, підписуватися на теми та отримувати повідомлення, які стосуються цих тем. Він має підтримку для SSL / TLS для забезпечення безпеки обміну повідомленнями та масштабованості. Щодо сумісності, то Mosquitto працює на більшості операційних систем, включаючи Linux, Windows та MacOS, та може бути запущений на різних пристроях, таких як Raspberry Pi, BeagleBone та інші. Він є відкритим джерелом, що дозволяє користувачам змінювати його джереловий код, доповнювати його функціональність та налаштувати його для власних потреб.

2.4 Висновки до розділу 2

Сформульований набір функціональних вимог до кіберфізичної системи, що передбачає виконання проектованою системою функцій ідентифікація проникнення у приміщення із фотофіксацією та ропізнаванням зображення, а також ідентифікація задимленості та наявності осередку вогню із фотофіксацією. З метою реалізації поставлених вимог запропоновано структуру кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi, а також проведно аналіз апаратних та програмних компонентів, необхідних для реалізації цієї системи.

3 РЕАЛІЗАЦІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ПОЖЕЖНОЇ ТА ОХОРОННОЇ СИГНАЛІЗАЦІЇ ІЗ ФУНКЦІЄЮ ФОТОФІКСАЦІЇ НА БАЗІ RASPBERRY PI

3.1 Встановлення та підготовка середовища Node-RED та брокера mosquitto

Пропонована кіберфізична система пожежної та охоронної сигналізації із функцією фотофіксації передбачає тісний взаємозв'язок між апаратними та прогармними компонентами. Передача даних між системою на кристалі ESP32 та одноплатною комп'ютерною системою Raspberry Pi здійснюється через бездротовий зв'язок. В якості протоколу обміну даними пропонується використати MQTT. Реалізація функцій брокера здійснюється за допомогою mosquitto. Для реалізації сценаріїв пожежної та охоронної сигналізації використано середовище розробки на основі потоків Node red. Обидві програмні системи розгорнуті на одноплатній комп'ютерній системі Raspberry Pi. Розглянемо кроки встановлення даного програмного забезпечення.

Спочатку у консолі введемо команду для завантаження Node red:

```
bash <(curl -sL
https://raw.githubusercontent.com/node-red/linux-
installers/master/deb/update-nodejs-and-nodered)
```

Активуємо функцію автоматичного запуску Node-RED при завантаженні Raspberry Pi:

```
sudo systemctl enable nodered.service
```

Після перезавантаження Raspberry Pi, виконаємо запуск середовища Node-RED, шляхом вводу у браузер IP адреси Raspberry Pi (hostname -I) та номера порту 1880:

```
http://192.168.0.3:1880
```

Важливо зазначити, що для того, щоб Node-RED продовжував працювати, потрібно залишати вікно з командним рядком відкритим.

Наступним кроком є встановлення MQTT брокера mosquitto. Для цього у новому вікні терміналу введемо команди :

```
sudo apt update
sudo apt install -y mosquitto mosquitto-clients
```

Також активуємо функцію автоматичного запуску брокера при завантаженні системи, шляхом виконання команди:

```
sudo systemctl enable mosquitto.service
```

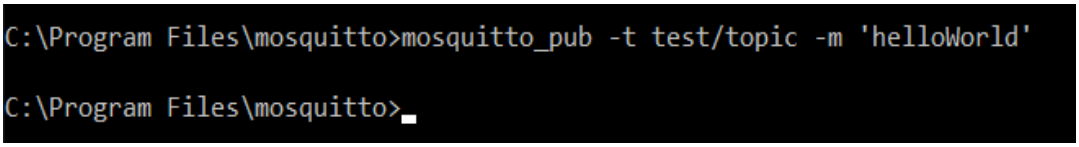
Після завершення встановлення брокера mosquitto, слід у терміналі виконати:

```
mosquitto
```

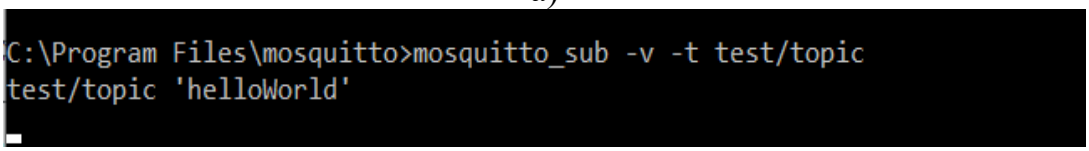
Слід візначити, що брокер mosquitto надає два клієнти командного рядку для підписки та публікації повідомлень mosquitto_sub та mosquitto_pub відповідно. Наприклад для демонстрації роботи обміну повідомленнями через брокер mosquitto відкриємо два термінали, де у першому виконаємо публікацію у топік, а в другому – підписку на цей топік:

```
mosquitto_pub -t test/topic -m 'helloWorld'
mosquitto_sub -v -t test/topic
```

Результати роботи команд зображено на рис. 3.1 (в якості операційної системи було використано Windows 10).



а)



б)

Рисунок 3.1 – Тестування брокера mosquitto: а) публікація повідомлення у топік; б) підписка на топік та зчитування повідомлення

3.2 Монтажна схема кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією

До складу розробленої кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією входять наступні апаратні компоненти: одноплатна комп'ютерна система Raspberry Pi 3 model B, ESP32 Wroom-32, три датчики (вимірювання рівня вуглекислого газу у повітрі MQ-135, температури DHT11, руху HC-SR501) та модуль п'єзодинаміку YL-44.

Для створення монтажної плати було використано систему автоматизованого проєктування (САПР) Fritzing, яка дозволяє створювати монтажні плати та електричні схеми за допомогою графічного інтерфейсу. Бібліотека Fritzing складається із великої кількості компонентів, що включає зокрема популярні електронні компоненти, такі як резистори, конденсатори, мікроконтролери тощо.

Для створення монтажної плати спочатку слід перенести необхідні компоненти на робочу область (слід відзначити, що не всі компоненти є у стандартній бібліотеці, тому попередньо слід виконати процес пошуку та інмпорту необхідних компонентів). Також додамо макетну плату, яка використовуватиметься для стоврення загальної шини живлення та шини заземлення, до яких будуть під'єднані відповідні піни всіх давачів. Давач температури та вологості повітря DHT11 під'єднується до піна GPIO2 на ESP32 (параметр вологості повітря не використовується у даній системі). Давач руху HC-SR501 під'єднується до піна GPIO5. Давач вимірювання рівня вуглекислого газу у повітрі під'єднано до піна GPIO8 ESP32. Сигнальний пін модуля п'єзодинаміка під'єднано до піна GPIO1 на ESP32. Піни живлення та заземлення підведені у окремі шини, які з'єднані із зовнішнім джерелом живлення через DC2.1 роз'єм.

Монтажну схему кіберфізичної системи пожежної та охоронної сигналізації із фотофіксацією наведено на рис. 3.2.

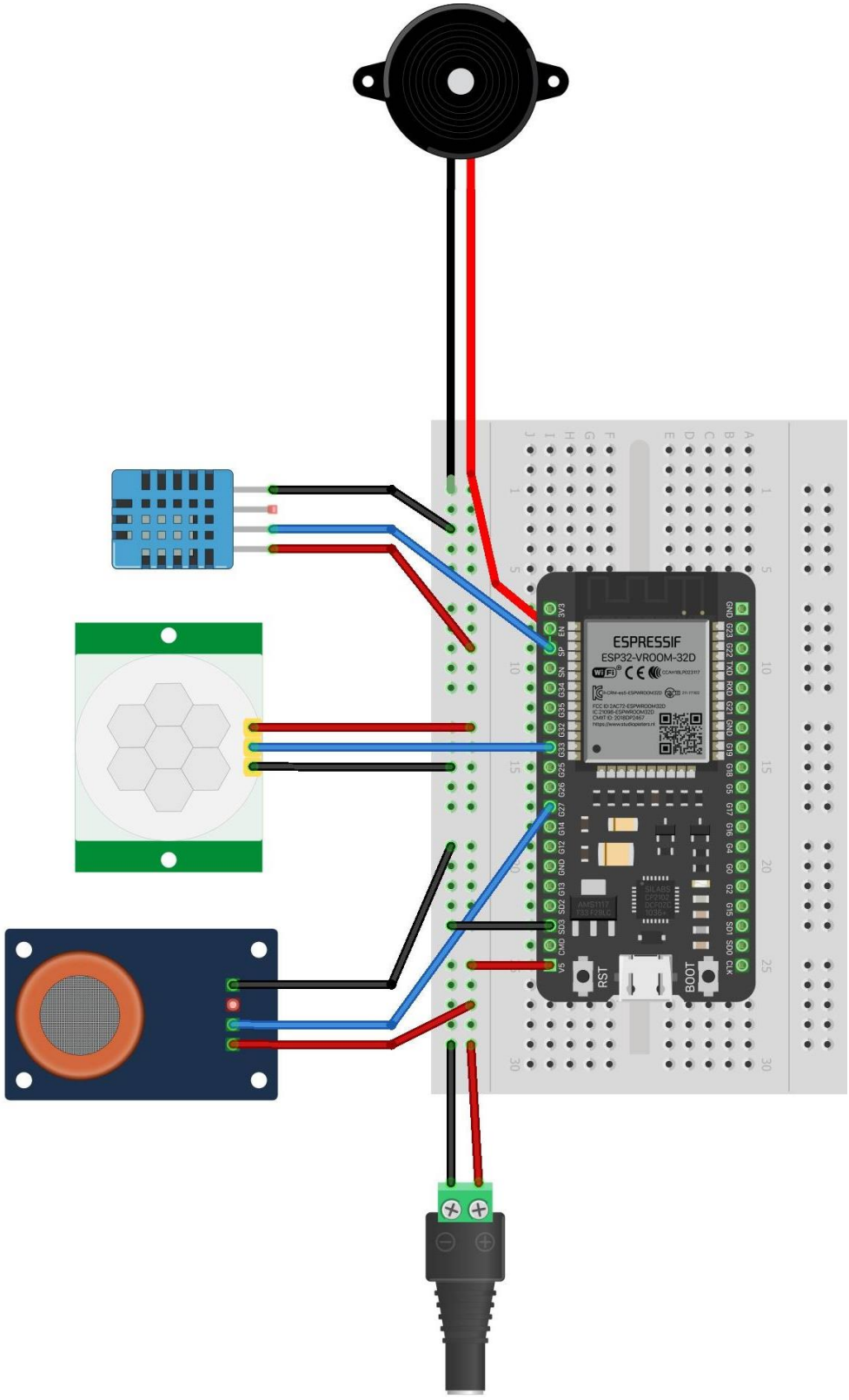


Рисунок 3.2 – Монтажна схема кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією

3.3 Принципова схема і схема розведення провідників на макетній платі

Електричні принципові схеми є важливим інструментом для проектування та розробки електричних та електронних пристроїв. Вони допомагають зрозуміти, як працює пристрій, відображаючи взаємодію між його основними елементами та функціональними блоками. Принципова схема показує зв'язки між елементами пристрою, відображаючи спосіб, у який вони підключені між собою та до джерела живлення. Вона надає інформацію про спосіб роботи пристрою та його взаємодію з навколишнім середовищем, дозволяє встановити правильну послідовність елементів та оптимізувати схему.

У проектованій кіберфізичній системі пожежної та охоронної сигналізації з фотофіксацією було використано такі компоненти як давачі температури та вологості повітря DHT11, руху HC-SR501, рівня вуглекислого газу у повітрі MQ-135, а також п’єзодинамік та система на кристалі ESP32. Живлення схеми реалізується від зовнішнього джерела живлення. Всі компоненти системи під’єднуються до загальної жини живлення та шини заземелення (рис. 3.3). Слід звернути увагу, що на даній схемі не наведено Raspberry Pi, а лише ESP32 із давачами.

