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

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266

Назва теми

КвРКІ 022041.22.02.42 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-22-2 _____ Андрій ХЛОПОТ
Підпис — Ініціали, прізвище

Керівник _____ Василь СТЕЦЮК
Підпис, дата — Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата — Ініціали, прізвище

До захисту допускаю:
зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис — Ініціали, прізвище

«16» червня 2025 р.

Хмельницький 2025

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 Ольга ПАВЛОВА

" 10 " 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Андрію ХЛОПОТУ

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266

Керівник проекту (роботи) Василь СТЕЦЮК,старший викладач.

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

Затверджена наказом ректора університету від 07.02.2025 р. № 23

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

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

Система охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266 та постановка задачі щодо її удосконалення

Проєктування системи обробки інформації у системі охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266

Програмно-апаратна реалізація системи охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266

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

Структурна схема ПЗ проєкту

Діаграма активності

Схема алгоритму функціонування системи

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Тетяна КИСІЛЬ, доцент кафедри КІІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІІС		

7. Дата видачі завдання «_10_»________01__________2025 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	10.01.2025	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2025	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2025	виконано
4	Робота над розділом 2 – вибір компонентів для проєктування системи охоронної сигналізації периметра об'єкта	01.04.2025	виконано
5	Робота над розділом 3 – проєктування системи охоронної сигналізації периметра об'єкта	29.04.2025	виконано
6	Оформлення пояснювальної записки згідно вимог	25.05.2025	виконано
7	Попередній захист ВКР	26.05.2025	виконано
8	Захист ВКР на засіданні ЕК	Червень 2025 року	

Студент ________ Андрій ХЛОПОТ
Підпис Ініціали, прізвище

Керівник роботи ________ Василь СТЕЦЮК
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 022041.22.02.42 ПЗ	Пояснювальна записка	55		
			Графічні матеріали			
2		КвРКІ 022041.22.02.42 Е8	Структурна схема ПЗ проєкту	1		
3		КвРКІ 022041.22.02.42 Е8	Діаграма активності	1		
4		КвРКІ 022041.22.02.42 Е8	Схема алгоритму Функціонування системи	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 022041.22.02.42 ВП			
Розробив		Хлопот		7.04.23	Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Стецюк		16.05.23		У	1	1
Н. контр.		Кисіль		16.05.23		ХНУ, КІ2с-22-2		
Затв.		Павлова						

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система охоронної сигналізації периметра об‘єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266»

Автор роботи: Андрій ХЛОПОТ

Керівник роботи: Василь СТЕЦЮК

Пояснювальна записка: 55 с., 6 рис., 3 табл., 3 дод., 26 джерел

Графічна частина: 3 креслення

МІКРОКОНТРОЛЕР, ESP8266, ДАТЧИК РУХУ, СИРЕНА, ПОВІДОМЛЕННЯ, СИСТЕМА БЕЗПЕКИ.

Метою даної роботи є розробка та реалізація системи безпеки на основі мікроконтролера ESP8266, яка здійснює моніторинг руху в певній зоні та сповіщає про можливу небезпеку за допомогою сирени та/або відправки сигналу на сервер.

Об’єктом дослідження є електронні системи безпеки, їх компоненти та взаємодія між датчиками, мікроконтролером і виконавчими елементами.

Предметом дослідження є методи обробки сигналів датчиків руху та магнітних детекторів, реалізація алгоритму функціонування системи безпеки, інтеграція з мікроконтролером ESP8266 та реалізація сповіщення через сирену.

Практичне значення полягає в тому, що розроблена система безпеки на базі мікроконтролера ESP8266 є ефективним інструментом для забезпечення безпеки на об'єктах. Система дозволяє автоматично виявляти рух, генерувати попереджувальні сигнали та забезпечувати моніторинг в реальному часі через підключення до інтернету.

Хлопот А

Підпис студента

30.05.2025

Дата

ЗМІСТ

Зм.	Арк.	№докум.	Підпис	Дата	КвРКІ 022041.22.02.42 ПЗ		
Виконав		Хлопот А.В.			Система охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266	Літера: У	Аркуш: 2
Перевір.		Стещок В.М.					Аркушів: 55
Н.контр.		Кисіль Т.М.				ХНУ КІ2с-22-2	
Затвер.		Павлова О.О.					

ВСТУП

Актуальність теми

Система охорони периметра є важливим елементом забезпечення безпеки різноманітних об'єктів, зокрема в таких критичних сферах, як промисловість, військові частини, склади, а також інші стратегічно важливі об'єкти. Використання автоматизованих технологій для моніторингу та оповіщення в реальному часі стає все більш важливим в умовах постійного розвитку технологій і збільшення кількості загроз. Одним з таких рішень є система охоронної сигналізації, яка забезпечує своєчасне виявлення порушень і перевищення критичних значень параметрів на об'єкті. Система, що передає дані на WEB-сервер на базі мікроконтролера ESP8266, дозволяє забезпечити безперервний моніторинг і оперативну реакцію на зміни, що робить її надзвичайно актуальною для сучасних підприємств.

В умовах високих вимог до безпеки та ефективності моніторингу, створення програмних рішень для інтеграції датчиків в єдину систему вимагає врахування численних факторів, таких як швидкість передачі даних, надійність з'єднання, збереження історії подій та реалізація інтуїтивно зрозумілого інтерфейсу для користувачів. Важливим аспектом є й інтеграція з іншими системами безпеки, що використовуються на об'єкті, що дозволяє створити комплексну систему захисту. Використання мікроконтролера ESP8266, який підтримує бездротову передачу даних через Wi-Fi, відкриває нові можливості для інтеграції різноманітних датчиків і зниження витрат на інфраструктуру.

Тематика автоматизованих систем охорони, зокрема в промислових об'єктах, набуває значної популярності через свою ефективність і здатність забезпечити надійний захист від несанкціонованого доступу. Пошук оптимальних рішень для реалізації таких систем вимагає використання передових технологій в області інформаційних технологій, програмування та електроніки. Сучасні системи оповіщення повинні враховувати не лише базові функції сповіщення про

порушення, але й оперативно аналізувати дані з численних датчиків для виявлення критичних ситуацій.

Завдяки розвитку бездротових технологій і доступності мікроконтролерів для побудови таких систем, досягнення високої надійності і швидкості обробки даних стало реальністю. Крім того, інтеграція таких систем у загальну інфраструктуру об'єкта дозволяє суттєво підвищити рівень безпеки, здійснюючи моніторинг не лише охоронних параметрів, але й таких, як температура, вологість, рівень руху тощо, що є важливими для безпеки в певних середовищах, таких як ливарні цехи.

Успішна розробка і впровадження таких систем дозволяє не лише підвищити безпеку об'єкта, але й зменшити ризики для персоналу, уникнути матеріальних втрат і потенційно небезпечних ситуацій. Таким чином, питання створення ефективних та надійних систем охоронної сигналізації з передачею даних на WEB-сервер на базі мікроконтролера ESP8266 набуває особливої важливості у світлі швидкого розвитку нових технологій.

Необхідність у застосуванні новітніх технологій в області автоматизованих систем охорони є невід'ємною частиною розвитку сучасної промисловості та підприємництва, оскільки це дозволяє оптимізувати витрати та підвищити рівень безпеки. Інноваційні підходи, які поєднують технології передачі даних, обробки інформації та інтеграції з іншими системами безпеки, є ключовими для забезпечення ефективної роботи таких комплексних систем.

Мета і завдання дослідження

Метою цього дослідження є розробка ефективної автоматизованої системи охорони периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266, яка включає зчитування та обробку даних датчиків, а також реалізацію інтерфейсу користувача для оперативного моніторингу і сповіщення про критичні ситуації.

Завдання дослідження:

– Аналіз сучасних технологій автоматизованих систем охорони;

– Розробка програмного забезпечення для зчитування та обробки даних датчиків;

– Оцінка ефективності передачі даних через мікроконтролер ESP8266;

– Створення інтерфейсу користувача для моніторингу та управління системою;

– Розробка алгоритмів для сповіщення про критичні параметри в реальному часі;

– Оцінка надійності та безпеки переданої інформації.

Об'єкт дослідження

Об'єктом дослідження є система охоронної сигналізації, що включає датчики, мікроконтролер ESP8266, сервер для зберігання та обробки даних, а також інтерфейс користувача для моніторингу та управління.

Предмет дослідження

Предметом дослідження є технології зчитування та обробки даних від датчиків, методи передачі даних через бездротову мережу, а також розробка інтерфейсу користувача для моніторингу стану об'єкта.

1 АНАЛІЗ І ТЕОРЕТИЧНІ ОСНОВИ ОХОРОННИХ СИСТЕМ

1.1 Аналіз сучасних систем охоронної сигналізації та їх особливостей

Сучасні системи охоронної сигналізації активно розвиваються у напрямку підвищення надійності, оперативності реагування та зручності інтеграції з інформаційними технологіями. В умовах зростаючої загрози несанкціонованого доступу до територій різного призначення, включаючи промислові об'єкти, житлові комплекси, складські приміщення та інші критично важливі зони, попит на ефективні охоронні рішення значно зростає.

Більшість сучасних систем охоронної сигналізації поділяються на дротові та бездротові. Дротові рішення залишаються популярними завдяки високому рівню стабільності передачі сигналу, однак вимагають складного монтажу та мають обмежену гнучкість у конфігурації. Бездротові системи, навпаки, дозволяють швидко розгортати охоронну мережу, однак можуть страждати від перешкод та втрат сигналу внаслідок впливу зовнішніх чинників [1, с. 16].

Однією з важливих особливостей новітніх систем є здатність інтеграції з інтернетом та передача даних на хмарні або локальні WEB-сервери. Це дає змогу не лише отримувати оповіщення у реальному часі, а й вести архів подій, контролювати стан системи з будь-якої точки світу та оперативно реагувати на загрози. Технології Internet of Things (IoT) все частіше використовуються в охороні, дозволяючи створювати розумні системи спостереження.

Значну роль у сучасних охоронних системах відіграють мікроконтролери, серед яких особливу популярність здобув ESP8266 завдяки своїй доступності, вбудованому Wi-Fi-модулю та сумісності з різними датчиками. Це дозволяє розробляти бюджетні, але ефективні охоронні рішення для різних об'єктів, зокрема й для промислових зон, таких як ливарні цехи.

У контексті промислових об'єктів, до яких належать ливарні цехи, охоронна сигналізація має враховувати специфіку середовища, включаючи високі температури, пил, шум та інші фактори, що можуть впливати на стабільність

роботи електронного обладнання. Саме тому важливо використовувати надійні компоненти та передбачати можливість резервування каналів зв’язку.

Зазвичай у таких умовах система охорони виконує не лише функцію контролю доступу до об'єкта, а й функції оповіщення про критичні значення параметрів навколишнього середовища, наприклад, температури, вологості або наявності диму. Це значно підвищує рівень безпеки та дозволяє запобігти аварійним ситуаціям на ранніх етапах. Існують різні підходи до побудови систем охоронної сигналізації: централізовані, децентралізовані або гібридні. У централізованих системах вся інформація стікається до одного центру керування, тоді як у децентралізованих – обробка сигналів може виконуватись локально, на рівні мікроконтролера. Гібридні підходи дозволяють поєднувати переваги обох моделей, підвищуючи надійність та швидкість реагування.

Розробка систем охоронної сигналізації часто базується на використанні цифрових датчиків руху, інфрачервоних сенсорів, магнітоконтактних датчиків для контролю дверей та вікон, а також камер відеоспостереження. У поєднанні з мікроконтролером ESP8266 вони формують ефективне рішення для віддаленого моніторингу периметра [2, с. 12].

Підключення до WEB-сервера відіграє важливу роль у фіксації інцидентів та веденні журналу подій. За допомогою протоколів HTTP або MQTT дані передаються до сервера, де зберігаються для подальшого аналізу або відображення на веб-інтерфейсі. Це надає змогу швидко ідентифікувати джерело загрози та прийняти відповідні заходи. Ще однією важливою рисою сучасних систем є здатність до самодіагностики. Такі системи можуть повідомляти про несправності у своїй роботі: обрив лінії, розряд батареї, втрату зв'язку з сервером. Це зменшує ризик того, що система вийде з ладу непомітно для користувача.