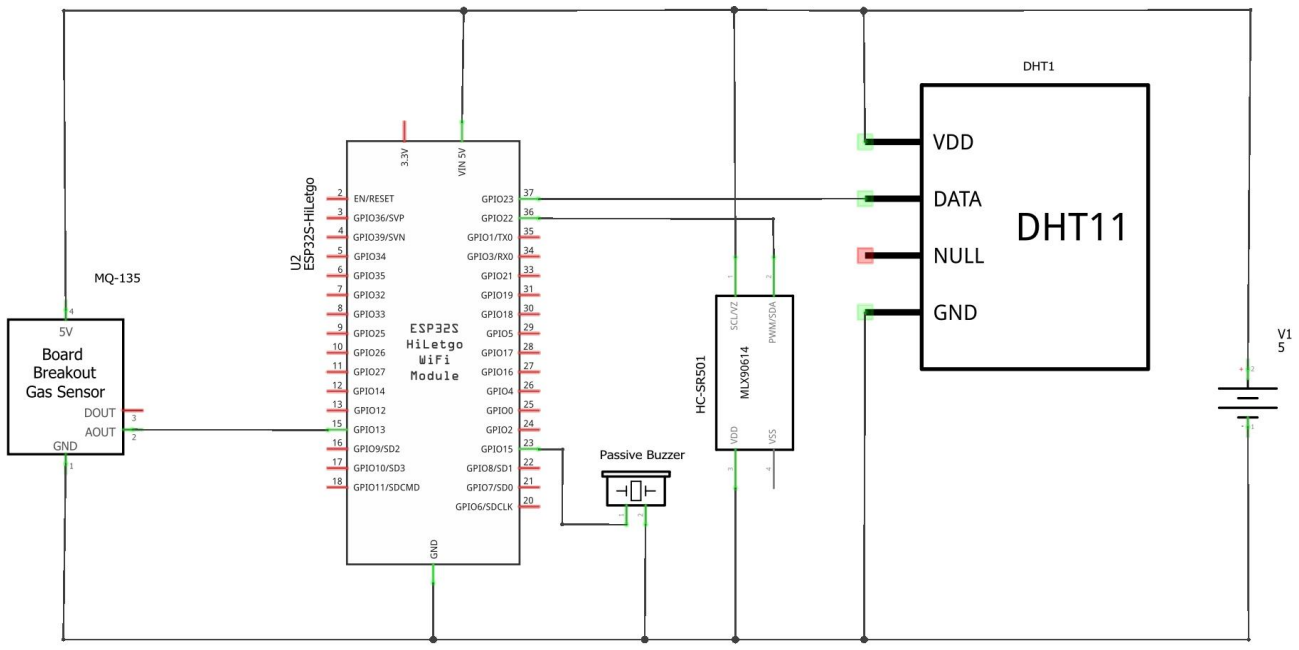


Рисунок 3.3 – Схема електрична приницпова проєктованої системи

Ще однією важливою схему для проєктування пристрою є схема роведення провідників, оскільки вона забезпечує коректне підключення елементів до джерела живлення та до інших елементів відповідно до вимог проекту. Для створення схеми розведення провідників було використано програму для автоматизованого проектування електронних пристроїв Fritzing. Після розстановки всіх компонентів в потрібному порядку, було здійснено розведення провідників шляхом використання меню «Розведення» та процесу автотрасування. Після завершення автотрасування було отримано схему розведення з надлишковими перегинами провідників. Ці недоліки було виправлено вручну, що дало змогу отримати остаточну схему розводки провідників, зображену на рис. 3.4. Як видно із схеми пропонована друкована плата складається із провідників, що розміщенні на обох сторонах друкованої плати.

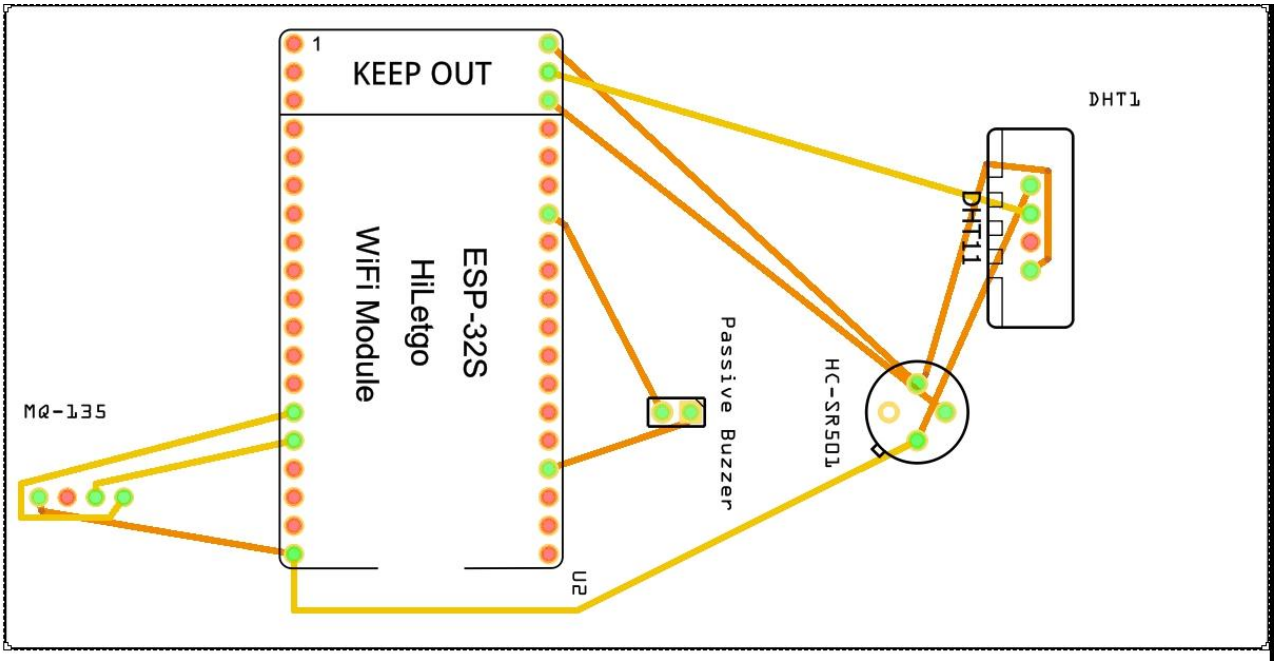


Рисунок 3.4 – Схема розведення провідників

3.4 Реалізація сценаріїв пожежної та охоронної сигналізації із реалізацією функції фотофіксації у Node red

Відповідно до поставлених вимог, реалізація функцій кіберфізичної системи включає в себе імплементацію наступних сценаріїв:

1. Сценарій ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням. У випадку наявності руху у приміщенні система повинна зробити фото та виконати процес його розпізнавання. Якщо буде визначено, що на фото зображена людина, надіслати повідомлення із прикріпленим фото на електронну пошту користувача.
2. Сценарій пожежної сигналізації із фотофіксацією. У випадку наявності задимленості (підвищення рівня концентрації вуглекислого газу у повітрі) або підвищення температури у приміщенні, система повинна увімкнути оповіщення, зробити фото та надіслати повідомлення із прикріпленим фото на електронну пошту користувача.

Розглянемо детальніше процес створення зазначених сценаріїв.

3.4.1 Сценарій ідентифікації проникнення у приміщення із фотофіксаціює та ропізнаванням

В основі свого функціонування запропонований сценарій ідентифікації проникнення у приміщенн використовує можливості бібліотека TensorFlow. TensorFlow.js – це реалізація на мові JavaScript відкритої платформи машинного навчання TensorFlow. Бібліотека TensorFlow дозволяє розробникам створювати складні моделі нейромереж та навчати їх за допомогою великих наборів даних. Вона підтримує різні мови програмування, включаючи Python, C ++ та Java, і може працювати як на CPU, так і на GPU. Однією із особливостей TensorFlow є те, що цю бібліотеку можна використовувати в режимі реального часу у браузері або на сервері.

Почнемо розгляд сценарію визначення порушника у Node red із створення потоку розпізнавання зображень.

Бібліотека потоків Node-RED має кілька вузлів із підтримкою TensorFlow.js. Одним із них є node-red-contrib-tensorflow, який містить навчені моделі. Для того, щоб встановити набір нодів для роботи із node-red-contrib-tensorflow слід перейти до верхнього правого меню редактора потоку, натиснути «Керувати палітрою», перейти на вкладку «Палітра» та вибрати вкладку «Встановити». Після цього слід ввести «node-red-contrib-tensorflow» у полі пошуку (рис. 3.5).

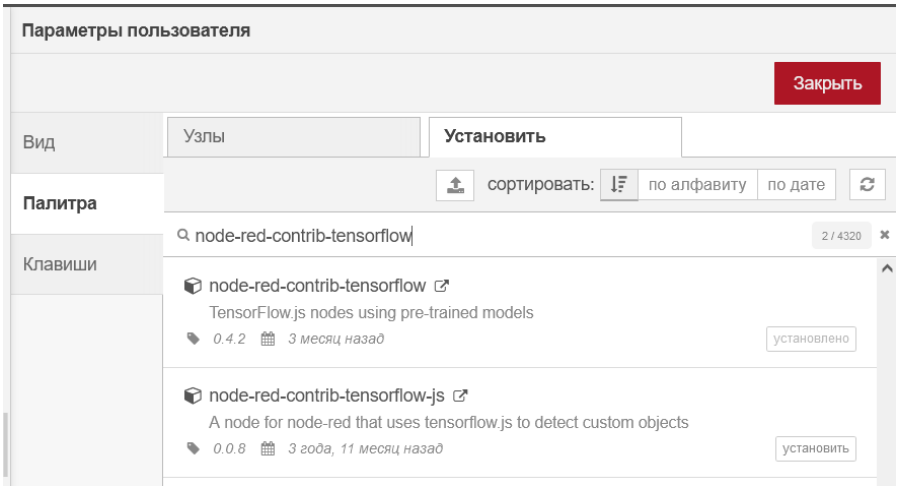


Рисунок 3.5 – Встановлення node-red-contrib-tensorflow

Після завершення інсталяції, помаранчеві вузли TensorFlow.js з’являться в категорії «Аналіз» на панелі зліва (рис.3.6).

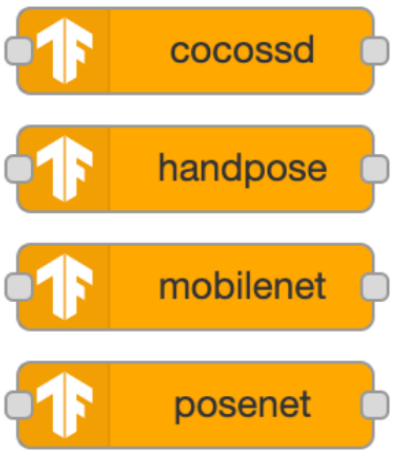


Рисунок 3.6 – Додатково встановлені ноди у Node red для роботи із TensorFlow

Усі наведені вище вузли є вузлами розпізнавання зображень, але вони також можуть генерувати дані зображення з анотаціями та виконувати інші функції, як наприклад розпізнавання зображень, що є необхідним для крайової аналітики.

Створення сценарію ідентифікації проникнення у приміщення розпочнемо із реалізації функції розпізнавання зображення із використанням TensorFlow. Для цього додамо ноду cocossd для розпізнавання, ноду завантаження зображення у потік та дві ноди виведення результатів, одну для виведення консоль (Debug), іншу – для відображення зображення у потоці (Image preview). Проєктований сценаріїв повинен бути здатним розпізнавати людину та тварину, оскільки в іншому випадку це призведе до хибних спрацювань системи, що може значно позначитись на ступеню довіри до проектованої кіберфізичної системи. Протестуємо роботу потоку, підвантаживши по черзі два зображення. На першому зображено людину-зловмисника, а на іншому – собаку.

Окрім того для реалізації інших функцій сценарію додатково встановимо ноди для надсилання електронної пошти, завантаження зображення із системи у потік Node red, а також ноди, що відображають зображення у потоці. Відповідні команди для встановлення цих нод виглядатимуть наступним чином:

```
node-red-node-email
node-red-contrib-browser-utils
node-red-contrib-image-output
```

Виконаємо налаштування ноди image preview, змінивши значення msg.payload на msg.annotatedInput, що дозволить тим самим відображати попередній перегляд зображення. Налаштування ноди Image preview зображено на рис. 3.7.

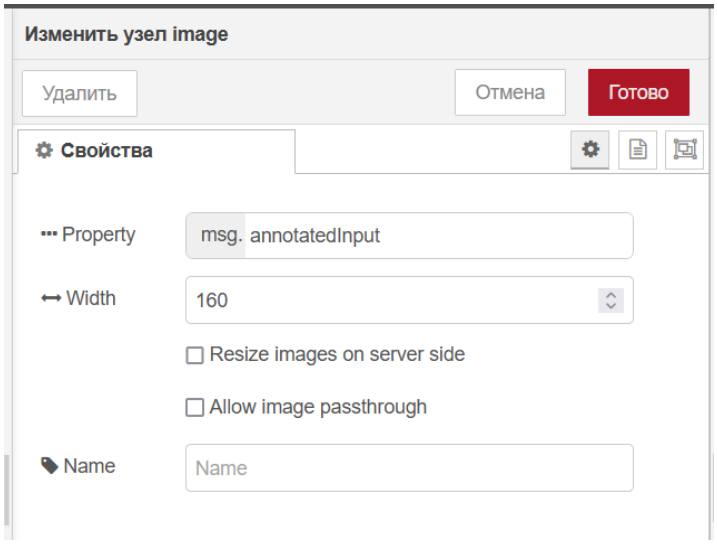


Рисунок 3.7 – Налаштування ноди Image preview

Результати розпізнавання двох зображень наведено на рис. 3.8 та 3.9.

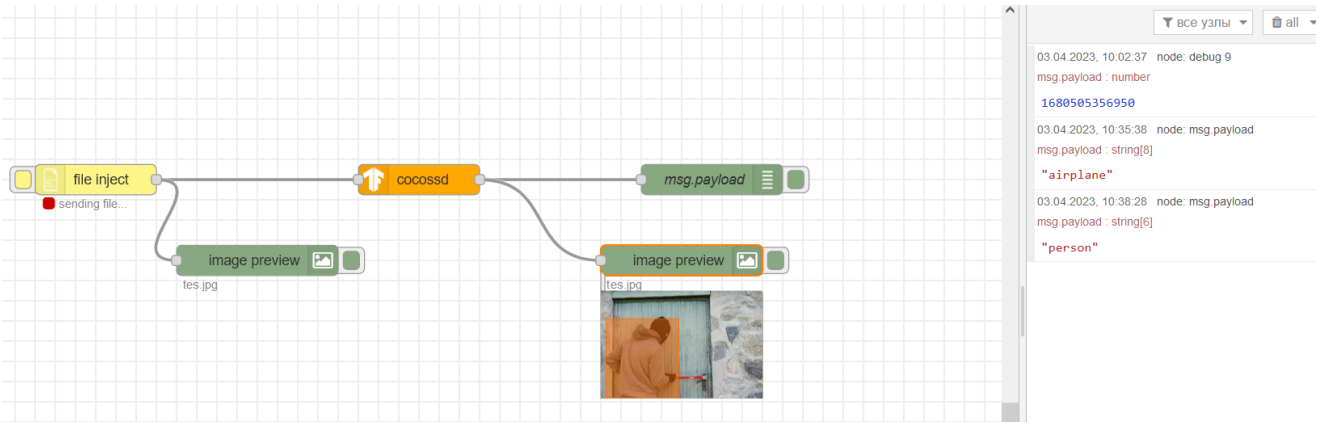


Рисунок 3.8 – Потік, що вірно розпізнав зображення зловмисника (у ноді image preview розпізнана область виділена прямокутником)

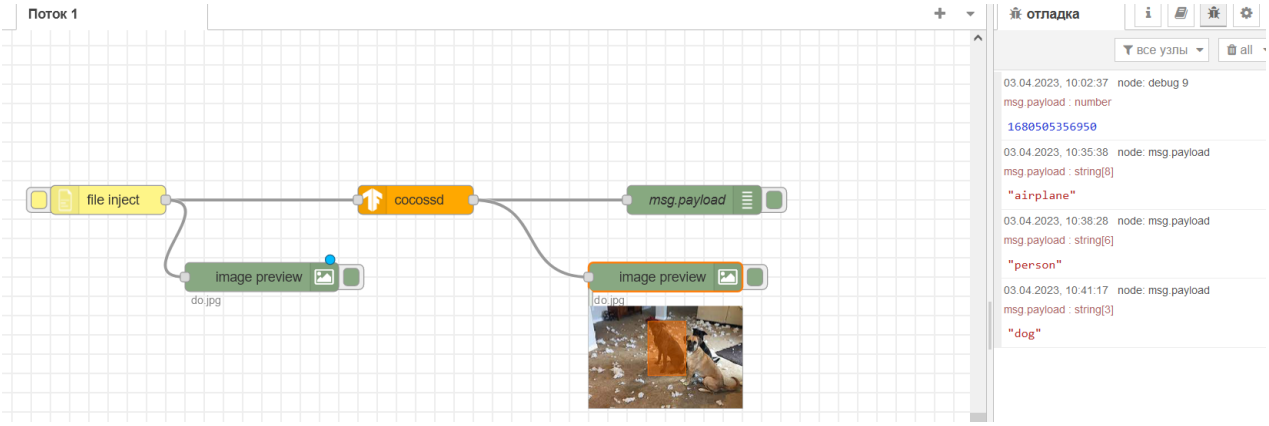


Рисунок 3.9 – Потік, що вірно розпізнав зображення собаки (у ноді image preview розпізнана область виділена прямокутником)

Як видно із результатів роботи потоку, система вірно розпізнала два зображення (можна помітити у вікні Debug у першому випадку було виведено “person”, а в другому “dog”), що таким чином дозволяє зменшити хибні сповіщення системи про потенційну загрозу проникнення у приміщення.

Для подальшого створення сценарію ідентифікації проникнення у приміщення приберемо всі ноди окрім cocossd.

Далі додамо ноду підписки на MQTT топік home/pir, якій дамо ім’я pir sensor (рис. 3.10). У цей топік публікуються повідомлення від давача руху із заданим інтервалом. Якщо було виявлено рух давач буде публікувати повідомлення «open», якщо руху не має – «close».

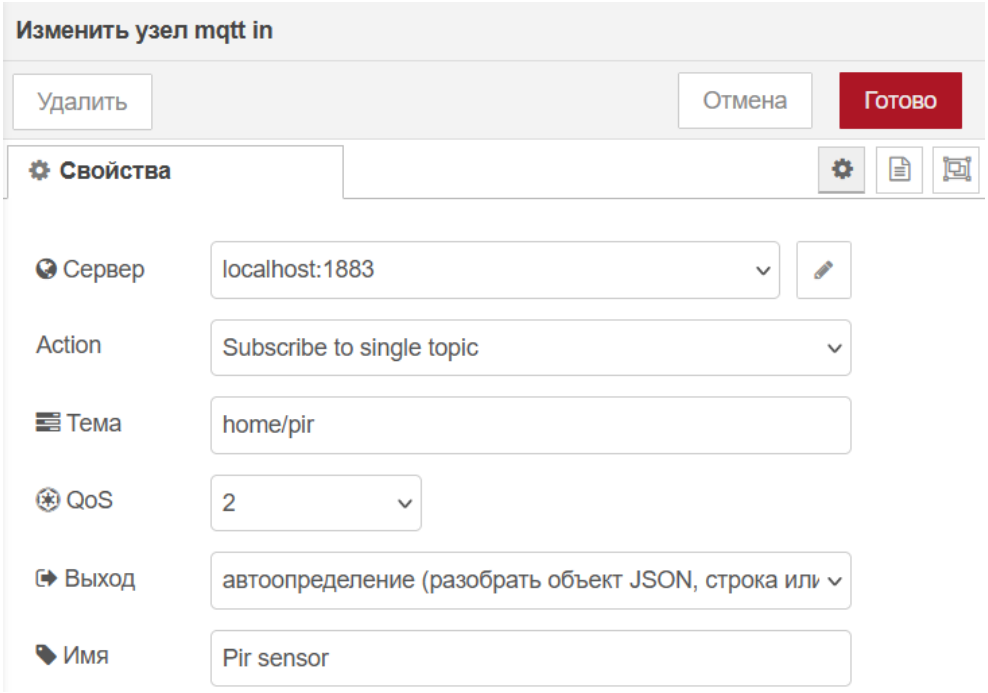


Рисунок 3.10 – Властивості ноди pir sensor

Також додамо switch, якій дамо назву check pir. Основним її призначенням є фільтрація повідомлень, і пропуск далі по ланцюгу тільки повідомлень «open», тобто коли рух виявлено.

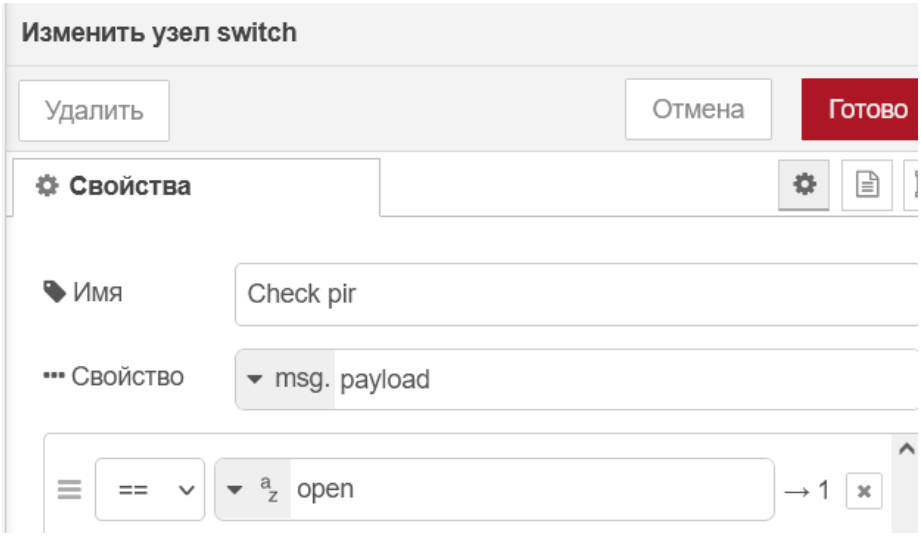


Рисунок 3.11 – Властивості ноди check pir

Далі послідовно додамо ноди Take photo node, а також switch та change, для яких змінимо ім’я на Check person та Prepare photo to send.

Нода Take photo node використовується для створення фото із камери, що під’єднана до одноплатної комп’ютерної системи Raspberry Pi. Після отримання зображення, воно передається у ноду cocossd для розпізнавання.

Нода Check person використовується для перевірки, чи розпізнане зображення відноситься до класу «person». Якщо в результаті перевірки, буде отримано інший клас, повідомлення не буде доставлено на наступну ноду.

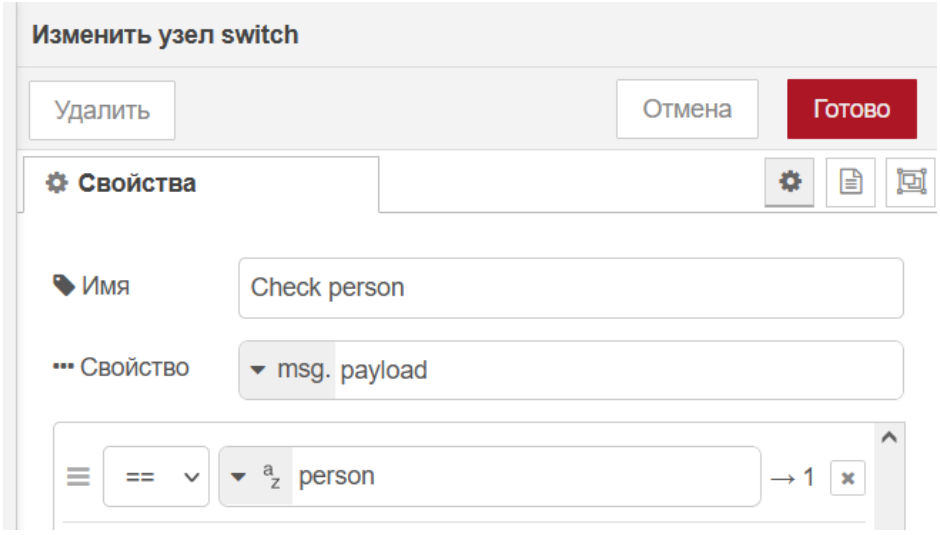


Рисунок 3.12 – Властивості ноди Check person

Нода Prepare photo to send використовується для конвертації даних в анотовані дані. Annotated input – це вхідні дані, що були доповнені або розмічені додатковою інформацією, яка допомагає виявляти певні залежності, структури або властивості даних. Наприклад, в машинному навчанні, при побудові моделей мови або моделей класифікації, до вхідних даних можна додати різноманітну розмітку, що характеризує властивості цих даних, наприклад, мітки класів, теги, ключові слова, тощо. В даному випадку на вихідне фото буде доданий червоний прямокутник із зоною інтересу, що дозволить підвищити ступінь наочності отриманого результату. На рис. 3.13 подано властивості ноди Prepare photo to send.