Системи охоронної сигналізації можуть бути інтегровані з іншими елементами автоматизації об'єкта, наприклад, системами пожежогасіння, вентиляції або управління освітленням. Це дозволяє реалізувати концепцію «розумного підприємства», де всі елементи працюють узгоджено задля підвищення загальної ефективності.

Особливої актуальності набуває використання охоронних систем у ливарних цехах, де існує постійний ризик техногенних аварій, пов’язаних із перегрівом обладнання, витоком металу або короткими замиканнями. У таких випадках своєчасне повідомлення про критичні зміни параметрів може врятувати майно, ресурси і навіть життя персоналу [3, с. 44].

Враховуючи велику площу ливарного цеху, доцільно використовувати модульну структуру системи охорони з розміщенням кількох вузлів на базі ESP8266, кожен з яких відповідатиме за свою ділянку периметра або зони контролю. Це забезпечує масштабованість системи та знижує ризики повного виходу з ладу у разі відмови одного з модулів. На сьогодні значну увагу приділяють також захисту переданих даних. У системах, які підключені до WEB-серверів, обов’язково має бути реалізоване шифрування трафіку та автентифікація користувачів, щоб уникнути несанкціонованого доступу до інформації або можливих кібератак.

Загалом, сучасні охоронні системи стають невід’ємною частиною комплексної безпеки об'єктів. Їх розвиток спрямований на підвищення автономності, розумної обробки інформації, адаптивності до умов середовища та зручності взаємодії з користувачем через WEB-інтерфейси.

1.2 Огляд можливостей мікроконтролера ESP8266 у побудові системи охорони

Мікроконтролер ESP8266 став одним із найпопулярніших рішень у сфері розробки бюджетних систем автоматизації та охорони завдяки своїй універсальності, компактності та низькій вартості. Його головна перевага полягає у вбудованому модулі Wi-Fi, що дозволяє створювати пристрої з можливістю бездротової передачі даних без необхідності додаткових модулів зв’язку. У контексті охоронних систем це означає можливість віддаленого моніторингу стану об'єкта у режимі реального часу [4, с. 27].

Завдяки підтримці стандартних протоколів зв’язку, таких як TCP/IP, HTTP, MQTT, ESP8266 може бути інтегрований у практично будь-яку систему, яка взаємодіє з сервером або хмарним сховищем. Це відкриває широкі можливості для створення систем оповіщення, які надсилають повідомлення про спрацювання датчиків або зміну критичних параметрів об'єкта на WEB-інтерфейс користувача.

Мікроконтролер підтримує роботу з великою кількістю цифрових і аналогових датчиків, таких як сенсори руху, температури, вологості, магнітні контакти, ультразвукові датчики відстані, детектори газу та диму. Це дозволяє гнучко формувати архітектуру охоронної системи відповідно до специфіки об'єкта, на якому вона впроваджується. Особливо корисним це є у випадках промислових об’єктів, де необхідно відстежувати не тільки проникнення, а й небезпечні зміни в умовах середовища.

ESP8266 має достатню обчислювальну потужність для обробки сигналів від декількох сенсорів одночасно. За необхідності можна реалізувати локальну логіку опрацювання даних без участі сервера, наприклад, генерувати тривогу при перевищенні встановлених порогів або збої у роботі одного з елементів системи. Це підвищує автономність охоронної системи, робить її стійкою до втрати зв’язку з мережею.

Оскільки ESP8266 підтримує функції енергозбереження, він придатний для використання в автономних системах з живленням від батарей або сонячних панелей. Такий підхід дозволяє розміщувати охоронні пристрої в важкодоступних місцях, де немає можливості провести дротове живлення, що особливо важливо при охороні великих промислових периметрів або віддалених технічних зон.

Окрім цього, ESP8266 легко програмується за допомогою середовищ, таких як Arduino IDE або PlatformIO. Це робить його доступним для широкого кола розробників, включаючи студентів, інженерів-початківців та аматорів. Завдяки великій спільноті користувачів, існує багато готових бібліотек і прикладів коду, які полегшують процес розробки та скорочують час впровадження системи.

У побудові охоронної системи ESP8266 часто використовується як центральний вузол, що приймає дані від датчиків і передає їх на WEB-сервер або у

вигляді повідомлень користувачу. Він також може виступати у ролі ретранслятора або вузла обробки даних у більш складних мережах, де використовується кілька пристроїв. Така масштабованість дозволяє адаптувати систему під конкретні потреби без значних змін в архітектурі. Однією з сильних сторін ESP8266 є можливість налаштування роботи у режимі точки доступу (Access Point) або клієнта мережі (Station). Це дозволяє розгортати як централізовані, так і децентралізовані системи, де кожен мікроконтролер працює незалежно, зберігаючи при цьому зв'язок із загальним сервером або управляючим пристроєм [5, с. 33].

У охоронних системах також важливо мати можливість реєстрації та логування подій. ESP8266 може зберігати події локально у пам'яті або передавати їх у вигляді HTTP-запитів до бази даних на WEB-сервері, де інформація зберігається для подальшого аналізу. Це дозволяє відслідковувати історію подій, виявляти закономірності та удосконалювати алгоритми виявлення загроз.

ESP8266 здатен працювати у режимі реального часу з мінімальними затримками, що дозволяє оперативно реагувати на події, такі як відкриття дверей, поява руху, підвищення температури тощо. У системах охорони це має вирішальне значення, оскільки навіть кількасекундна затримка може вплинути на ефективність реагування.

У разі використання датчиків, які вимагають аналогового зчитування, ESP8266 забезпечує обробку таких сигналів за допомогою вбудованого аналогово-цифрового перетворювача. Це розширює перелік сумісних сенсорів, зокрема газоаналізаторів або датчиків тиску, що також можуть бути застосовані у спеціалізованих охоронних системах.

Системи охорони, створені на базі ESP8266, можуть бути обладнані інтерфейсами керування – наприклад, веб-сторінками з HTML-інтерфейсом для відображення поточного стану датчиків, журналу подій або керування режимами роботи (охорона, техобслуговування, тривога). Такі інтерфейси можна переглядати з будь-якого пристрою, підключеного до мережі, що забезпечує високу зручність для користувачів.

Ще одним напрямом використання ESP8266 є інтеграція з голосовими асистентами або месенджерами для отримання тривожних сповіщень. Наприклад, система може надсилати повідомлення на Telegram або Email у випадку спрацювання одного з датчиків, що значно підвищує мобільність та інформованість користувача. Можливість регулярного оновлення прошивки ESP8266 "по повітрю" (Over-the-Air, OTA) дозволяє вносити зміни до програмної логіки без фізичного доступу до пристрою. Це важливо у випадках встановлення охоронних систем у важкодоступних місцях або для підтримки безперервної роботи пристрою.

Мікроконтролер ESP8266 також може бути використаний для забезпечення високої безпеки комунікацій між різними компонентами охоронної системи завдяки вбудованим механізмам шифрування. Це важливо, оскільки в системах, що передають чутливі дані, необхідно забезпечити захист від несанкціонованого доступу. Використання стандартних протоколів шифрування, таких як WPA2 для Wi-Fi з'єднань, дозволяє значно підвищити рівень безпеки при передаванні даних між пристроями та сервером. Це дозволяє уникнути ризиків перехоплення або модифікації інформації.

Ще одним важливим аспектом використання ESP8266 є можливість реалізації багатокористувацького доступу до охоронної системи. Веб-інтерфейс, що працює на основі ESP8266, може бути налаштований для підтримки різних рівнів доступу, що дозволяє адміністраторам, охоронцям і навіть кінцевим користувачам мати різні права для перегляду або керування системою. Це дозволяє гнучко налаштовувати права доступу в залежності від конкретних вимог безпеки.

Додатково, ESP8266 підтримує роботу з мобільними додатками, що розширює можливості використання охоронної системи. Наприклад, можна створити мобільний додаток, який дозволяє користувачам отримувати сповіщення про спрацьовування датчиків або переглядати дані системи в реальному часі. Мобільні додатки для iOS та Android можуть бути інтегровані з сервером через MQTT або HTTP, що дозволяє реалізувати гнучке й оперативне реагування на події.

Для більш складних охоронних систем ESP8266 може бути використаний для створення мережі з кількох пристроїв, де кожен мікроконтролер відповідає за певну

зону об'єкта. Це дозволяє організувати масштабовану систему охорони, де кожен вузол може незалежно збирати і передавати дані на загальний сервер для подальшого аналізу. Така архітектура дозволяє ефективно управляти великими об'єктами з мінімальними витратами на інфраструктуру.

Ще однією перевагою ESP8266 є його здатність працювати в умовах слабкого сигналу або з обмеженим доступом до мережі. Це стає можливим завдяки підтримці режиму Mesh, де кілька пристроїв взаємодіють між собою, формуючи мережу з низьким енергоспоживанням та можливістю підтримки зв'язку на великих відстанях. Така мережа дозволяє створювати складні системи охорони для великих територій, де можуть бути розташовані кілька зон з різними датчиками. Іншою цікавою особливістю є можливість налаштування та оновлення програмного забезпечення для ESP8266 віддалено. Ця функція, відома як OTA (Over-the-Air), дозволяє розробникам зручно виправляти помилки, оновлювати прошивку або додавати нові функції без фізичного доступу до пристроїв, що є важливим, особливо для віддалених або важкодоступних об'єктів. Це значно спрощує підтримку та вдосконалення системи в процесі її експлуатації.

Для підвищення точності і надійності датчиків, підключених до ESP8266, можна застосувати зовнішні плати розширення. Наприклад, використання A/D перетворювачів для більш точного зчитування аналогових сигналів або спеціалізованих сенсорів для виявлення певних газів або частинок у повітрі дозволяє створити більш складні і точні системи охорони. Це особливо корисно в умовах, де важливим є не лише виявлення проникнення, але й моніторинг навколишнього середовища для забезпечення безпеки працівників або мешканців.

Додатково, система на основі ESP8266 може бути інтегрована з іншими автоматизованими системами об’єкта, такими як освітлення, опалення чи кондиціювання, для досягнення синергії в управлінні периметром та загальною безпекою. Наприклад, спрацювання датчиків охорони може автоматично включити освітлення у разі виявлення руху, що не лише покращує безпеку, але й дозволяє заощаджувати енергію в разі неактивності [6, с. 21].

Мікроконтролер ESP8266 також дозволяє побудувати багатофункціональні системи оповіщення, що підтримують різні способи передачі тривожних сигналів. Це може включати не лише повідомлення на мобільні пристрої або електронну пошту, а й інтеграцію з сиренами, візуальними сигналами або навіть системами автоматичного виклику служб безпеки. Це дозволяє забезпечити надійне та оперативне реагування на будь-які спроби проникнення чи інші загрози.

Для збереження налаштувань і параметрів системи в разі відключення живлення, можна використовувати додаткові елементи, такі як акумулятори або конденсатори, які дозволяють ESP8266 продовжувати працювати навіть при короткочасних перебоях в електроживленні. Це забезпечує безперервну роботу системи в умовах нестабільного електричного живлення.

Мікроконтролер ESP8266 також може бути застосований для інтеграції з іншими сторонніми платформами для моніторингу і управління охоронною системою. Наприклад, можливість зв’язку з такими популярними платформами, як Blynk або Home Assistant, відкриває нові можливості для створення кастомізованих інтерфейсів і додатків для управління та моніторингу безпеки в реальному часі.

Таким чином, мікроконтролер ESP8266 є потужним інструментом у побудові охоронних систем нового покоління. Його функціональні можливості, підтримка бездротового зв’язку, енергоефективність та програмна гнучкість роблять його ідеальним вибором для розробки масштабованих, надійних і доступних систем безпеки для промислових об’єктів, таких як ливарні цехи та інші важливі інфраструктурні об'єкти.

1.3 Вибір архітектури системи та обґрунтування використання WEB-сервера для передачі даних

У процесі розробки системи охоронної сигналізації одним з ключових етапів є вибір архітектури. Саме архітектурне рішення визначає ефективність, масштабованість та надійність системи в реальних умовах експлуатації. Залежно від особливостей об'єкта, вимог до безпеки, кількості точок контролю та рівня

автоматизації, можуть застосовуватись централізовані, децентралізовані або комбіновані підходи до побудови охоронної системи.

У контексті охорони периметра промислового об’єкта, зокрема ливарного цеху, доцільно реалізовувати децентралізовану або гібридну архітектуру. Це дозволяє розміщувати кілька вузлів на базі мікроконтролера ESP8266 по периметру території, кожен з яких контролює локальні датчики та передає зібрані дані на центральний WEB-сервер. Такий підхід підвищує стійкість системи до відмов окремих вузлів та дозволяє зменшити навантаження на центральний контролер [7, с. 18].

Головною перевагою архітектури з передачею даних на WEB-сервер є можливість організації віддаленого доступу до інформації у режимі реального часу. Завдяки цьому користувачі можуть моніторити стан охоронної системи з будь-якого пристрою, підключеного до Інтернету. Це особливо актуально для керівників підприємств, охоронного персоналу або операторів, які відповідають за безпеку об'єкта в різні зміни.

WEB-сервер виступає у системі в ролі центрального вузла збереження, обробки та візуалізації даних. До нього надходять сигнали тривоги, повідомлення про зміну стану датчиків, інформація про несправності та інші події. За допомогою серверного ПЗ здійснюється облік подій, їх сортування, збереження у базі даних та відображення у вигляді графіків, журналів або інтерфейсів сповіщення.

Передача даних на WEB-сервер через інтернет забезпечується вбудованим Wi-Fi-модулем ESP8266, що дозволяє уникати складної мережевої інфраструктури. Замість прокладання дротів або встановлення додаткових шлюзів, кожен вузол самостійно передає дані на сервер, що значно спрощує монтаж системи та знижує витрати на обладнання. Важливо також зазначити, що серверна частина може бути реалізована на базі відкритих технологій, таких як Apache, Nginx, PHP, Node.js або Python Flask. Це забезпечує гнучкість при налаштуванні функціоналу, можливість інтеграції з іншими системами (відеоспостереження, пожежна сигналізація, СКУД) та адаптацію інтерфейсу під потреби користувача.

Реалізація WEB-сервера відкриває можливість організації багаторівневого доступу до даних – наприклад, технічному персоналу можуть бути доступні функції діагностики, а охороні – лише відображення стану охоронної зони. Це сприяє розподілу відповідальності та підвищує інформаційну безпеку всієї системи. Для того щоб розробити таку структуру організації WEB-серверу охоронної сигналізації потрібно видати потрібні права користувачам охоронної системи, запобігаючи виданню зайвих прав, що може привести до помилкових дій користувача системи охоронної сигналізації.

Одним із важливих факторів на користь використання WEB-сервера є можливість архівування подій. Завдяки цьому можна отримати статистику за довільний проміжок часу, виявити аномалії у роботі системи, перевірити ефективність реагування персоналу на тривоги або оцінити частоту технічного обслуговування. У разі необхідності система може бути налаштована на автоматичне сповіщення відповідальних осіб у разі надзвичайних ситуацій – наприклад, через електронну пошту, Telegram або SMS. Для цього на сервері можна реалізувати додаткові скрипти, які активуються за певними умовами, такими як виявлення проникнення, тестування, відключення живлення або втрата зв’язку з вузлом.

Правильний вибір архітектури з використанням WEB-сервера також полегшує процес масштабування системи та дозволяє масштабувати систему швидко та уникати додаткових витрат на масштабування системи охоронної сигналізації. При розширенні охоронної зони достатньо додати нові вузли ESP8266, налаштувати їх для передачі даних на сервер – і система буде готова до роботи без повного оновлення інфраструктури, що полегшить майбутнє масштабування.

Нижче представлена таблиця, яка порівнює особливості трьох основних архітектур охоронних систем: централізованої, децентралізованої та гібридної. Це дозволяє краще зрозуміти переваги і недоліки саме гібридної архітектури з WEB-сервером для конкретного випадку, для мінімізації недоліків у системі охоронної сигналізації.

Таблиця 1.3.1 – Порівняння архітектур охоронних систем

Критерій	Централізована	Децентралізована	Гібридна
Надійність при відмові вузла	Низька	Висока	Висока
Гнучкість у масштабуванні	Обмежена	Висока	Висока
Складність реалізації	Низька	Середня	Вища
Реакція на події	Централізована	Локальна	Локальна + централізована
Вартість впровадження	Середня	Низька	Середня
Можливість аналізу даних	Часткова	Обмежена	Повна (через сервер)
Вимоги до інтернет-зв’язку	Високі	Середні	Середні

Як видно з таблиці, саме гібридна архітектура поєднує в собі переваги двох підходів – централізованого керування та локальної автономності. Це дозволяє створити ефективну, гнучку та стійку до збоїв охоронну систему. [8, с. 39]

Вибір архітектури з використанням WEB-сервера також полегшує процес масштабування системи. При розширенні охоронної зони достатньо додати нові вузли ESP8266, налаштувати їх для передачі даних на сервер – і система буде готова до роботи без повного оновлення інфраструктури. Важливою особливістю є також можливість дистанційного налаштування та оновлення програмного забезпечення всіх вузлів через інтернет, що значно знижує потребу в фізичному доступі до пристроїв, знижуючи витрати на обслуговування та мінімізуючи ризики при оновленнях.

Ще одним важливим аспектом є інтеграція WEB-сервера з іншими зовнішніми системами, такими як система управління доступом (СКУД) або інтелектуальні відеокамери. Це дозволяє створити єдину платформу для управління не лише охоронними датчиками, а й іншими елементами безпеки, забезпечуючи більш глибоке інтегроване спостереження за об'єктами. В такому випадку система не лише фіксує порушення безпеки, а й автоматично коригує доступ на об'єкт в залежності від ситуації. Завдяки таким інтеграціям, система може

бути налаштована на спільну роботу з іншими технологіями, такими як біометричні системи і розпізнавання осіб, що додатково підвищує рівень безпеки об'єкта.

Крім того, наявність інтеграції із зовнішніми сервісами дозволяє реалізувати складніші алгоритми реагування на події. Наприклад, система може бути налаштована таким чином, щоб в разі виявлення тривоги, вона не лише відправляла повідомлення про подію, а й автоматично активувала додаткові заходи безпеки, такі як блокування виходів, включення освітлення на території, або запуск додаткових моніторингових пристроїв, що забезпечить швидку реакцію на інциденти.

Одним з перспективних напрямів є впровадження штучного інтелекту для аналізу даних, що надходять на сервер. Система може автоматично оцінювати рівень загрози на основі зібраних даних, таких як тривожні сигнали, зміни в патернах поведінки на об'єкті або незвичні дії персоналу. Використання таких технологій дозволить зменшити людський фактор у прийнятті рішень та підвищити ефективність реагування на інциденти. Крім того, штучний інтелект може бути використаний для прогнозування потенційних загроз на основі історичних даних і моделей поведінки.

Завдяки впровадженню таких інноваційних підходів у розробку архітектури системи охорони, можна досягти високого рівня автоматизації, що знижує ризики помилок, забезпечує швидке реагування на різноманітні загрози та створює умови для ефективного моніторингу за великими об'єктами з мінімальними затратами часу та ресурсів. Технології, що використовуються для зберігання та обробки даних, також можуть бути оптимізовані для використання в умовах промислових об'єктів, що значно підвищує надійність та безпеку системи [9, с. 15].

Таким чином, обґрунтований вибір архітектури на базі мікроконтролерів ESP8266 з передачею даних на WEB-сервер дозволяє побудувати інтелектуальну систему охорони, яка буде відповідати сучасним вимогам безпеки, зручності в обслуговуванні та інтеграції з іншими системами автоматизації. Цей підхід дозволяє легко масштабувати систему та забезпечує оперативне інформування користувача про всі критичні події.

2 РОЗРОБКА СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

2.1 Проектування схеми підключення датчиків до мікроконтролера ESP8266

Проєктування схеми підключення датчиків до мікроконтролера ESP8266 є критичним етапом у створенні системи охоронної сигналізації. На цьому етапі необхідно врахувати як функціональні, так і технічні параметри взаємодії мікроконтролера з периферійними пристроями, що відповідають за виявлення загроз та передачу сигналу. У нашій системі будуть використовуватись датчики руху (PIR-сенсори), магнітні датчики (геркони), а також додаткові сенсори (наприклад, температурні або вібраційні), залежно від вимог до рівня безпеки об'єкта. Кожен із цих сенсорів має власну специфіку підключення, яку необхідно враховувати при проєктуванні [10, с. 7].

Мікроконтролер ESP8266 має обмежену кількість портів GPIO, які можна використовувати як входи або виходи. Для ефективного використання цих портів потрібно правильно розподілити сигнали, враховуючи логіку обробки інформації в прошивці. Наприклад, для PIR-сенсора зручно використовувати GPIO5, оскільки він підтримує вхідні сигнали й не конфліктує з процесом завантаження мікроконтролера.

Підключення магнітного геркона може здійснюватися до GPIO4. Цей датчик працює як звичайний перемикач, замкнений у нормальному стані, а при відкриванні дверей або вікна – розмикається. Це дозволяє просто реалізувати логіку “тривога / немає тривоги”. Живлення датчиків є ще одним важливим елементом підключення. PIR-сенсори зазвичай працюють при напрузі 5 В, але сигнал на виході має логічний рівень 3.3 В, сумісний з ESP8266. У випадку, коли вихід сенсора має 5 В, потрібно використовувати резистивний дільник або логічний перетворювач рівня для захисту входів ESP8266.

Для спрощення схеми можна використовувати загальні лінії живлення та землю, проклавши їх до всіх датчиків. Важливо також уникати зашумлених

сигналів, особливо для датчиків, розташованих на великій відстані від плати керування. Для цього можна застосувати фільтруючі конденсатори та виту пару.

Щоб зменшити кількість фізичних з'єднань, можливо застосування мультиплексорів або цифрових портів розширення через шину I2C. Наприклад, модуль PCF8574 дозволяє отримати додаткові входи/виходи, які можна використовувати для обробки великої кількості сенсорів без перевантаження GPIO ESP8266. Особливу увагу слід приділити правильній обробці сигналів із датчиків. Необхідно передбачити “debounce” – програмне або апаратне усунення дрібних коливань сигналу, які виникають при замиканні контактів, наприклад, у герконі. Інакше можливе помилкове спрацювання сигналізації.

Система також має містити елемент зворотного зв’язку – оповіщення. Сирена або бузер може бути підключений до GPIO2, який конфігурується як вихід. Для керування бузером використовується транзисторний ключ, керований з ESP8266, оскільки мікроконтролер не може самостійно подавати достатній струм для живлення звукового елементу.

Живлення ESP8266 має бути стабілізованим. Він працює при напрузі 3.3 В, тому при використанні джерела 5 В необхідний стабілізатор, наприклад AMS1117-3.3. Слід також додати конденсатори на вході та виході стабілізатора для фільтрації пульсацій. Для забезпечення оновлення прошивки та налагодження слід під’єднати UART-інтерфейс. Це можливо через USB-UART адаптер, який підключається до контактів TX і RX ESP8266. Важливо передбачити перемикачі або джампери для активації режиму програмування мікроконтролера [11, с. 23].

Ще однією важливою деталлю є індикатори. Наприклад, світлодіод, що вказує на активний стан Wi-Fi або тривогу. Такі світлодіоди можна підключити через резистор до GPIO0 або GPIO13. Вони дозволяють візуально контролювати стан системи без підключення до WEB-інтерфейсу.

Для зв’язку з WEB-сервером ESP8266 використовує вбудований Wi-Fi модуль. Після обробки сигналу з датчиків, мікроконтролер відправляє HTTP-запит або дані на віддалений сервер або хмарний сервіс. Це дає змогу контролювати стан системи дистанційно через браузер або мобільний застосунок.

Під час проєктування необхідно протестувати макет системи, змоделювавши поведінку кожного з датчиків. Такий підхід дозволяє виявити можливі конфлікти, проблеми із живленням або збої в логіці керування ще до монтажу на постійну плату.

У результаті, правильне проєктування схеми підключення датчиків до ESP8266 забезпечує стабільну, масштабовану й безпечну роботу системи охоронної сигналізації. Всі компоненти повинні бути сумісні за напругою та струмом, а також правильно підключені відповідно до електричних характеристик мікроконтролера [12, с. 64].