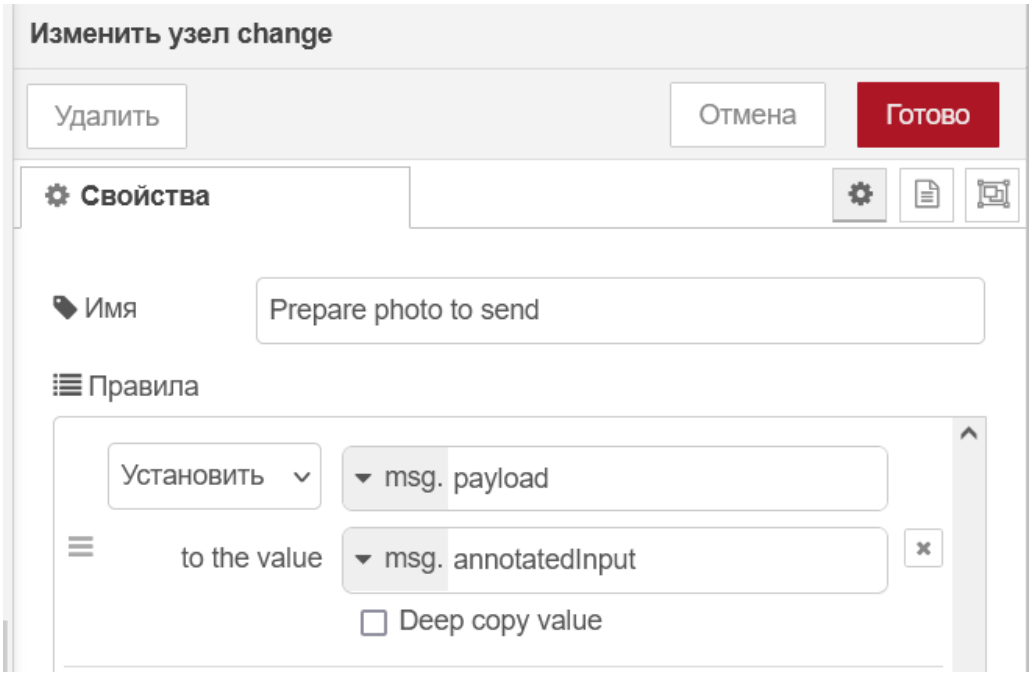


Рисунок 3.13 – Властивості ноди Prepare photo to send

В кінці створеного ланцюга додамо ноду email, що використовується для надсилання на пошту повідомлення. Властивості ноди, що використовується для надсилання повідомлення на пошту подано на рис. 3.14.

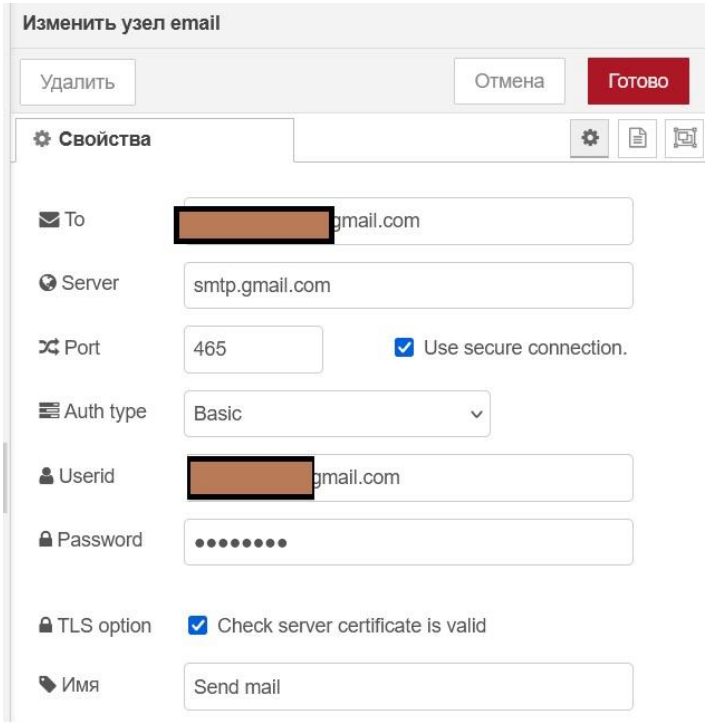


Рисунок 3.14 – Властивості ноди mail

Слід відзначити, що з метою надання дозволу надсилання сторонніми сервісами повідомлень на електронну пошту Google слід створити пароль для за стосунку. Для цього слід перейти у налаштування акаунту Google, вибрати «Безпека», далі «Двохфакторна аутентифікація» та перейти до «паролі застосунків» (рис. 3.15).

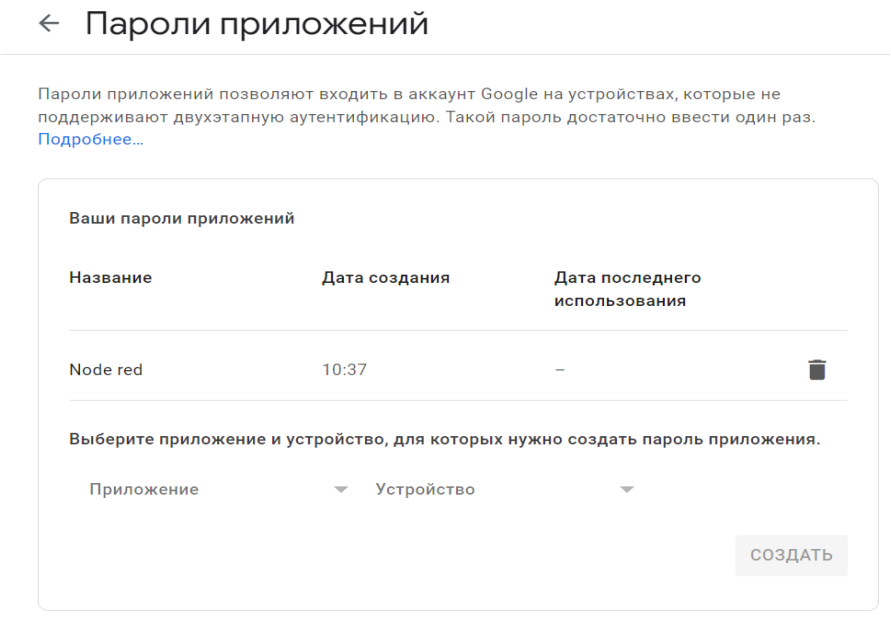


Рисунок 3.15 – Створення паролю для застосунку

В результаті буде згенерований код доступу, який потрібно встаивти у поле Password ноди mail (рис. 3.14).

Результуючи сценарій ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням зображено на рис. 3.16

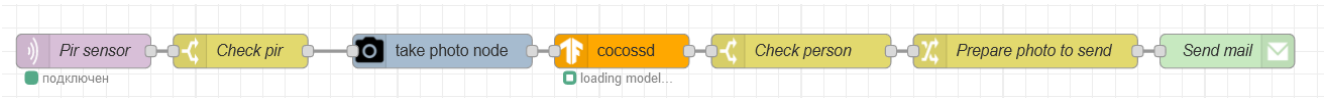


Рисунок 3.16 – Сценарій ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням

Для локального тестування розробленого сценарію без залучення Raspberry Pi додамо до сценарію можливість перевірки фото зробленого не із камери Raspberry Pi, а отриманого через http запит. Для цього додамо ноду http запит та ще одну ноду cocossd. Вигляд сценраію ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням із функцією тестування без отриманого зображення від камери Raspberry Pi наведено на рис. 3.17.

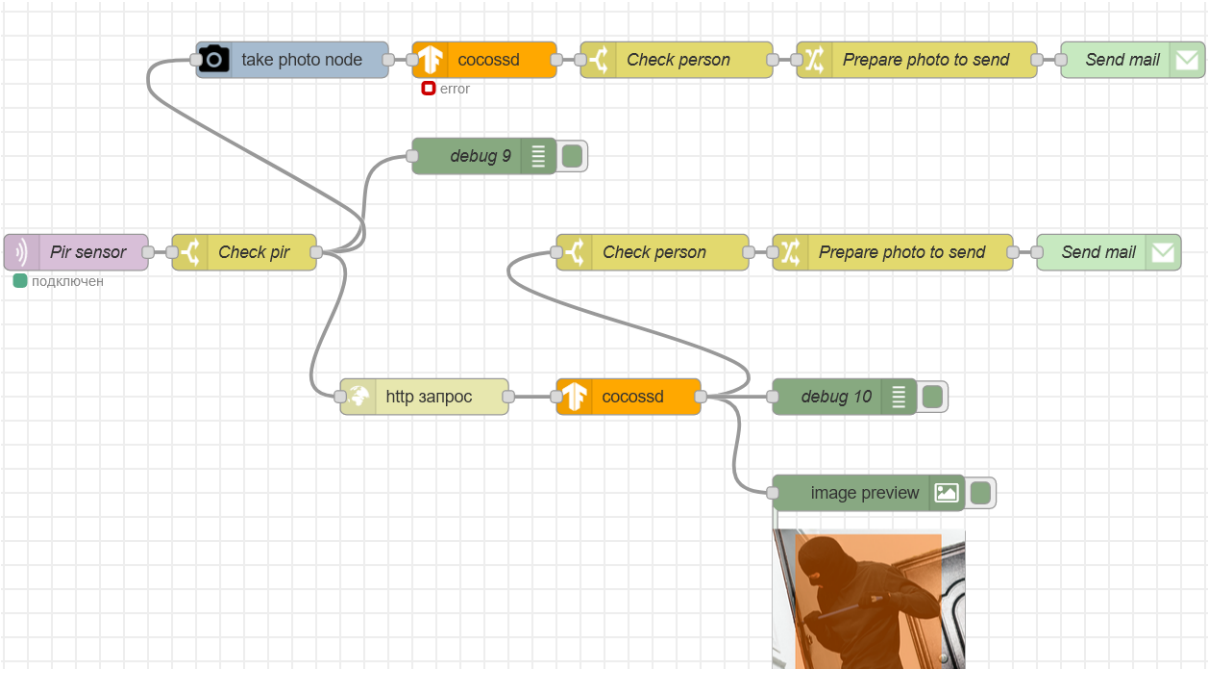


Рисунок 3.17 – Сценарій ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням із функцією тестування без отриманого зображення від камери Raspberry Pi (локальне тестування)

Таким чином в результаті публікації у топік home/pir повідомлення від давача руху «open» буде надіслано повідомлення на електронну пошту (рис. 3.18 та 3.19) із прикріпленим фото порушника.

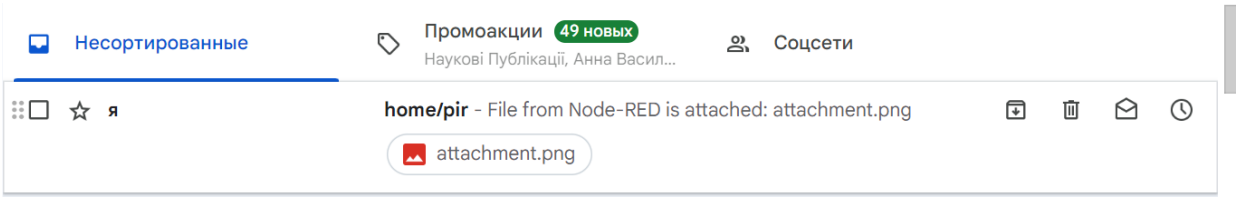


Рисунок 3.18 – Повідомлення про проникнення у приміщення із вкладенням зображення

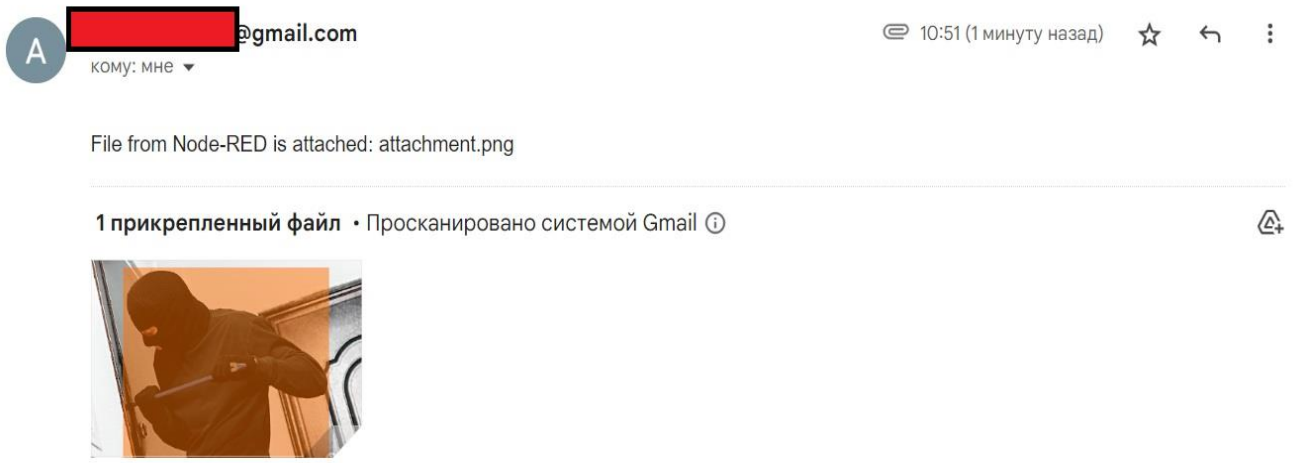


Рисунок 3.19 – Прикріплення у повідомленні про проникнення

3.4.2 Сценарій пожежної сигналізації із фотофіксацією

Відповідно до поставлених вимог, які повинна реалізовувати проєктована кіберфізична система, виділяються два параметри навколишнього середовища, що повинні контролюватися сценарієм – це значення температури та рівень вуглекислого газу у приміщенні. Тобто сценарії повинен спрацьовувати у випадку перевищення допустимого рівня або одного із зазначених фізичних параметрів або двох одночасно. Результатом роботи цього сценарію буде увімкнення звукової сигналізації, що довзолить оповістити всіз присутніх у приміщенні, а

також надсилання на електронну пошту повідомлення, для інформування про ситуація, яка склалась.