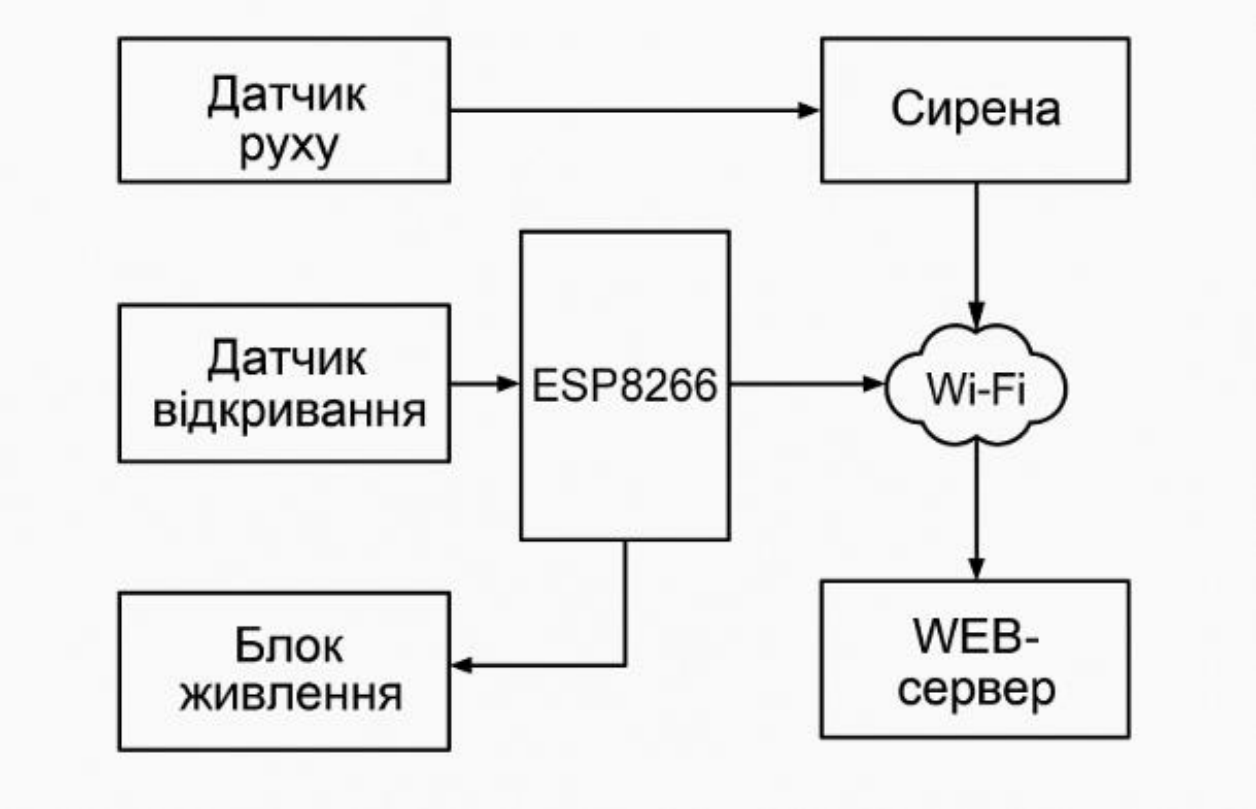


Рисунок 2.1.1 – Схема електрична структурна системи сповіщення

За допомогою схеми електричної структури можна завчасно зобразити взаємодію компонентів системи охоронної сигналізації периметра об’єкта.

Нижче представлена схема електричної функціональної системи, яка використовується при об’єднуванні модулів системи охоронної сигналізації периметра об’єкта з передачею даних на WEB-сервер на базі мікроконтроллера ESP8266.

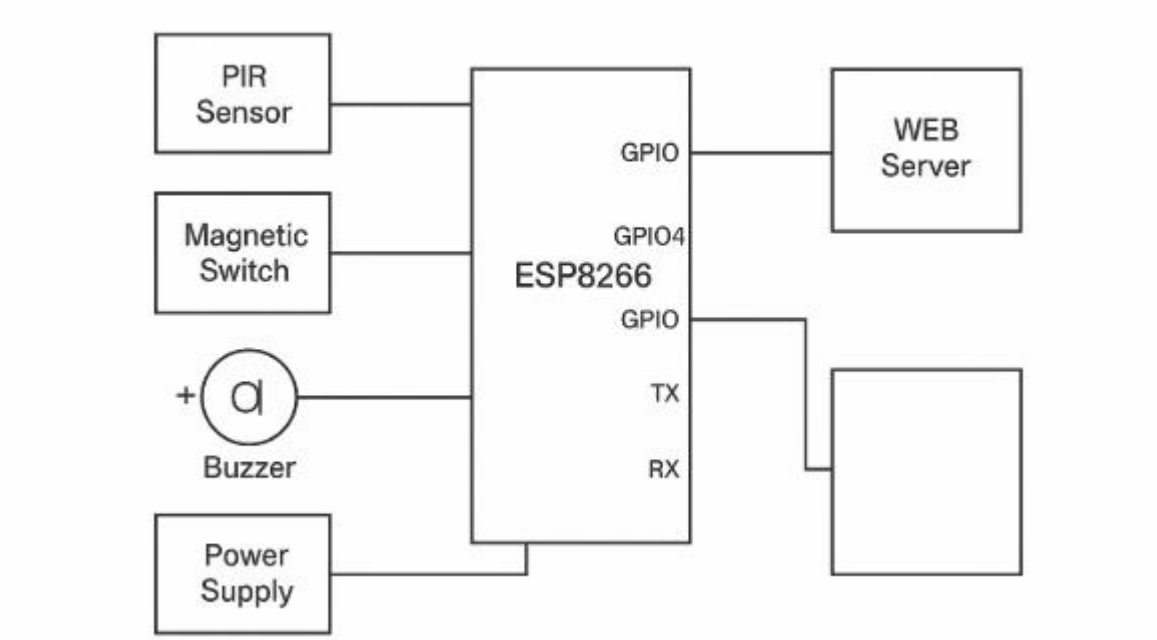


Рисунок 2.1.2 – схема електричної функціональної системи сповіщення

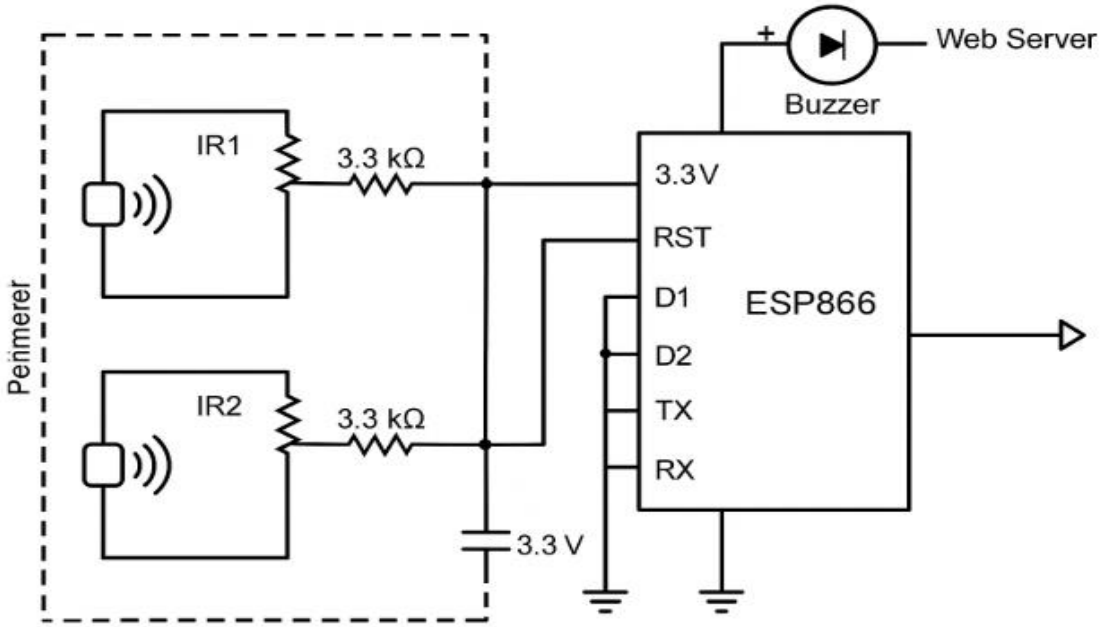


Рисунок 2.1.3 – Схема електрична принципова системи сповіщення

2.2 Розробка програмного забезпечення для зчитування та обробки даних датчиків

У процесі розробки системи охоронної сигналізації периметра об’єкта, що передає дані на WEB-сервер на базі мікроконтролера ESP8266, особливу увагу слід

приділити програмному забезпеченню для зчитування та обробки даних датчиків, а також створенню алгоритмів, які дозволяють ефективно опрацьовувати отриману інформацію. Це необхідно для забезпечення своєчасного сповіщення про порушення охорони або перевищення критичних параметрів на території об'єкта, зокрема в ливарному цеху.

Основною метою розробки такого програмного забезпечення є створення інтерфейсу, здатного ефективно обробляти дані з численних датчиків, що встановлені в різних точках периметра охорони. Для цього необхідно налаштувати взаємодію між датчиками, мікроконтролером ESP8266 та сервером, що зберігає всі отримані дані, обробляє їх і надає інформацію користувачеві через інтерфейс на веб-сервері [13, с. 9].

Програмне забезпечення для зчитування даних датчиків має забезпечити швидке й безперервне отримання інформації про зміни параметрів навколишнього середовища, таких як температура, вологість, рух чи інші фактори, що можуть впливати на безпеку об'єкта. Для досягнення цієї мети використовується відповідне програмування мікроконтролера ESP8266, що включає налаштування для збору і передачі даних на сервер у реальному часі.

Алгоритм роботи системи передбачає регулярне зчитування даних від датчиків, що дозволяє постійно контролювати стан периметра об'єкта. Інформація від датчиків передається через бездротову мережу Wi-Fi, що забезпечує високу швидкість передачі даних без необхідності проводити кабелі, що значно полегшує установку і зменшує витрати на інфраструктуру.

Крім того, програмне забезпечення має інтегрувати систему оповіщення, яка буде спрацьовувати при досягненні критичних значень параметрів. У ливарному цеху, де температурні показники і рівень вологості є критичними для безпеки, важливо своєчасно реагувати на перевищення допустимих меж. Для цього в програмному коді розробляються алгоритми, що здійснюють порівняння поточних значень з установленими критеріями і при їх порушенні надсилають повідомлення на сервер.

Оповіщення про критичні значення параметрів буде здійснюватися за допомогою електронної пошти або через смс-повідомлення на мобільний телефон, що дозволить оперативно реагувати на загрозу. Важливою складовою є також налаштування часового інтервалу між перевірками датчиків, що дозволяє зберігати баланс між швидкістю збору даних і енергозбереженням, оскільки ESP8266 є малопотужним пристроєм і потребує оптимізації ресурсів.

Забезпечення безперервного моніторингу також вимагає наявності алгоритмів для аналізу зібраної інформації. Програмне забезпечення повинно здійснювати не тільки фіксацію поточних значень параметрів, а й зберігати історичні дані, що дозволяє проводити аналіз змін у часі. Це має важливе значення для виявлення потенційних проблем або змін у стані охорони об'єкта, що можуть вказувати на порушення чи несанкціоновані дії.

Крім того, система повинна бути гнучкою для впровадження нових датчиків та параметрів, що дозволяє в подальшому розширювати функціональність без необхідності переписувати програмне забезпечення. Для цього використовуються модульні алгоритми, де кожен датчик має свій власний модуль, який може бути легко змінений або доданий без порушення роботи всієї системи. Зокрема, для розробки програмного забезпечення використовуються мови програмування, які дозволяють інтегрувати ESP8266 з різними типами датчиків. Наприклад, для роботи з датчиками температури і вологості використовуються популярні бібліотеки, такі як DHT, що дозволяє легко налаштувати зв'язок між датчиком і мікроконтролером [14, с. 30].