Проєктування сценарію функціонування кіберфізичної системи розпочнемо із створення нодів для підписки та публікації повідомлень. Оскільки сценарій дозволяє моніторити два фізичних параметри, то й нодів для підписки повинно бути дві (рис. 3.20 та рис. 3.21).

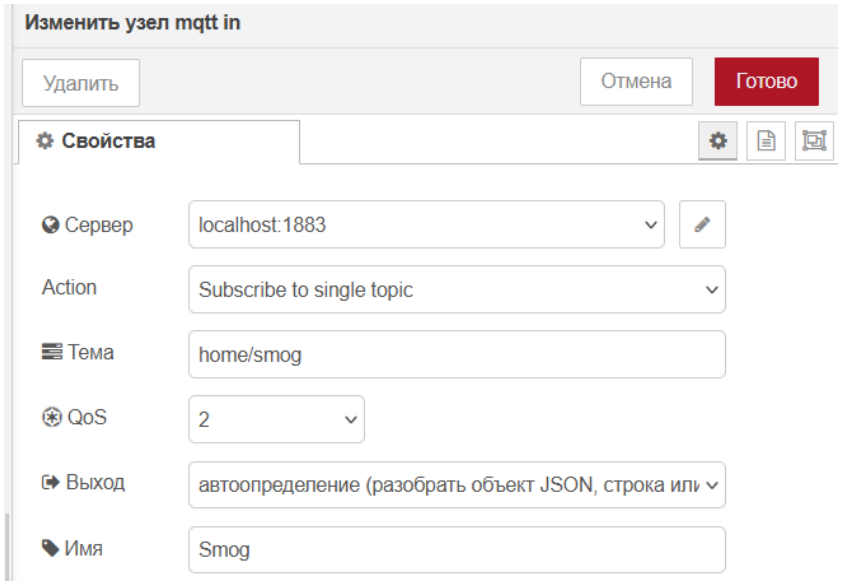


Рисунок 3.20 – Властивості ноди підписки Smog

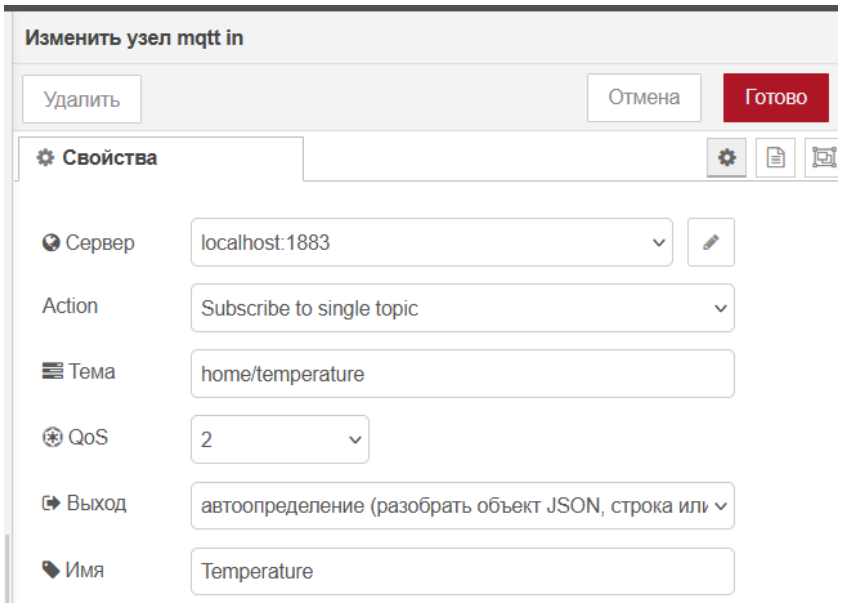


Рисунок 3.21 – Властивості ноди підписки Temperature

Перша нода підписана на топік home/temperature, друга – на home/smog.

Також додамо ноду для публікації у топік home/buzer, на який підписаний модуль бузера (рис. 3.22).

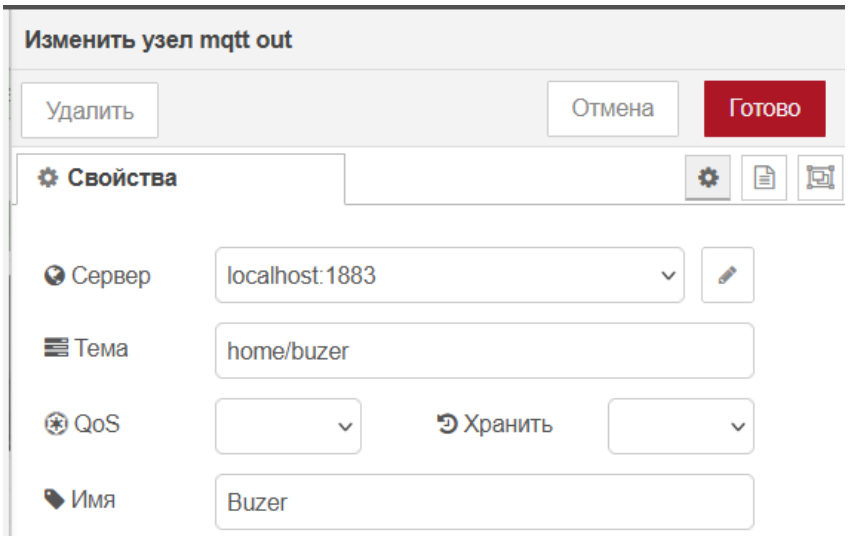


Рисунок 3.22 – Властивості ноди публікації Buzer

Додамо у ланцюг ноду funcion, яка повинна аналізувати отримані значення із нод temperature та smog, і у випадку перевищення граничних (порогових) значень генерувати повідомлення «fire», яке буде публікуватись у топік home/buzzer (рис. 3.23). У випадку відсутності перевищення граничних показників температури та рівня вуглекислого газу, публікуватиметься повідомлення «nofire». В якості граничних показників для температури обрано значення більше 30 градусів, а для рівня вуглекислого газу – 300 ppm. Лістинг коду для ноди function наведено на рис. 3.24.

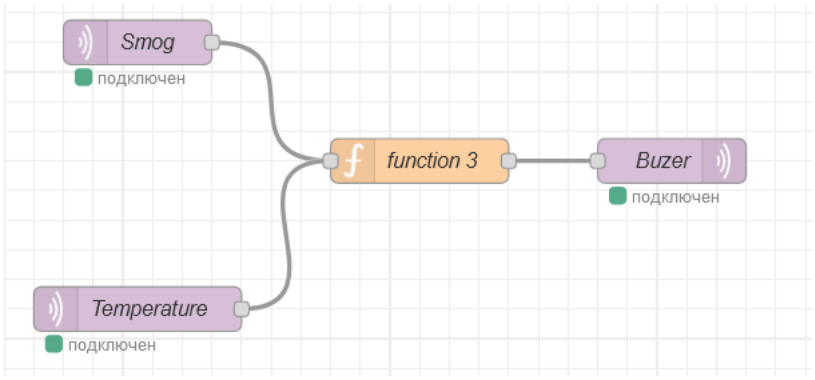


Рисунок 3.23 – Ланцюг підписки на топіки home/temperature та home/smog та публікації у топік home/buzer у випадку перевищення граничних значень

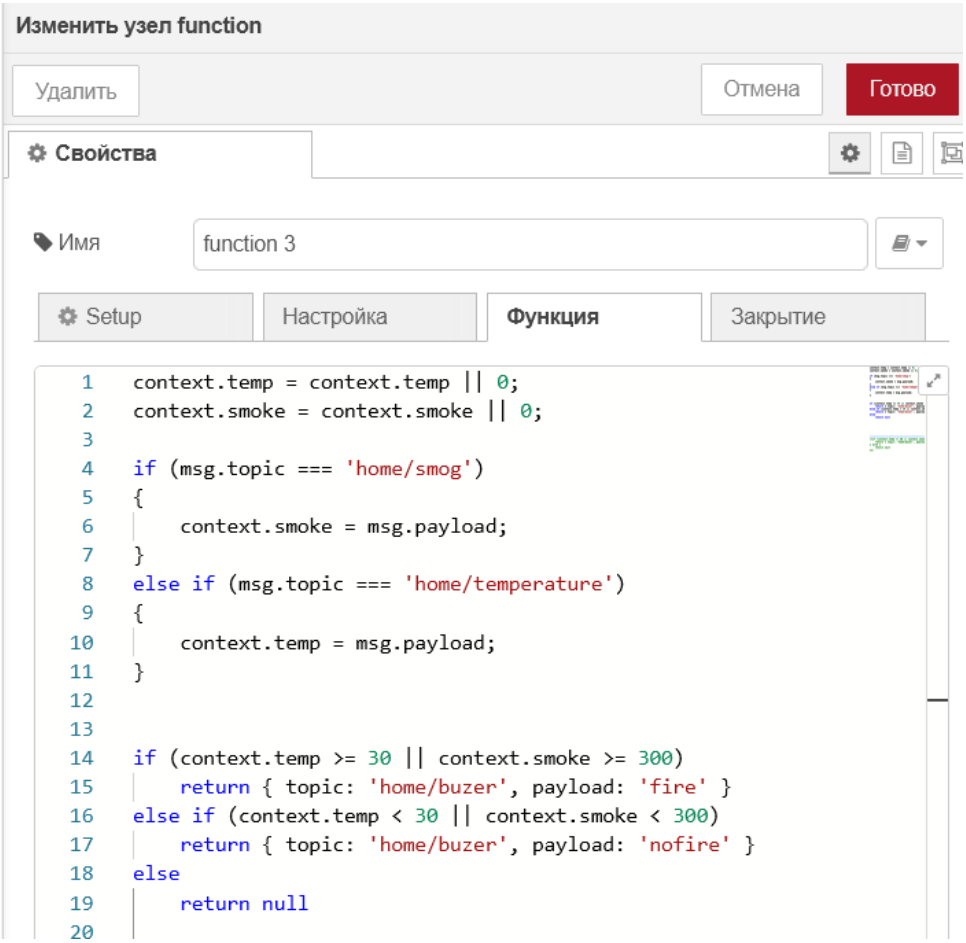


Рисунок 3.24 – Властивості ноди function

Наступним кроком додамо ноди switch, take photo node та email. Ноді switch привласнимо ім’я Check fire. Основна функція цієї ноди це перевірка повідомлення від ноди function, й у випадку надходження повідомлення «fire» здійснюється його передача далі по ланцюгу.

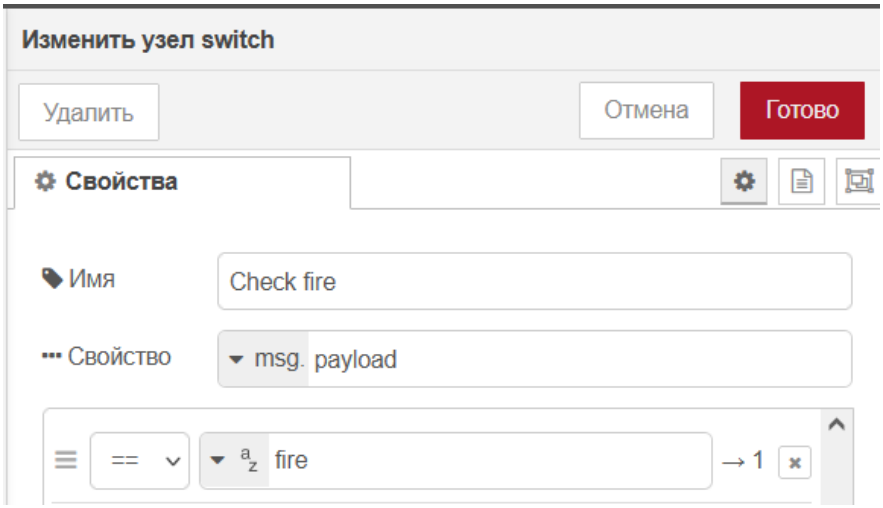


Рисунок 3.25 – Властивості ноди Check fire

У випадку появи повідомлення «fire» здійснюється створення фото за допомогою камери на Raspberry Pi та його надсилання за допомогою ноди email. Налаштування параметрів ноди email аналогічні налаштуванням у сценарії ідентифікації проникнення у приміщення.

Результуючий сценарій пожежної сигналізації із фотофіксацією зображено на рис. 3.26.

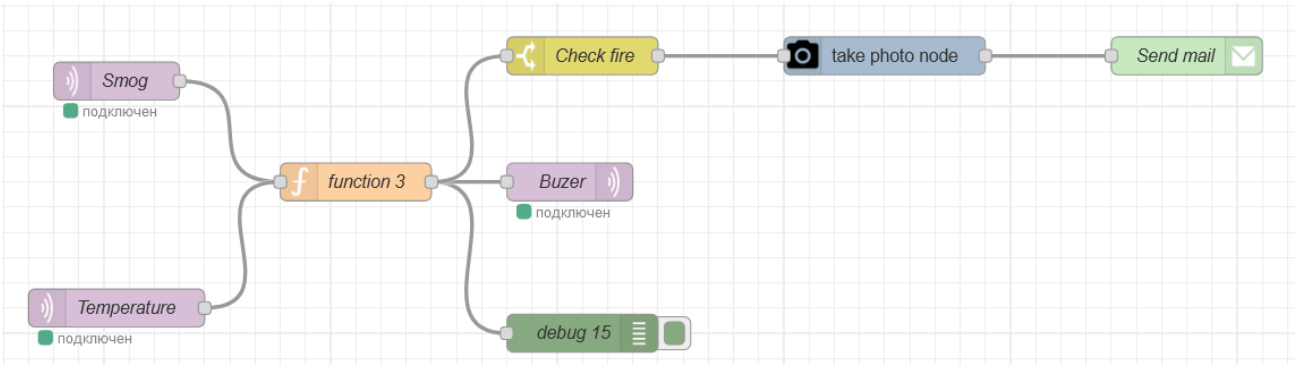


Рисунок 3.26 – Сценарій пожежної сигналізації із фотофіксацією

Для зручності тестування додатково додамо ноду http запит, яка буде виконувати запит, що отримує картинку. А також додамо ноду Debug, яку включимо одразу після ноди function, основна мета якої виведення діагностичного повідомлення у консоль Debug (рис. 3.27).

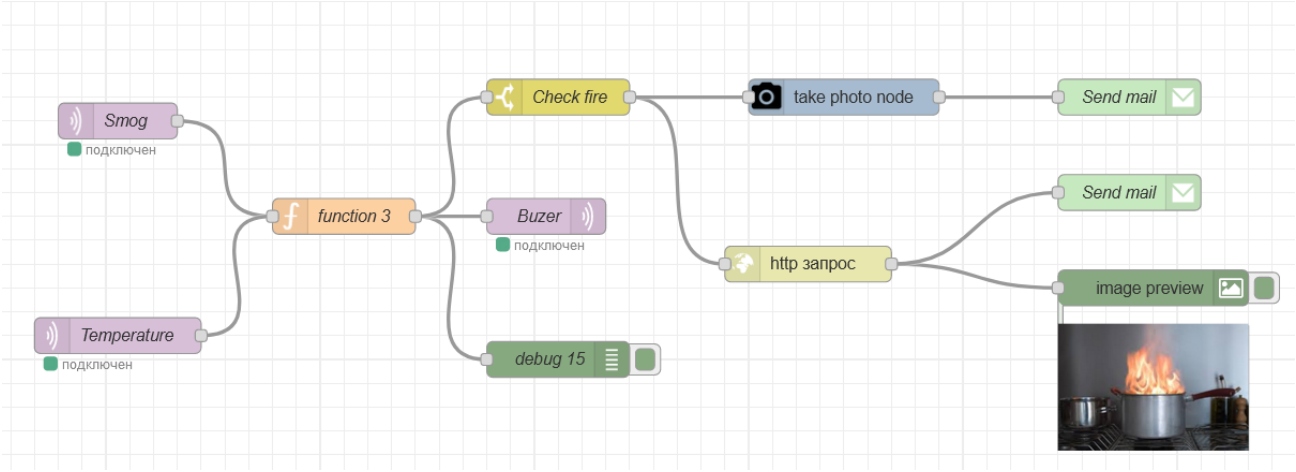


Рисунок 3.27 – Сценарій пожежної сигналізації із фотофіксацією без отриманого зображення від камери Raspberry Pi (локальне тестування)

Для локального тестування спроєктованого сценарію виконаємо публікацію у топік home/smog повідомлення, що перевищує порогове значення для показнику газу у приміщенні (рис. 3.28).

```
C:\Program Files (x86)\mosquitto>mosquitto_pub -t home/smog -m "400"
```

Рисунок 3.28 – Тестування сценарію: публікація повідомлення із значенням рівня газу, що перевищує норму у топік home/smog

Паралельно виконаємо підписку на топік home/buzer, у якому очікуватимемо надходження повідомлення fire, що дозволить активувати звукову сигналізацію.

В результаті роботи сценарію буде отримано повідомлення «fire» (рис. 3.5), а також буде виведено це повідомлення у консолі Debug (рис. 3.5). Ще однією реакції кіберфізичної системи буде надсилання повідомлення із прикріпленим фото.

```
c:\Program Files (x86)\mosquitto>mosquitto_sub -t home/buzer
fire
```

Рисунок 3.29 – Тестування сценарію: підписка на топік home/buzer (увімкнення сигналізації)

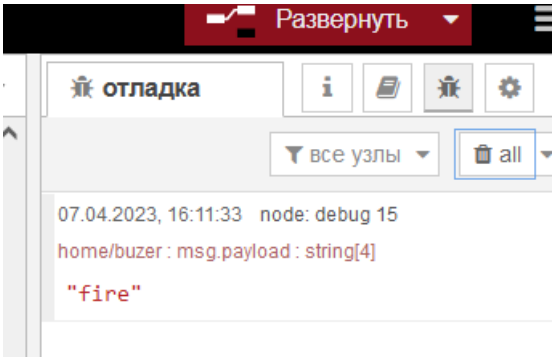


Рисунок 3.30 – Результат виведення у Debug повідомлення «fire» при перевищенні рівня вуглекислого газу

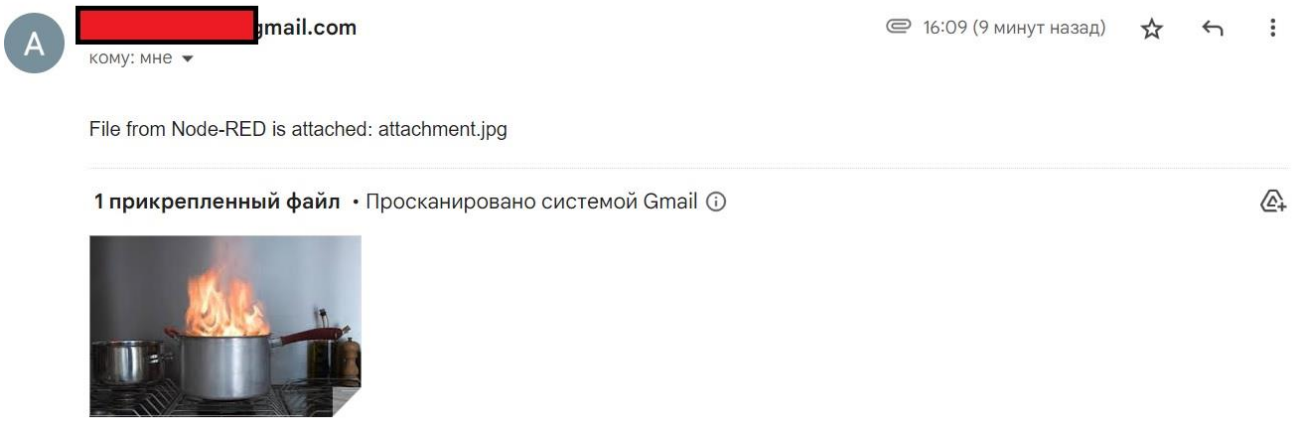


Рисунок 3.31 – Прикріплення у повідомлення, надісланого реалізованою кіберфізичною системою при виявленні пожежі,

3.5 Висновки за розділом 3

Таким чином запропоновано принципову схему і схему розведення провідників на макетній платі, наведено монтажну схему компонентів. Проведено встановлення відповідних програмних компонентів та налаштовано камеру для Raspberry Pi. У середовищі Node-Red реалізовано сценарій ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням й сценарій пожежної сигналізації із фотофіксацією.

ВИСНОВКИ

Тема створення кіберфізичної системи охоронної та пожежної сигналізації із фотофіксацією є дуже актуальною в сучасному світі. Зростаюча кількість різних злочинів, крадіжок, пограбувань та пожеж вимагає використання новітніх технологій для забезпечення безпеки майна та життя людей. Тому в результаті виконання даної кваліфікаційної роботи було запропоновано проєкт кіберфізичної системи охоронної та пожежної сигналізації із фотофіксацією на базі одноплатної комп'ютерної системи Raspberry Pi.

Окрім охоронної сигналізації фотофіксація дозволяє виявляти пожежу на ранніх стадіях та оперативно реагувати на неї. Збір зображень із об'єкта дозволяє визначити точне місце та масштаб пожежі, а також стан пожежогасіння. І нарешті фотофіксація забезпечує зберігання доказів про будь-які небезпечні події або злочини, які можуть відбутися на об'єкті спостереження, що може допомогти у подальшому при розслідуванні інцидентів.

Кіберфізична система охоронної та пожежної сигналізації із фотофіксацією поєднала в собі різні технології, такі як інтернет речей, машинне навчання та обробку зображень. Спроєктована система забезпечує постійний моніторинг об'єкта та автоматичне сповіщення про будь-які події, які можуть статися, такі як вторгнення чи пожежа.

У першому розділі розглянуто концепція та принципи функціонування кіберфізичних систем, наведено відмінності між концепціями «кіберфізичні сисетма» та «інтернет речей», проведено огляд відомих систем охоронної та пожежної сигналізації. В результаті аналізу попередніх досліджень було встановлено, що головним недоліком відомих систем є відсутність розпізнавання створених зображень. В даній роботі цей недолік усунуто шляхом реалізації відповідних сценаріїв у середовищі Node red.

У другому розділі сформульований набір функціональних вимог до кіберфізичної системи, що передбачає виконання проектованою системою функцій ідентифікація проникнення у приміщення із фотофіксацією та ропізнаванням зображення, а також ідентифікація задимленості та наявності осередку вогню із фотофіксацією. З метою реалізації поставлених вимог запропоновано структуру кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi, а також проведно аналіз апаратних та програмних компонентів, необхідних для реалізації цієї системи.

У третьому розділі запропоновано принципову схему і схему розведення провідників на макетній платі, наведено монтажну схему компонентів. Проведено встановлення відповідних програмних компонентів та налаштовано камеру для Raspberry Pi. У середовищі Node-Red реалізовано сценарій ідентифікації проникнення у приміщення із фотофіксацією та розпізнаванням й сценарій пожежної сигналізації із фотофіксацією.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Basri A. H. H. Ibrahim S. N., Malik N. A. and Asnawi A. L. Integrated Surveillance System with Mobile Application, *2018 7th International Conference on Computer and Communication Engineering (ICCCE)*, Kuala Lumpur, Malaysia, 2018 218-222

2. Satishkumar M., Rajini S. Smart Surveillance System using PIR sensor network and GSM, *IJARCET*, 2015.

3. Karpagam G.R., Kumar B.V., Maheswari J.U., Gao X.-Z. Smart Cyber Physical Systems Chapman and Hall, *CRC*, 2020, 294 p.