Для обробки даних датчиків і передавання їх на веб-сервер використовується протокол HTTP або MQTT, що дає можливість обмінюватися даними в реальному часі з мінімальними затримками. Система на сервері обробляє ці дані, що дозволяє створювати детальні звіти, графіки і показники для операторів, які здійснюють моніторинг.

Задача обробки даних також включає в себе фільтрацію шуму, що дозволяє усунути випадкові зміни в даних, викликані зовнішніми факторами, такими як

зміни в погодних умовах чи інші непередбачувані події. Це забезпечує більшу точність вимірювань і дозволяє системі реагувати тільки на реальні загрози.

Розробка програмного забезпечення також передбачає інтеграцію з іншими системами безпеки, які можуть бути в рамках об'єкта. Наприклад, наявність камери спостереження або системи контролю доступу може бути об'єднана з даними датчиків для підвищення рівня охорони. Інтерфейс програмного забезпечення має бути інтуїтивно зрозумілим і дозволяти швидко отримувати інформацію про стан усіх підключених датчиків [15, с. 47].

Програмне забезпечення повинно підтримувати функцію оновлення, що дозволяє безпечно і безперервно вдосконалювати систему без необхідності зупиняти її роботу. Це може включати в себе оновлення алгоритмів обробки даних або зміну критеріїв для сповіщень про критичні значення.

У процесі розробки системи охоронної сигналізації периметра об’єкта, що передає дані на WEB-сервер на базі мікроконтролера ESP8266, особливу увагу слід приділити програмному забезпеченню для зчитування та обробки даних датчиків, а також створенню алгоритмів, які дозволяють ефективно опрацьовувати отриману інформацію. Це необхідно для забезпечення своєчасного сповіщення про порушення охорони або перевищення критичних параметрів на території об'єкта, зокрема в ливарному цеху.

Основною метою розробки такого програмного забезпечення є створення інтерфейсу, здатного ефективно обробляти дані з численних датчиків, що встановлені в різних точках периметра охорони. Для цього необхідно налаштувати взаємодію між датчиками, мікроконтролером ESP8266 та сервером, що зберігає всі отримані дані, обробляє їх і надає інформацію користувачеві через інтерфейс на веб-сервері [16, с. 60].

Програмне забезпечення для зчитування даних датчиків має забезпечити швидке й безперервне отримання інформації про зміни параметрів навколишнього середовища, таких як температура, вологість, рух чи інші фактори, що можуть впливати на безпеку об'єкта. Для досягнення цієї мети використовується відповідне

програмування мікроконтролера ESP8266, що включає налаштування для збору і передачі даних на сервер у реальному часі.

Алгоритм роботи системи передбачає регулярне зчитування даних від датчиків, що дозволяє постійно контролювати стан периметра об'єкта. Інформація від датчиків передається через бездротову мережу Wi-Fi, що забезпечує високу швидкість передачі даних без необхідності проводити кабелі, що значно полегшує установку і зменшує витрати на інфраструктуру.

Крім того, програмне забезпечення має інтегрувати систему оповіщення, яка буде спрацьовувати при досягненні критичних значень параметрів. У ливарному цеху, де температурні показники і рівень вологості є критичними для безпеки, важливо своєчасно реагувати на перевищення допустимих меж. Для цього в програмному коді розробляються алгоритми, що здійснюють порівняння поточних значень з установленими критеріями і при їх порушенні надсилають повідомлення на сервер.

Оповіщення про критичні значення параметрів буде здійснюватися за допомогою електронної пошти або через смс-повідомлення на мобільний телефон, що дозволить оперативно реагувати на загрозу. Важливою складовою є також налаштування часового інтервалу між перевірками датчиків, що дозволяє зберігати баланс між швидкістю збору даних і енергозбереженням, оскільки ESP8266 є малопотужним пристроєм і потребує оптимізації ресурсів.

Забезпечення безперервного моніторингу також вимагає наявності алгоритмів для аналізу зібраної інформації. Програмне забезпечення повинно здійснювати не тільки фіксацію поточних значень параметрів, а й зберігати історичні дані, що дозволяє проводити аналіз змін у часі. Це має важливе значення для виявлення потенційних проблем або змін у стані охорони об'єкта, що можуть вказувати на порушення чи несанкціоновані дії [17, с. 36].

Крім того, система повинна бути гнучкою для впровадження нових датчиків та параметрів, що дозволяє в подальшому розширювати функціональність без необхідності переписувати програмне забезпечення. Для цього використовуються модульні алгоритми, де кожен датчик має свій власний модуль, який може бути

легко змінений або доданий без порушення роботи всієї системи. Зокрема, для розробки програмного забезпечення використовуються мови програмування, які дозволяють інтегрувати ESP8266 з різними типами датчиків. Наприклад, для роботи з датчиками температури і вологості використовуються популярні бібліотеки, такі як DHT, що дозволяє легко налаштувати зв'язок між датчиком і мікроконтролером.

Для обробки даних датчиків і передавання їх на веб-сервер використовується протокол HTTP або MQTT, що дає можливість обмінюватися даними в реальному часі з мінімальними затримками. Система на сервері обробляє ці дані, що дозволяє створювати детальні звіти, графіки і показники для операторів, які здійснюють моніторинг.

Задача обробки даних також включає в себе фільтрацію шуму, що дозволяє усунути випадкові зміни в даних, викликані зовнішніми факторами, такими як зміни в погодних умовах чи інші непередбачувані події. Це забезпечує більшу точність вимірювань і дозволяє системі реагувати тільки на реальні загрози.

Розробка програмного забезпечення також передбачає інтеграцію з іншими системами безпеки, які можуть бути в рамках об'єкта. Наприклад, наявність камери спостереження або системи контролю доступу може бути об'єднана з даними датчиків для підвищення рівня охорони. Інтерфейс програмного забезпечення має бути інтуїтивно зрозумілим і дозволяти швидко отримувати інформацію про стан усіх підключених датчиків.

Програмне забезпечення повинно підтримувати функцію оновлення, що дозволяє безпечно і безперервно вдосконалювати систему без необхідності зупиняти її роботу. Це може включати в себе оновлення алгоритмів обробки даних або зміну критеріїв для сповіщень про критичні значення [18, с. 24].

У результаті розроблене програмне забезпечення повинно забезпечувати надійний та ефективний моніторинг стану об'єкта, що дозволяє швидко реагувати на порушення або зміни параметрів, що можуть загрожувати безпеці. Важливим аспектом є забезпечення високої надійності програмного забезпечення і його

безпеки, оскільки система охорони є критично важливою для забезпечення безпеки об'єкта.

У результаті розроблене програмне забезпечення повинно забезпечувати надійний та ефективний моніторинг стану об'єкта, що дозволяє швидко реагувати на порушення або зміни параметрів, що можуть загрожувати безпеці. Важливим аспектом є забезпечення високої надійності програмного забезпечення і його безпеки, оскільки система охорони є критично важливою для забезпечення безпеки об'єкта.

2.3 Організація передачі даних на WEB-сервер та реалізація інтерфейсу користувача

Передача даних на веб-сервер є важливим етапом у розробці системи охоронної сигналізації, оскільки це дозволяє забезпечити доступ до інформації про стан об'єкта в реальному часі. Враховуючи використання мікроконтролера ESP8266, який підтримує бездротову передачу даних через Wi-Fi, важливо забезпечити надійний і швидкий обмін інформацією між мікроконтролером та сервером, на якому зберігається та обробляється інформація з датчиків. Для цього розробляються спеціальні алгоритми, що дозволяють передавати дані у вигляді запитів через інтернет-протоколи, зокрема HTTP або MQTT, в залежності від вимог до швидкості та надійності передачі.

Основною метою організації передачі даних є забезпечення безперервного моніторингу параметрів охорони об'єкта. Мікроконтролер ESP8266 передає дані з датчиків на сервер, де вони обробляються та зберігаються для подальшого використання. Сервер може бути як локальним, так і віддаленим, що дозволяє зберігати дані для доступу з будь-якої точки, підключеної до інтернету. Програма на мікроконтролері регулярно зчитує інформацію від датчиків та передає її на сервер через HTTP-запити, забезпечуючи таким чином постійну актуалізацію даних [19, с. 223].

Для реалізації надійної передачі даних важливо використовувати протоколи, які гарантують стабільну і швидку передачу. Протокол HTTP забезпечує простоту використання та інтеграцію з багатьма веб-серверами, а також дозволяє швидко обробляти запити від користувача. Водночас, для більш стабільної та швидкої передачі даних в реальному часі можна застосовувати протокол MQTT, що є оптимальним для передачі невеликих обсягів даних з мінімальними затримками. У цьому випадку дані від мікроконтролера надходять на сервер через послідовні повідомлення, що дозволяє знижувати навантаження на мережу.

Однією з ключових задач є забезпечення безпеки при передачі даних. Враховуючи, що система охорони є критично важливою для безпеки об'єкта, всі дані, що передаються через мережу, повинні бути зашифровані, щоб запобігти їх перехопленню або модифікації сторонніми особами. Для цього використовуються сучасні методи криптографії, зокрема SSL/TLS, що забезпечує захищений канал передачі даних між мікроконтролером та сервером. Це гарантує, що вся інформація буде передаватися в зашифрованому вигляді, що значно підвищує рівень безпеки системи.

Реалізація інтерфейсу користувача на веб-сервері є важливою складовою частиною проекту, оскільки вона дозволяє операторам зручно переглядати дані про стан об'єкта та отримувати сповіщення про потенційні загрози. Інтерфейс повинен бути інтуїтивно зрозумілим, простим у використанні та забезпечувати швидкий доступ до важливої інформації. Для цього розробляється графічний інтерфейс, який надає візуальне представлення даних, що зчитуються з датчиків, а також дозволяє отримувати сповіщення про критичні ситуації.

Для реалізації інтерфейсу користувача використовуються сучасні веб-технології, такі як HTML, CSS та JavaScript. HTML відповідає за структуру сторінки, CSS – за її оформлення, а JavaScript – за взаємодію з користувачем і динамічне оновлення даних. Через JavaScript користувач може отримувати повідомлення про зміни в стані об'єкта без необхідності перезавантажувати сторінку, що значно покращує взаємодію з системою. Інтерфейс має включати відображення даних у реальному часі. Це можуть бути показники температури,

вологості, рівня руху або інших важливих параметрів, що фіксуються датчиками на периметрі об'єкта. Для зручності користувачів інформація повинна бути представлена у вигляді графіків або таблиць, що дозволяє швидко оцінити ситуацію та вжити необхідних заходів.

Крім того, важливою частиною інтерфейсу є система сповіщень, яка інформує користувача про критичні значення параметрів або про спрацювання сигналізації. Сповіщення можуть бути представлені у вигляді спливаючих вікон, повідомлень у вигляді смс або електронних листів, що дозволяє оперативно реагувати на загрозу навіть за межами об'єкта. Це особливо важливо для ливарного цеху, де порушення технологічних параметрів може призвести до серйозних наслідків.

Інтерфейс також має забезпечувати можливість налаштування параметрів сигналізації та критичних значень для кожного датчика. Це дозволяє користувачам адаптувати систему до змінюваних умов експлуатації або специфічних вимог охорони. Наприклад, оператор може змінити поріг температури або вологості, при якому система почне спрацьовувати, в залежності від ситуації на об'єкті. [20, с. 18]

Для зручності користувачів також реалізується функціонал з історії подій, що дозволяє переглядати дані про всі попередні сповіщення, зміни параметрів і події, що відбулися на об'єкті. Це важливо для аналізу ситуацій та виявлення потенційних проблем або слабких місць у системі охорони. Історія подій також може включати час і дату кожного події, що дозволяє відстежувати зміни у часі.

Один з ключових аспектів інтерфейсу – це можливість доступу до даних з будь-якого пристрою, підключеного до інтернету. Це може бути персональний комп'ютер, планшет або мобільний телефон. Для цього веб-інтерфейс адаптовано під різні пристрої, що дозволяє користувачам зручно взаємодіяти з системою, незалежно від того, який пристрій вони використовують. Система також повинна підтримувати багаторівневу систему доступу, що дозволяє надавати різні права користувачам. Наприклад, деякі користувачі можуть тільки переглядати дані, в той час як інші можуть налаштовувати систему або отримувати сповіщення про

критичні ситуації. Це дозволяє підвищити безпеку системи, обмежуючи доступ до чутливої інформації.

Для забезпечення стабільної та ефективної передачі даних з мікроконтролера ESP8266 на веб-сервер важливо врахувати можливість тимчасового збоїв у з'єднанні. У таких випадках система повинна мати функціонал автоматичного відновлення з'єднання, щоб гарантувати безперервний моніторинг стану об'єкта. У разі втрати з'єднання мікроконтролер має спробувати встановити нове з'єднання через визначені інтервали часу. Це дозволяє уникнути втрат даних і забезпечує оперативне поновлення зв'язку після відновлення мережі.

Один із важливих аспектів функціонування системи – це оптимізація передачі даних для зменшення навантаження на мережу та зниження ймовірності затримок при обробці запитів. Для цього використовуються спеціальні алгоритми стиснення даних перед передачею, що дозволяє зменшити обсяг інформації, яка передається через мережу. Стиснення даних допомагає значно знизити витрати на пропускну здатність каналу та підвищити ефективність роботи системи, особливо в умовах обмежених ресурсів.

Також важливою складовою є організація збору та обробки даних у реальному часі. Для цього на сервері створюються спеціальні процеси, які обробляють отримані від мікроконтролера дані і формують з них необхідні звіти або сповіщення для користувачів. Важливо налаштувати обробку таких даних у вигляді інформаційних блоків, що дозволяють швидко й ефективно інтерпретувати отриману інформацію.

Для того щоб забезпечити надійний доступ до системи для користувачів, розробляється багаторівнева система автентифікації. Вона дозволяє контролювати доступ до різних функцій веб-інтерфейсу, забезпечуючи безпеку та контроль за правами користувачів. Це важливо для обмеження доступу до критичних налаштувань і даних, що можуть бути використані для змін у роботі системи.

Для аналізу великих обсягів зібраних даних на сервері також передбачена можливість створення звітів, графіків та інших візуальних елементів, що допомагають операторам в оперативному моніторингу та прийнятті рішень.

Розробка таких візуалізацій здійснюється з використанням сучасних бібліотек для побудови графіків, таких як Chart.js або D3.js, що дозволяє оперативно оцінювати зміну параметрів на об'єкті.

Окрім цього, доцільно передбачити в системі можливість налаштування параметрів інтерфейсу в реальному часі, щоб користувачі могли коригувати межі спрацьовування сигналізації або вимоги до оповіщень, не вимикаючи систему. Це дає можливість адаптувати систему під різні умови роботи або специфічні вимоги охорони, зберігаючи при цьому високу ефективність роботи всієї системи. Ще одним важливим аспектом є використання кешування для зберігання часто використовуваних даних на веб-сервері. Це дозволяє зменшити навантаження на базу даних, прискорити доступ до інформації та підвищити загальну швидкість роботи інтерфейсу.

Програмне забезпечення також повинно забезпечити автоматичне оновлення даних у реальному часі без необхідності перезавантаження веб-сторінки. Для цього використовуються техніки веб-сокетів або AJAX-запитів, що дозволяє безперервно отримувати нову інформацію про стан об'єкта та сповіщати користувачів про критичні зміни без необхідності повторно відкривати або оновлювати сторінку.

Таким чином, організація передачі даних на веб-сервер та реалізація інтерфейсу користувача є важливими етапами розробки системи охорони. Вони забезпечують зручний і надійний доступ до інформації, підвищують ефективність моніторингу стану об'єкта та дозволяють здійснювати своєчасне реагування на потенційні загрози.

Найбільш важливою складовою розробки ситеми охоронної сигналізації периметра об’єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266 є розробка серверної частини та її взаємодії із базою даних. Для розробки серверної частини я обрав мову програмування Python та фреймворк Flask.

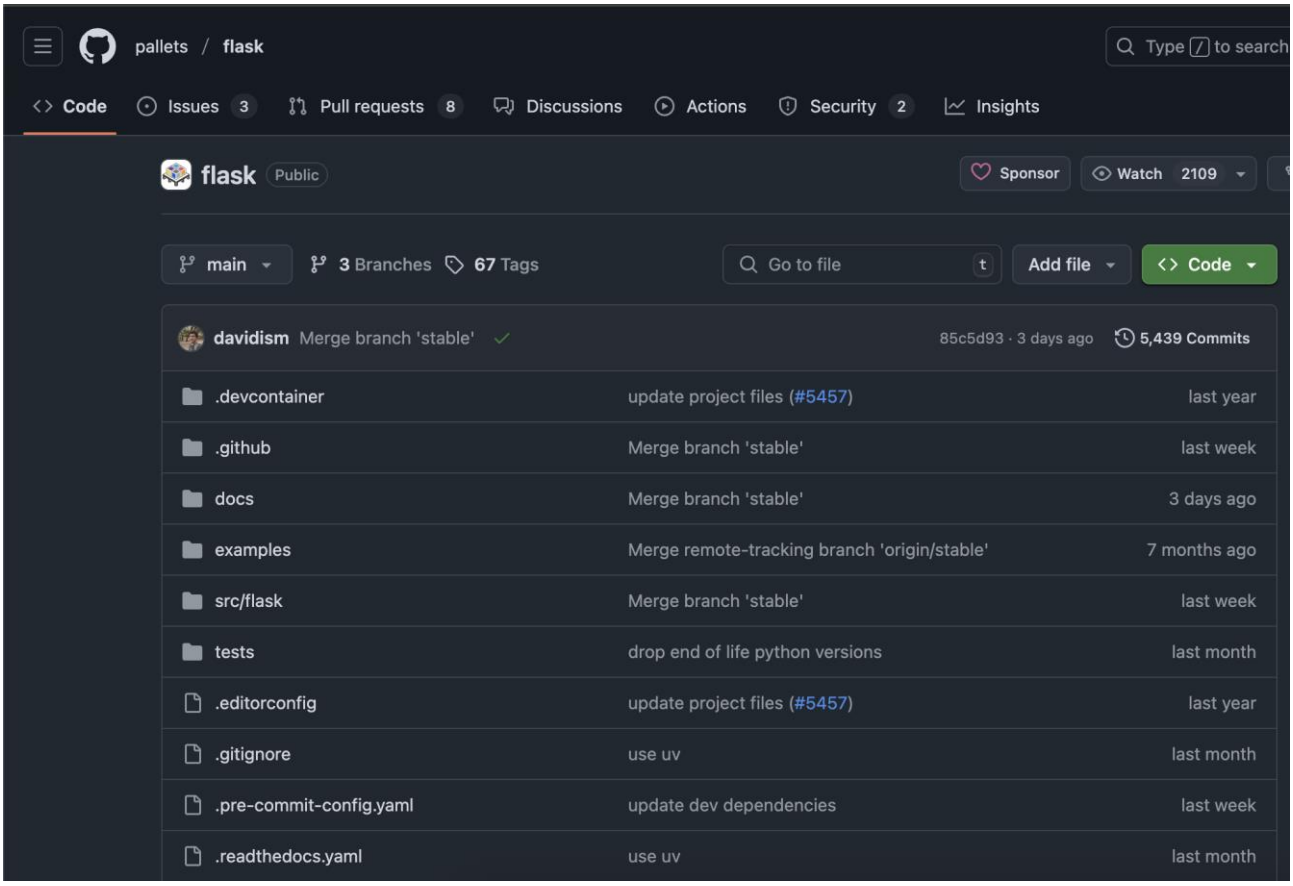


Рисунок 2.3.1 – Git-репозиторій фреймворку Flask

Переваги мови програмування Python:

– легкість використання;

– спектр можливостей;

– наявність великої кількості допоміжних матеріалів та документації.

Фреймворк – це набір готових інструментів, бібліотек та правил, що спрощують і прискорюють розробку програмного забезпечення.

Він задає структуру (каркас) для створення застосунків і дозволяє зосередитися на логіці програми, замість того щоб писати все з нуля.

Основні риси фреймворку:

– має архітектуру (наприклад, MVC);

– визначає стандарти і конвенції**;**

– включає готові модулі (для маршрутизації, роботи з базою даних тощо);

– керує потоком виконання.

Переваги фреймворку Flask:

– малий розмір

– низьке використання потужностей фреймворком

– Мінімальний об’єм завантажуваних за стандартом бібліотек

Для взаємодії із базою даних з використанням фреймворку Python Flask найчастіше використовують ORM-систему SQLAlchemy, що дозволяє швидко створювати запити до бази даних, уникаючи взаємодії з мовою SQL, натомість використовуючи лише код мовою програмування Python. Також ORM-система SQLAlchemy дозволяє створити відображення бази даних у коді за допомогою створення класів відповідно до таблиці бази даних, та використовувати міграції, що значно полегшує процес створення та нормалізації бази даних через механіку роботи міграцій.

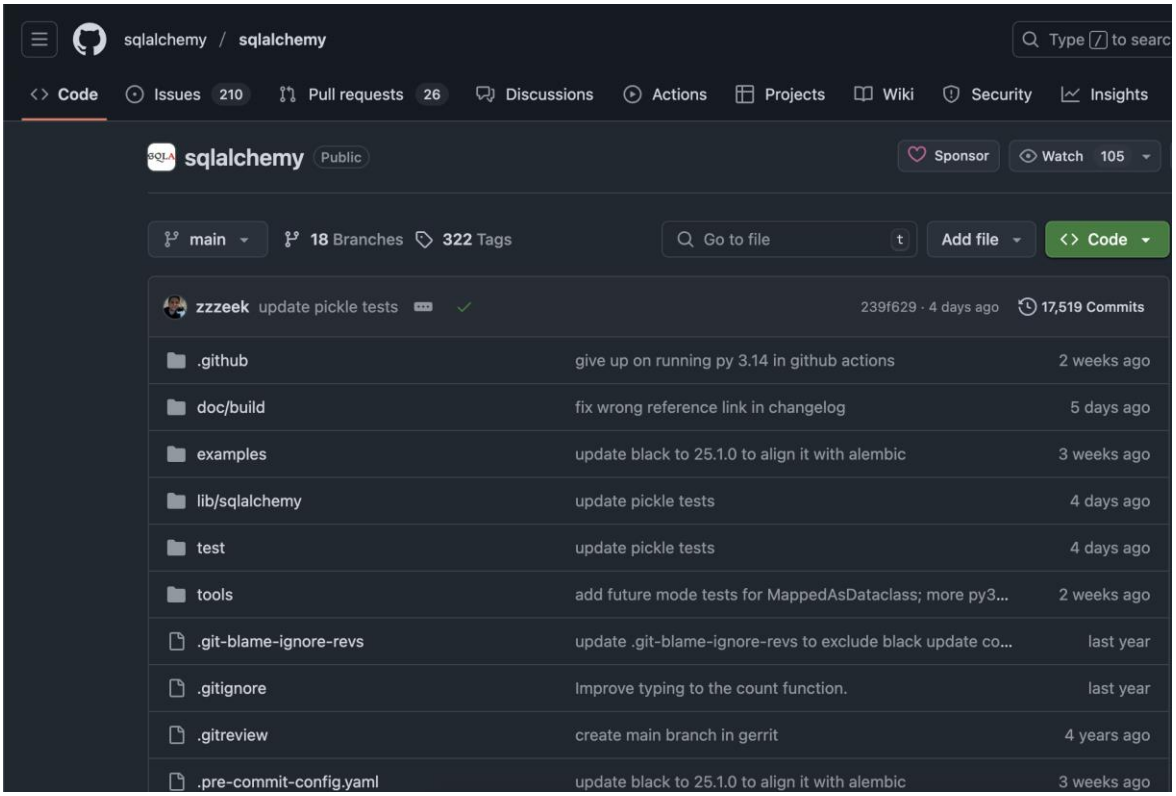


Рисунок 2.3.2 – Git-репозиторій ORM-системи SQLAlchemy

ORM-система – це технологія, яка дозволяє працювати з базою даних, використовуючи об’єктно-орієнтований підхід замість написання сирих SQL-запитів.

```
>>> from typing import List
>>> from typing import Optional
>>> from sqlalchemy import ForeignKey
>>> from sqlalchemy import String
>>> from sqlalchemy.orm import DeclarativeBase
>>> from sqlalchemy.orm import Mapped
>>> from sqlalchemy.orm import mapped_column
>>> from sqlalchemy.orm import relationship

>>> class Base(DeclarativeBase):
...     pass

>>> class User(Base):
...     __tablename__ = "user_account"
...
...     id: Mapped[int] = mapped_column(primary_key=True)
...     name: Mapped[str] = mapped_column(String(30))
...     fullname: Mapped[Optional[str]]
...
...     addresses: Mapped[List["Address"]] = relationship(
...         back_populates="user", cascade="all, delete-orphan"
...     )
...
...     def __repr__(self) -> str:
...         return f"User(id={self.id!r}, name={self.name!r}, fullname={self.fullname!r}
```

Рисунок 2.3.3 – Приклад опису моделей бази даних за допомогою SQLAlchemy

Для швидкого та зручного згортання та розгортання під час розробки системи охоронної сигналізації периметру об’єкта з передачею даних на WEB-сервер я використовував систему контейнерів Docker.