4. Katravath R. et al Fire Alarm Robot and Authentication System Using Raspberry Pi and Cloud, *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Vol. 8, Iss. 4S2, 2019. 256-259

5. Глибовець А.М., Моголівський В.О. Аналіз систем підтримки розумного будинку. *Control systems and computers*. 2019. No 5(283), 30–37.

6. Arduino ua, Модуль давача якості повітря MQ135, URL: https://arduino.ua/ru/prod1201-modyl-datchika-kachestva-vozdyha-mq135

7. Arduino ua, Давач вологості та температури DHT 11 (v2), URL: https://arduino.ua/ru/prod185-datchik-vlajnosti-i-temperatyri-dht11

8. Arduino ua, Модуль із динаміком активний (buzzer), URL: https://arduino.ua/ru/prod490-modyl-s-dinamikom-buzzer

9. Arduino ua, ІЧ давач руху HC-SR501, URL: https://arduino.ua/ru/prod193-ik-datchik-dvijeniya-dlya-arduino-hc-sr501

10. Buniyamin N. Development of Fire Alarm System using Raspberry Pi and Arduino Uno, Conference: *International Conference On Electrical, Electronics and Systems Engineering (ICEESE)*, December 2013, 37-42.

11. Bhuvaneswari S. Fire Detection Using Raspberry Pi, *International Journal of Electrical Engineering and Technology*, Vol. 12, № 1, 2022, 73-80.

12. Конспект лекцій з дисципліни « Комп'ютерні системи» для студентів напряму підготовки «Комп'ютерна інженерія», І. М. Лазарович. – Івано-

Франківськ : Видавництво Прикарпатського національного університету імені Василя Стефаника, 2014. 190 с.

13. Feng J., Feng Y., Ningzhao L. and Benxiang W., Design and experimental research of video detection system for ship fire, *2019 2nd International Conference on Safety Produce Informatization (IICSPI)*, 2019, 367-370, doi: 10.1109/IICSPI48186.2019.9095929.

14. Jamadagni S., Sankpal P., Patil S., Chougule N. and Gurav S., Gas Leakage and Fire Detection using Raspberry Pi, 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 2019, pp. 495-497, doi: 10.1109/ICCMC.2019.8819678.

15. Sheth M., Trivedi A., Suchak K., Parmar K. and Jetpariya D., Inventive Fire Detection utilizing Raspberry Pi for New Age Home of Smart Cities, *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2020, 724-728, doi: 10.1109/ICSSIT48917.2020.9214108.

16. Mahamudul H., Islam M., Shameem A., Rana J. and Metselaar H., Modelling of PV module with incremental conductance MPPT controlled buck-boost converter, *2013 2nd International Conference on Advances in Electrical Engineering (ICAEE)*, 2013,197-202

17. Фурман І.О., Старовєров Р.М., Мельський Д.О. Огляд можливостей «розумного будинку» для покращання побутових умов та зменшення витрат на утримання домогосподарств. *Енергетика та комп'ютерно-інтегровані технології в АПК*. 2014. No 2. 79-80.

18. Singh N. J. and Sidhu E., Raspberry pi based smart fire management system employing sensor based automatic water sprinkler, *2017 International Conference on Power and Embedded Drive Control (ICPEDC)*, 2017, 102- 106, doi: 10.1109/ICPEDC.2017.8081068

19. Sathyakala G., Kirthika V. and Aishwarya B., Computer Vision Based Fire Detection with a Video Alert System, *2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018, pp. 0725-0727, doi: 10.1109/ICCSP.2018.8524216.

20. Bin Bahrudin M. S., Kassim R. A. and Buniyamin N., evelopment of Fire alarm system using Raspberry Pi and Arduino Uno, *2013 International Conference on Electrical, Electronics and System Engineering (ICEESE)*, 2013, 43-48, doi: 10.1109/ICEESE.2013.6895040.

21. Верусь В.С., Кондратюк О.І., Ляшко С.С. Розумний будинок або автоматизована система керування житлом. *Студентський вісник Національного університету водного господарства та природокористування*. 2019. Вип. 1(11). 119–122.

22. Takahashi H. et al., Improvement of automatic fire extinguisher system for residential use, *2015 International Conference on Informatics, Electronics & Vision (ICIEV)*, 2015, 1-4, doi: 10.1109/ICIEV.2015.7333992.

23. Swain K. B., Dash S. and Gouda S. S., Raspberry PI based Integrated Autonomous Vehicle using LabVIEW, *2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS)*, 2017, 69-73, doi: 10.1109/SSPS.2017.8071567.

24. Дужак І.О. Розумний будинок. *Автоматизація технологічних і бізнес-процесів*. 2013. No 13(13–14). 31-33.

25. Sarath Kumar R., Hariharan J., Revanth R. S., Prasanth K. R. and Lokesh J., Automatic Fire Fighting Robot using RPI, *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, 2021, 136-139, doi: 10.1109/ICOSEC51865.2021.959168

26. Гунько Н.В. SMART HOME як інструмент оптимізації вартості житлово-комунальних послуг в Україні, *Матеріали Науково-практичної Інтернет-конференції «Проблеми регіоналістики: минуле, сучасне, майбутнє»*, КНЕУ, березень 2017 р. С. 228-231

27. Jan H., Yar H., Iqbal J., Farman H., Khan Z. and Koubaa A., Raspberry Pi Assisted Safety System for Elderly People: An Application of Smart Home, *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, 2020, 155-160, doi: 10.1109/SMARTTECH49988.2020.00046.

28. Khan M. N. A., Tanveer T., Khurshid K., Zaki H. and Zaidi S. S. I., Fire Detection System using Raspberry Pi, *2019 International Conference on Information Science and Communication Technology (ICISCT)*, 2019, 1-6, doi: 10.1109/CISCT.2019.8777414.

29. Проєктування комп'ютеризованих систем управління: Опорний конспект лекцій, Тернопіль, ТНЕУ. URL: http://dspace.tneu.edu.ua/retrieve/52377/Лекції_ПКСУ.pdf.

30. Тарарака В.Д. Архітектура комп'ютерних систем: навч. посіб, Житомир: ЖДТУ, 2018. 383 с.

31. Raspberry Pi, URL: https://www.raspberrypi.org/

32. Момот Т.В., Мураєв Є.В. Компаративний аналіз зарубіжних практик розвитку розумних міст та можливості їх імплементації в Україні. *Електронний науково-практичний журнал «Інфраструктура ринку»*. 2020. Вип. 42. 232–237.

33. Nisan N., Schocken S. The Elements of Computing Systems, second edition: Building a Modern Computer from First Principles 2nd Edition, The MIT Press, 2021.

34. Yadin A. Computer Systems Architecture, Chapman and Hall, *CRC*, 2016. 467 p.

35. Null L., Lobur Y. Essentials of Computer Organization and Architecture, *Jones & Bartlett Learning*; 5th edition, 2018. 744 p.

36. Kravets A.G., Bolshakov A.A., M.V. Shcherbakov Cyber-Physical Systems: Industry 4.0 Challenges (Studies in Systems, Decision and Control, 260), *Springer*; 1st ed., 2020. 349 p.

37. Rea P., Ottaviano E., Machado J. and Antosz K. Design, Applications, and Maintenance of Cyber-Physical Systems, *Engineering Science Reference*, 2021. 314 p. DOI: 10.4018/978-1-7998-6721-0

38. Степаненко О.І. Пасивний будинок – шлях до ефективного використання енергії, *Енергетика: економіка, технології, екологія*. 2014. №3.

39. Гайдукевич С.В., Семенова Н.П., Леськів Я.А. Особливості SMART-технологій на прикладі автоматизації житлового будинку, *Таврійський науковий вісник*. №1. 2022. 12-21.

40. Li B. S. X., Wan B., Wang C., Zhou X., Chen X. Definitions of predictability for cyber physical systems, *J. of Systems Architecture*. 2016. DOI: 10.1016/j.sysarc.2016.01.007.

41. Poliakov, M., Larionova, T. Control Systems with programmable logic controllers, Remote and virtual tools in engineering: textbook, general editorship Dr.Ing.Karsten Henke, Zaporizhzhya: Dike Pole, 2016. 250 p.

42. С. Г. Натрошвілі, Г. Р. Натрошвілі, Т. Г. Бабина, Б. М. Злотенко, Т. І. Кулік Комп'ютерно-інтегрована система керування природним і штучним освітленням розумного будинку, *Вісник Хмельницького національного університету. Серія : Технічні науки*. 2020. № 5 (289). 65-71.

43. Monk S. Programming Arduino Next Steps: Going Further with Sketches, *McGraw-Hill Education TAB*, 2018. 320 p.

44. Barrett S.F. Microchip AVR® Microcontroller Primer: Programming and Interfacing, *Morgan & Claypool Publishers*, 2019. 374 p.

45. Papazoglou P. M. An Educational Guide to the AVR Microcontroller Programming: AVR Programming::Demystified (Assembly Language) (Volume 1), *CreateSpace Independent Publishing Platform*, 2018. 274 p.

46. Василенко В. І., Ремізов І.А. Особливості побудови інтелектуальних енергетичних систем будівель та споруд, *Енергетичний менеджмент: стан та перспективи розвитку – PEMS : зб.матеріалів IV міжнар. наук.-техн. конф.*, 4-7 черв. 2019 р. К. : НТУУ «КПІ», 2019. 21-22.

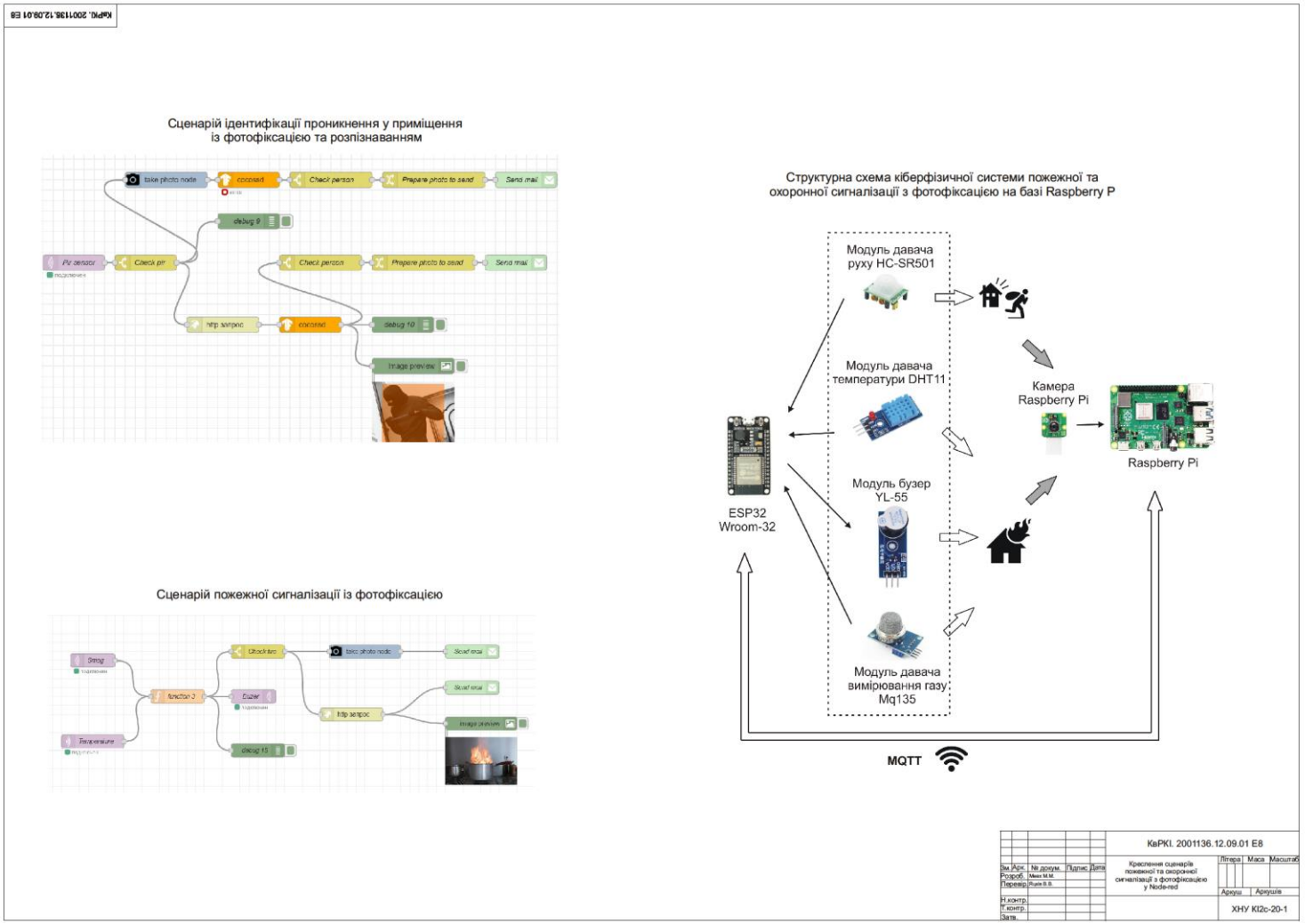
47. Kishita Y., Mizuno Y., Fukushige S., Umeda Y. Scenario structuring methodology for computer-aided scenario design: An application to envisioning sustainable futures, *Technol. Forecast. Soc. Chang*. 2020. 160. 120207