Для контейеру із базою даних я використав офіційний ресурс Docker, а саме контейнер із базою даних PostgreSQL. Для контейнеру із кодом WEB-серверу я створив Dockerfile, який потрібен для ініціювання та створення контейнеру Docker. Такий файл містить у собі ініціювання версії мови програмування Python, встановлення додаткових модулів до операційної системи (за необхідності) та встановлення потрібних python-бібліотек, які попередньо записуються у файл requirements.txt.

Таблиця 2.3.1 – Порівняння протоколів для передачі даних

Протокол	Переваги	Недоліки	Використання
HTTP	Простота використання, підтримка багатьох серверів, інтеграція з веб-сервісами	Висока затримка при передачі великих обсягів даних	Підходить для стандартних запитів і передачі невеликих обсягів інформації
MQTT	Легкий, швидкий, оптимізований для малих обсягів даних, низька затримка	Не підтримує передачу великих обсягів даних, вимагає налаштування брокера	Ідеально підходить для систем з високими вимогами до швидкості передачі та надійності
WebSocket	Безперервне з'єднання, підтримка реального часу	Не підходить для всіх серверів, потребує спеціальних налаштувань	Використовується для додатків, де важливий безперервний моніторинг даних

Насамкінець, важливим етапом є тестування і оптимізація передачі даних та роботи інтерфейсу користувача. Це дозволяє виявити та усунути потенційні помилки, знизити час затримки між змінами параметрів і їх відображенням на інтерфейсі, а також переконатися в надійності і безпеці системи в цілому.

3 ТЕСТУВАННЯ ТА ОПТИМІЗАЦІЯ СИСТЕМИ

3.1 Налаштування та тестування роботи охоронної системи в реальних умовах

Налаштування та тестування роботи охоронної системи є критично важливими етапами розробки, оскільки вони дозволяють перевірити працездатність усіх складових системи в реальних умовах експлуатації. Для цього необхідно провести кілька етапів перевірок, включаючи налаштування обладнання, перевірку точності датчиків, а також забезпечення надійної передачі даних та правильності роботи програмного забезпечення. Важливою частиною цього процесу є також тестування взаємодії між усіма компонентами системи: датчиками, мікроконтролером ESP8266, сервером та користувацьким інтерфейсом [21, с. 133].

Перед початком тестування необхідно провести налаштування всіх елементів охоронної системи, зокрема датчиків, що фіксують параметри навколишнього середовища, та налаштувати їх на роботу з мікроконтролером. Це включає в себе перевірку підключень датчиків, встановлення відповідних порогових значень, які визначатимуть, коли система повинна спрацьовувати, а також програмування мікроконтролера для обробки сигналів від датчиків і передачі даних на сервер.

Одним з основних етапів налаштування є тестування працездатності всіх датчиків у різних умовах. Наприклад, датчики руху повинні точно визначати будь-які зміни в навколишньому середовищі, а температурні та вологісні датчики повинні реагувати на зміни кліматичних умов. Для цього необхідно вивести значення, що зчитуються з датчиків, на монітор, щоб переконатися в точності їх роботи. Оскільки датчики можуть бути чутливими до різних факторів, таких як перепади температури або зовнішній шум, важливо тестувати систему в умовах, наближених до реальних, щоб оцінити, наскільки вона стійка до змін навколишнього середовища.

Тестування також включає перевірку передачі даних від датчиків через мікроконтролер ESP8266 на сервер. Мікроконтролер повинен стабільно передавати

інформацію без затримок або втрат даних. Тому важливо переконатися в тому, що з'єднання Wi-Fi на об'єкті є надійним і достатньо швидким для обміну даними між усіма компонентами системи.

Особливу увагу слід приділити налаштуванню системи оповіщень. Алгоритм оповіщення повинен бути протестований в умовах перевищення критичних значень, що визначені для кожного датчика. Для цього необхідно симулювати ситуації, при яких параметри, наприклад температура або вологість, перевищують задані порогові значення, і перевірити, чи система правильно реагує на ці зміни. Оповіщення мають надходити своєчасно, в правильному форматі, і повинні бути надійно доставлені користувачам.

Крім того, необхідно протестувати програмне забезпечення для відображення даних на веб-сервері. Веб-інтерфейс має бути здатний правильно відображати дані, що передаються з датчиків, та своєчасно оновлювати їх в реальному часі. Важливо також перевірити, чи коректно працюють сповіщення на веб-сторінці, чи правильно відображаються графіки та таблиці з даними.

Одним із важливих етапів тестування є перевірка системи в умовах навантаження. Необхідно протестувати, як система працює при великих обсягах даних або при одночасній роботі кількох користувачів, що підключаються до веб-сервера. Це дозволяє оцінити, чи справляється система з навантаженням і чи не виникають затримки в передачі або обробці даних.

Налаштування параметрів для сповіщень є важливим етапом. Для кожного датчика повинна бути можливість встановлення індивідуальних порогових значень, що дозволяє налаштовувати систему відповідно до специфіки об'єкта. Наприклад, для ливарного цеху температура може бути критичним параметром, і її перевищення повинно спрацьовувати сигналізацію. Водночас для інших об'єктів можуть бути важливими інші параметри, і система має бути налаштована на виявлення змін у цих параметрах.

Після налаштування та первинного тестування необхідно виконати низку реальних тестів в умовах, близьких до тих, у яких система буде експлуатуватися. Це може включати тестування в умовах змінної погоди, перевірку роботи вночі та

вдень, а також в умовах різних зовнішніх впливів, таких як дощ, вітер або температурні коливання. Важливо, щоб система була стабільною в будь-яких умовах і забезпечувала належний рівень безпеки.

Також необхідно перевірити стабільність роботи системи при відключеннях електроживлення або мережі Wi-Fi. Система має бути здатною відновити свою роботу після збоїв і продовжувати моніторинг без втрат даних. Для цього тесту важливо симулювати відключення живлення та перевірити, чи відновлюється система автоматично.

Не менш важливим є тестування функціонування системи при використанні різних пристроїв для доступу до веб-інтерфейсу. Користувачі можуть використовувати як комп'ютери, так і мобільні пристрої, тому інтерфейс має бути адаптований до різних розмірів екранів і пристроїв. Тестування вимагає перевірки зручності навігації та відображення даних на різних типах пристроїв.

Паралельно з тестуванням на реальному обладнанні важливо проводити моніторинг продуктивності системи, щоб визначити, чи є затримки в передачі даних або обробці запитів. Для цього необхідно здійснювати вимірювання часу від моменту передачі даних від датчиків до моменту їх відображення на веб-інтерфейсі.

У процесі тестування також необхідно перевірити роботу з великими обсягами даних, особливо коли система повинна працювати протягом тривалого часу. Це дозволяє визначити, чи не виникають проблеми з пам'яттю мікроконтролера або серверного обладнання при накопиченні великих обсягів інформації. Ще однією важливою задачею є тестування енергоспоживання системи, оскільки багато датчиків і мікроконтролер працюють на батареях. Необхідно оцінити, скільки часу система може працювати без підзарядки і чи не потребує вона частого обслуговування.

Тестування інтерфейсу користувача включає також перевірку сповіщень, що надсилаються на мобільні пристрої чи електронну пошту. Сповіщення мають надходити своєчасно та правильно відображати інформацію про критичні ситуації.

Особливу увагу треба приділити перевірці функціонування системи в умовах різних температурних коливань. Оскільки система може бути встановлена в різних кліматичних умовах, важливо тестувати її на стійкість до різких змін температури і впливу вологи.

Важливим етапом є тестування на надійність і довговічність, яке дозволяє оцінити, наскільки стабільно система працює протягом тривалого часу в умовах експлуатації. Це включає перевірку всіх складових системи на стійкість до механічних пошкоджень, впливу вологи і пилу.

Крім того, необхідно перевірити процес налаштування нових датчиків у систему. Це дозволяє переконатися, що система є гнучкою і здатною до розширення в разі потреби [22, с. 105].

Для того щоб результати тестування були більш об’єктивними, всі вимірювання і результати повинні фіксуватися в таблицях. Вони дозволяють зберігати інформацію про кожен етап тестування та оцінювати ефективність роботи системи.

Таблиця 3.1.1– Тестування роботи охоронної системи

Параметр	Значення	Оцінка працездатності	Коментар
Час передачі даних	1,2 секунди	Відмінно	Швидка передача даних
Стабільність сигналу	100% без втрат	Відмінно	Надійний сигнал
Точність датчиків	±0,5°C (температура)	Хорошо	Відхилення в межах норми
Відповідність порогів	0,3% від заданих значень	Добре	Пороги налаштовані точно
Надійність роботи при відключенні	Відновлення за 10 секунд	Добре	Система відновлює роботу

Продовження тестування охоронної системи включає в себе додаткові перевірки, пов’язані з реальними умовами роботи в постійно змінюваному

середовищі. Одним з ключових аспектів є перевірка на стійкість до зовнішніх перешкод, таких як електромагнітні завади, які можуть впливати на стабільність роботи датчиків та мікроконтролера. Це особливо важливо, якщо система встановлена в індустріальних зонах, де можуть бути джерела електромагнітних випромінювань, що знижують ефективність зв'язку. Для цього здійснюються тести, при яких мікроконтролер і датчики розташовуються поруч з джерелами таких перешкод, щоб перевірити, чи зберігається надійність передачі даних.

Додатково важливо перевірити ефективність системи при роботі в умовах зниженого рівня сигналу Wi-Fi. У реальних умовах покриття бездротових мереж часто буває непостійним, і система може втратити зв'язок із сервером. Тестування у таких умовах допомагає оцінити, чи система може адаптуватися до зміни якості з'єднання, забезпечуючи передачу даних навіть при слабкому сигналі. У разі втрати сигналу система має бути налаштована таким чином, щоб зберігати дані до моменту відновлення з'єднання, а також повторно передавати їх після відновлення зв'язку.

Іншим важливим етапом є перевірка адаптивності системи до змін в інтерфейсі користувача. Веб-інтерфейс системи повинен забезпечувати коректне відображення даних на різних пристроях, таких як мобільні телефони, планшети та десктопи. Для цього проводяться додаткові тестування на різних типах пристроїв і браузерах, щоб впевнитися в універсальності та зручності використання інтерфейсу. Потрібно перевірити, чи коректно оновлюється інформація на всіх екранах при будь-яких змінах на сервері, і чи не виникають помилки при відображенні графіків та таблиць на екранах різних розмірів.

Особливу увагу варто приділити тестуванню функціональності системи при зміні параметрів охорони або налаштувань датчиків. Система повинна дозволяти легко додавати нові датчики або змінювати порогові значення існуючих без порушення роботи вже підключених компонентів. Також важливо перевірити механізм оновлення програмного забезпечення, оскільки в процесі експлуатації можуть з'являтися нові версії прошивок або програм, які повинні бути безперешкодно інтегровані в систему.

Тестування також включає в себе перевірку на масштабованість системи. Наприклад, чи буде система стабільно працювати в разі підключення великої кількості додаткових датчиків або розширення її функціональності. Для цього створюються умови, при яких кількість датчиків та параметрів для моніторингу збільшується, що дозволяє оцінити, чи не виникають проблеми з продуктивністю або зберіганням даних.