48. Teslyuk, V., Kazarian, A., Kryvinska, N., Tsmots, I., Teslyuk, T. Automated synthesis method of smart home systems based on the architectural pattern redux. *CEUR Workshop Proceedings*, 2019. 2533. 58-69

49. Hu Y., Tilke D., Adams T. et al. Smart home in a box: usability study for a large scale self-installation of smart home technologies. *J Reliable Intell Environ* 2. 2016, 93-106

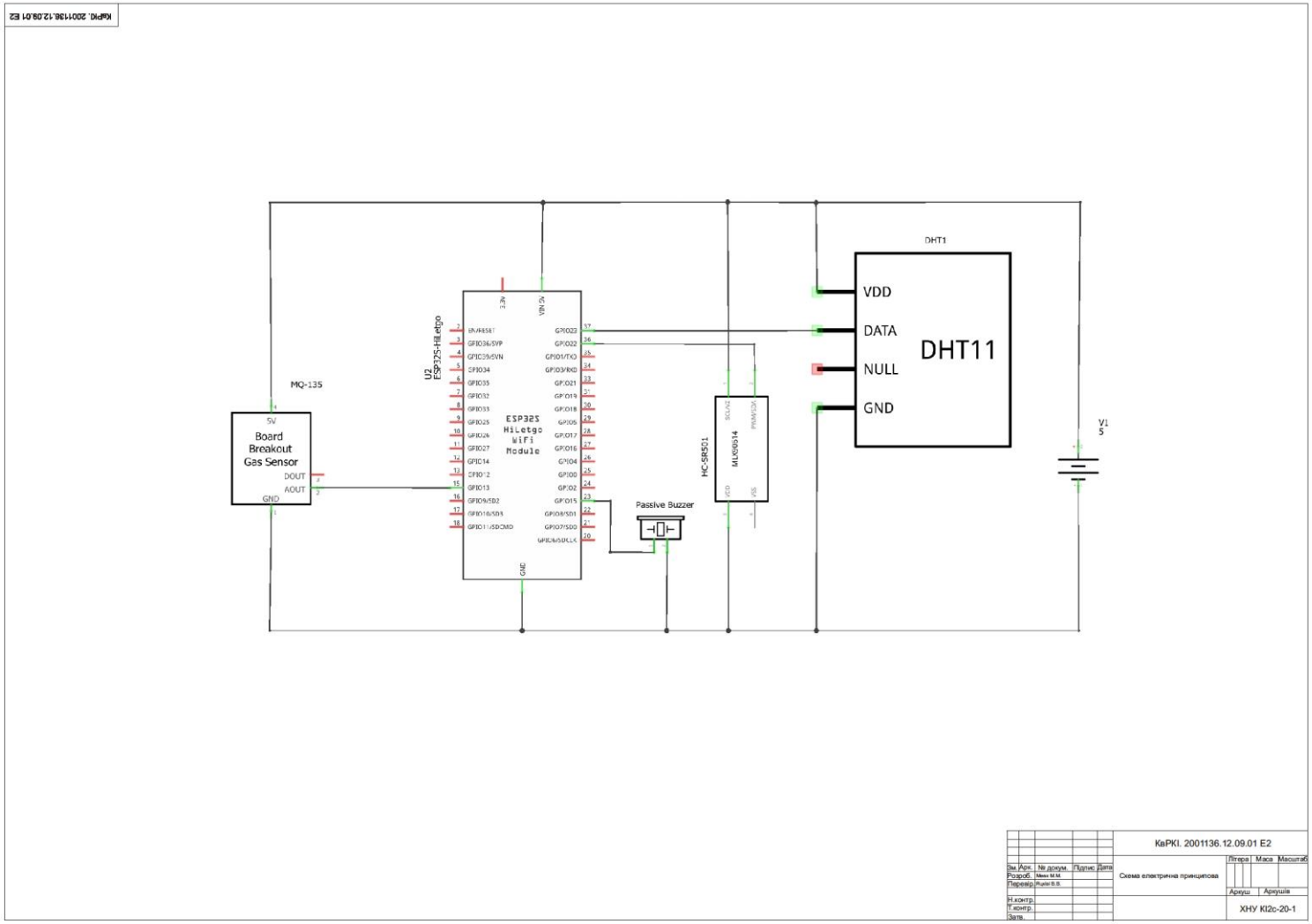
ДОДАТОК А

Копія креслення «Креслення сценаріїв пожежної та охоронної сигналізації з фотофіксацією у Node-red»

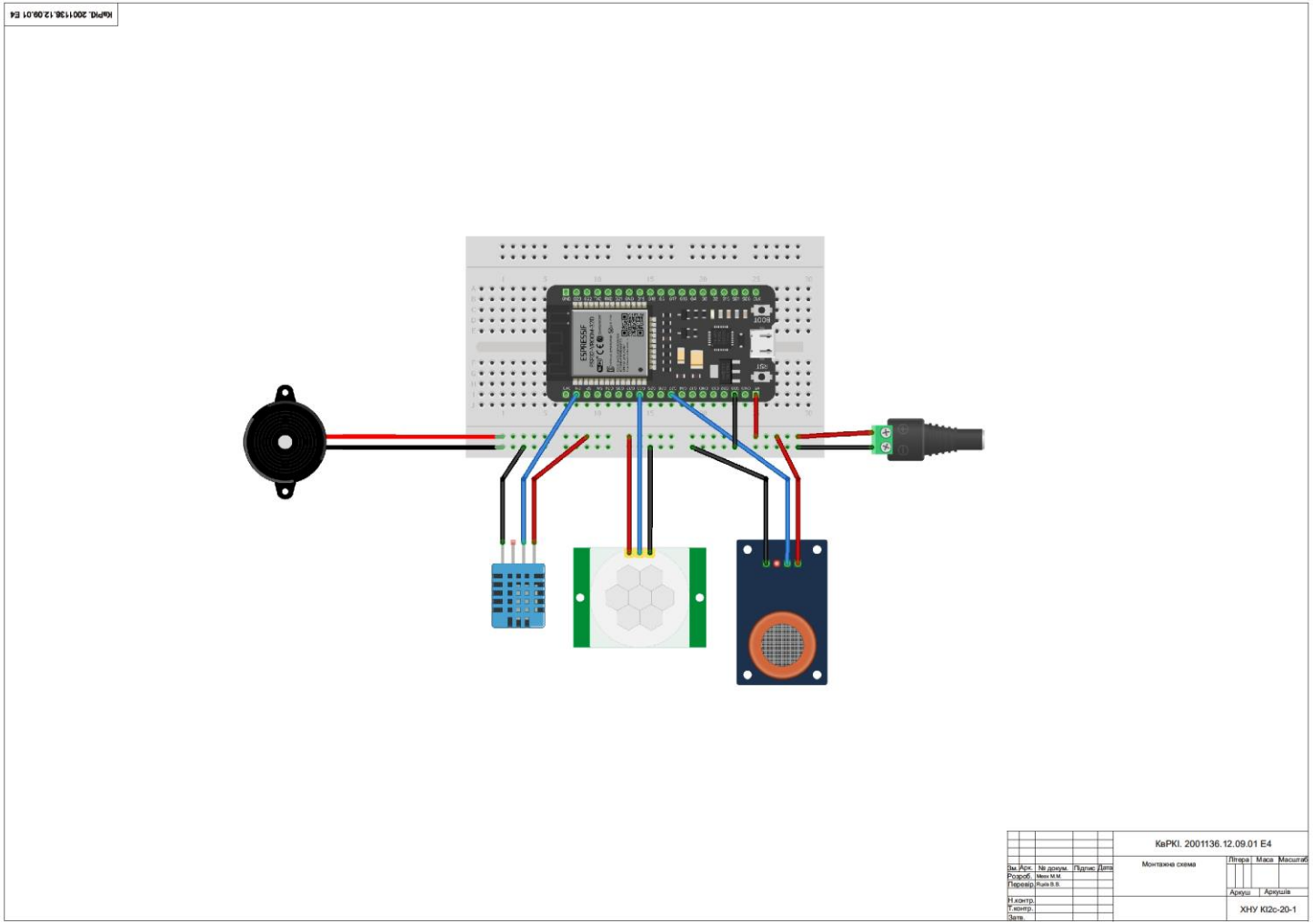


ДОДАТОК Б

Копія креслення «Схема електрична принципова»



ДОДАТОК В
Копія креслення «Монтажна схема»



UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1014814494

Дата перевірки:
26.04.2023 15:46:12 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
26.04.2023 15:47:27 EEST

ID користувача:
100005591

Назва документа: **Мевх_Кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі R...**

Кількість сторінок: **63** Кількість слів: **10013** Кількість символів: **75127** Розмір файлу: **4.80 MB** ID файлу: **1014517653**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

9.15%
Схожість

Найбільша схожість: **4.16%** з Інтернет-джерелом (https://klaster.ua/ua/stati-i-obzory/oborudovanie-dlja-okhranno-pozh...

7.88% Джерела з Інтернету	95	Сторінка 65
3.94% Джерела з Бібліотеки	41	Сторінка 65

0.67% Цитат

Цитати	3	Сторінка 66
Посилання	1	Сторінка 66

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	1
Підозріле форматування	12 сторінок

Wed Apr 26 14:52:51 EEST 2023, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 7.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 18%**

ID: 112609 Назва: БКР Кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi Додано в БД: 2023-04-26 Автора: Мевх М.М. Керівники: Яцків В.В. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	68073	539	5191 (8%)	59 (11%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми
112551	Назва: БКР Програмно-технічний засіб автоматизованого керування освітленням у системі «Розумний будинок» на основі одноплатної комп'ютерної системи Raspberry Pi Додано в БД: 2023-04-25 Автора: М.О. Ратушний Керівники: А.О. Нічепорук Консультанти: Опоненти:	4912 (7.0%)	57 (11.0%)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Мевх Максим Миколайович

Тема: Кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг дипломної роботи:

Кількість листів креслень 3; кількість сторінок записки 56

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано кіберфізичну систему пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi

2. Висновок про відповідність роботи дипломному завданню Дипломний проект відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз предметної області. У другому розділі спроєктовано структуру кіберфізичної системи. У третьому розділі проведено реалізацію кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi

4. Позитивні сторони роботи: Запропоновано структуру кіберфізичної системи пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi та проведено реалізацію сценаріїв у середовищі Node-red

5. Негативні сторони роботи: В роботі не наведено порівняння запропонованого рішення із відомими аналогами, відсутні оцінки кількісних та якісних характеристик розробленого пристрою.

6. Оцінка графічного оформлення та пояснювальної записки роботи: пояснювальна записка та листи креслення виконані згідно діючих вимог

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому рівні.

8. Інші зауваження: –

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої дипломної роботи вважаю, що робота заслуговує оцінки «добре» 3,75 (С)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) к.ф.-м.н., проф. зав. кафедри ІПЗ Бедратих Л.П.

"02" червня 2023р.

Завідувачу кафедри КІС
д-р.техн.наук, проф. Говорущенко Т. О.

Мевх Максим Миколайович
ПІБ здобувача вищої освіти

ФІТ, 3 курсу, групи КІ2с-20-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

02.06.2023
дата

підпис

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Кіберфізична система пожежної та охоронної сигналізації з фотофіксацією на базі Raspberry Pi

Автор: Мевх Максим Миколайович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Яцків Василь Васильович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділі аналізу існуючих аналогів та відомих рішень, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 9,15% і адресується до 155 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В. В. Яцків

Гарант ОП _____ С. М. Лисенко

Завідувач кафедри КІІС _____ Т. О. Говорущенко