Паралельно з тестуванням апаратної частини важливо також провести перевірку на стабільність програмного забезпечення сервера. Сервер має бути здатний обробляти численні запити одночасно, а також виконувати резервне копіювання даних без затримок. Крім того, важливо, щоб сервер не зазнавав збоїв при великому навантаженні, яке виникає, наприклад, при великій кількості користувачів, що одночасно отримують доступ до веб-інтерфейсу.

Крім тестування на навантаження, необхідно оцінити час відгуку на запити користувачів. Веб-інтерфейс повинен працювати швидко, з мінімальними затримками при відображенні інформації, адже у випадку з охоронною системою кожна затримка може негативно вплинути на оперативність реагування. Для цього проводяться тестування часів відгуку сервера при різних типах запитів, таких як отримання даних про стан датчиків або зміна налаштувань.

Важливим аспектом є також перевірка механізмів зберігання та обробки даних. Дані з датчиків повинні бути збережені на сервері з можливістю доступу до історії подій. Необхідно перевірити, чи система зберігає інформацію без втрат, а також чи можна за допомогою інтерфейсу здійснювати пошук і фільтрацію цих даних.

Наприкінці тестування варто оцінити ефективність навчання користувачів і операторів системи. Навіть найсучасніша охоронна система потребує належної підготовки користувачів для правильної експлуатації. Проводяться тренінги для персоналу, що користується системою, і перевіряється, чи зможуть вони оперативно реагувати на події та налаштовувати систему в разі необхідності. Тестування також передбачає оцінку ефективності системи з точки зору її енергоспоживання. Оскільки система може функціонувати в автономному режимі,

важливо перевірити час роботи на батареях і можливість оптимізації споживаної енергії. Для цього проводяться заміри енергоспоживання в різних режимах роботи, наприклад, при постійному моніторингу або в періодах низької активності.

Продовження тестування охоронної системи також включає в себе дослідження поведінки системи в умовах довгострокової експлуатації. Одним з важливих аспектів є перевірка на стійкість до деградації компонентів при тривалому використанні. Це може включати тестування датчиків на точність після декількох місяців роботи або перевірку на знос електронних компонентів мікроконтролера. Важливо, щоб система зберігала свою працездатність навіть через тривалий період експлуатації.

Один з можливих експериментів полягає у тестуванні системи при використанні її в умовах різних сезонних змін, таких як зміна температури чи вологості, що може впливати на чутливість датчиків. Для цього можна налаштувати систему в умовах змінної температури – наприклад, поміщення датчиків у холодильну камеру для вимірювання температури в умовах низьких температур та порівняння їх показів з аналогічними датчиками, що працюють при нормальних температурних умовах. Таке тестування дозволить оцінити, наскільки стабільно система працює в умовах, коли температура змінюється від дуже низьких до високих значень, що є особливо важливим для використання охоронної системи в різних кліматичних зонах.

Також необхідно провести дослідження ефективності роботи системи при змінному живленні. Для цього можна виконати експеримент, в якому система буде функціонувати під час перебоїв з електроживленням. У разі використання батарей або альтернативних джерел енергії важливо перевірити, як система поводиться при низькому рівні заряду.

Наприклад, симулювати ситуацію, при якій живлення системи змінюється з основного джерела на резервне, і оцінити, чи відновлюється система без втрат даних або погіршення її продуктивності. Під час таких тестів також важливо перевірити, чи є на сервері інформація про стан живлення та про будь-які зміни в живленні системи.

Особливо важливим є тестування на стійкість до механічних пошкоджень, оскільки охоронні системи часто встановлюються в умовах, де є ризик фізичних пошкоджень, наприклад, у промислових зонах або на будівельних майданчиках. Для цього можна провести експеримент з механічними впливами на датчики, мікроконтролери та інші елементи системи, наприклад, впливати на них ударами чи вібраціями, щоб оцінити, чи зберігається працездатність системи після таких впливів [23, с. 11].

Нарешті, важливим аспектом тестування є перевірка здатності системи до швидкої реакції на змінні ситуації, що потребують миттєвого втручання. Для цього можна провести тестування на базі сценаріїв реальних надзвичайних ситуацій, таких як спроби проникнення на об'єкт. Симулювати умовне проникнення можна шляхом активізації датчиків руху чи температури в умовах, наближених до реальних, щоб перевірити швидкість оповіщення користувача через веб-сервер або мобільний додаток.

Забезпечення безперервності роботи охоронної системи на різних етапах тестування дозволяє оцінити її надійність у реальних умовах. Результати таких тестів можна використовувати для подальшої оптимізації системи, покращення її елементів або програмного забезпечення, що дозволяє знизити ймовірність несправностей та підвищити ефективність системи в процесі її експлуатації.

Загалом, тестування системи в реальних умовах є багатофакторним процесом, що вимагає не тільки перевірки технічних характеристик, але й оцінки її стабільності, ефективності роботи та зручності користування. Тільки після повного тестування можна буде бути впевненим у надійності та безпеці охоронної системи.

3.2 Аналіз можливих проблем та оптимізація продуктивності

Після проведення тестування системи охоронної сигналізації та збору даних про її роботу, настає етап аналізу можливих проблем, що можуть виникати під час експлуатації, а також оптимізації продуктивності всієї системи. Виявлення і вирішення таких проблем є важливою частиною процесу удосконалення системи,

що дозволяє підвищити її надійність, ефективність та зручність використання. Однією з основних проблем, яку необхідно врахувати, є можливі затримки в передачі даних, що можуть виникати через нестабільність Wi-Fi-з'єднання або перевантаження мережі.

Однією з основних причин таких затримок є нестабільність бездротового зв'язку, що може бути спричинена низькою якістю сигналу в певних зонах. Оскільки система використовує мікроконтролер ESP8266 для передавання даних на сервер, важливо забезпечити стабільне підключення до мережі Wi-Fi. Для оптимізації цього процесу можна застосувати методи автоматичного повторного підключення до мережі у разі її втрати, а також використовувати систему кешування даних на мікроконтролері. Це дозволяє зберігати дані в локальній пам'яті до відновлення з'єднання, після чого інформація передається на сервер.

Іншою важливою проблемою є надмірне навантаження на сервер при обробці великої кількості запитів або великого обсягу даних. Якщо на сервер надходить занадто багато запитів одночасно, це може призвести до зниження його продуктивності і затримок у відображенні даних в інтерфейсі користувача. Для вирішення цієї проблеми можна застосувати методи оптимізації серверного коду, зокрема, розподіл обробки запитів на кілька потоків або серверів, а також кешування результатів запитів, що дозволить зменшити навантаження на сервер та знизити час обробки запитів.

Крім того, важливо забезпечити ефективне зберігання даних. Зберігання великої кількості даних, що надходять від датчиків, може вимагати значних ресурсів, особливо в умовах довгострокової експлуатації системи. Тому необхідно застосувати методи оптимізації зберігання даних, наприклад, архівування старих даних, що більше не потрібні для поточного моніторингу, або використання баз даних, оптимізованих для великих обсягів даних, таких як NoSQL.

Ще однією проблемою є обмежені ресурси мікроконтролера, зокрема, пам'ять і обчислювальна потужність. Оскільки ESP8266 має обмежені можливості в порівнянні з потужнішими комп'ютерами чи серверами, потрібно оптимізувати програмний код, щоб зменшити навантаження на мікроконтролер. Для цього

можна використовувати легкі алгоритми обробки даних, мінімізувати кількість обчислень і забезпечити ефективне використання пам’яті, обмежуючи збереження лише найнеобхідніших даних.

Один з важливих аспектів оптимізації продуктивності – це зменшення енергоспоживання системи, особливо в умовах автономної роботи датчиків. Мікроконтролери та датчики, які працюють від батарей, повинні бути енергоефективними. Для досягнення цієї мети можна реалізувати режим глибокого сну для ESP8266, коли мікроконтролер не активно обробляє дані або не передає їх, а також оптимізувати частоту зчитування даних з датчиків, знижуючи їх частоту в періоди, коли немає потреби в частих вимірюваннях.

Іншою проблемою може бути неправильне реагування системи на критичні значення параметрів датчиків. Залежно від умов, датчики можуть подавати неточні покази, що призводить до помилкових спрацьовувань сигналізації. Це може виникнути через вібрації, електромагнітні перешкоди чи інші зовнішні фактори. Для покращення точності роботи системи потрібно застосувати алгоритми фільтрації даних, які допоможуть зменшити вплив шуму та інших перешкод на покази датчиків. Щоб покращити взаємодію користувача з системою, можна також оптимізувати веб-інтерфейс. Важливо, щоб інтерфейс був не тільки функціональним, але й зручним, без зайвих затримок у відображенні даних. Одна з можливих проблем – це низька швидкість завантаження сторінок, що може виникати при великій кількості запитів до сервера. Для цього можна застосувати техніки оптимізації, такі як попереднє завантаження даних або кешування результатів запитів на стороні клієнта.

У разі великого обсягу даних, що зберігаються на сервері, важливо забезпечити ефективний пошук і доступ до цих даних. Це можна досягти шляхом впровадження індексації та розбиття даних на менші блоки, що дозволить скоротити час на їх обробку та запит до бази даних. Іншою стратегією є використання компресії даних, що дозволить знизити вимоги до місця на сервері та зменшити час, необхідний для їх передачі.

Не менш важливою є проблема безпеки передавання даних між мікроконтролером і сервером. Оскільки система може обробляти чутливі дані, необхідно реалізувати захищений канал зв'язку для запобігання несанкціонованому доступу. Використання протоколів шифрування, таких як TLS/SSL, дозволить забезпечити захист переданих даних від перехоплення і змін. Додатково варто звернути увагу на питання масштабування системи. Якщо система передбачає можливість підключення додаткових датчиків або інших пристроїв, то вона повинна бути гнучкою і підтримувати таку можливість без втрат продуктивності. У цьому випадку доцільно використовувати модульну архітектуру програмного забезпечення та апаратних компонентів, що дозволяє безперешкодно додавати нові елементи системи [24, с. 169].

Однією з можливих проблем може бути обмежена здатність системи до самодіагностики. Якщо система несправна або є проблеми з її компонентами, це може призвести до втрати даних або некоректної роботи сигналізації. Для вирішення цієї проблеми можна додати механізм самоперевірки, який буде регулярно аналізувати стан системи та виводити відповідні попередження про наявність несправностей або неполадок.

Покращення продуктивності системи охоронної сигналізації є багатогранним процесом, що включає як апаратні, так і програмні оптимізації. Від правильного налаштування компонентів, ефективного використання ресурсів і надійного зберігання даних залежить стабільність і ефективність роботи всієї системи. Тому необхідно постійно проводити моніторинг її роботи, визначати потенційні проблеми і оперативно їх усувати.

3.3 Перспективи вдосконалення системи та можливості масштабування

Перспективи вдосконалення системи охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер є важливим напрямом розвитку, оскільки технології постійно еволюціонують, і для забезпечення максимальної ефективності системи необхідно адаптувати її до нових умов і потреб користувачів.

Одним із можливих напрямків розвитку є інтеграція нових датчиків і сенсорів, що дозволить розширити можливості моніторингу і забезпечити більшу точність виявлення небезпечних ситуацій. Це можуть бути, наприклад, датчики температури, вологості, або навіть сенсори для моніторингу повітряного простору, що дозволить вчасно виявляти ризики для здоров'я або пожежі.

Також перспективою вдосконалення є інтеграція з іншими системами безпеки, такими як відеоспостереження або доступ до будівель. Це дозволить створити єдину комплексну систему охорони, що автоматично реагує на події, пов'язані з проникненням або іншими загрозами. Поєднання різних типів сенсорів і камер відеоспостереження дозволить оперативно здійснювати аналіз ситуації і коригувати рівень безпеки в реальному часі.

Ще одним важливим аспектом вдосконалення є покращення користувацького інтерфейсу. Веб-інтерфейс є основним засобом взаємодії з системою, тому важливо забезпечити його зручність і функціональність. Розширення можливостей інтерфейсу для мобільних пристроїв дозволить користувачам відслідковувати дані системи з будь-якої точки світу через смартфони або планшети. Це дозволить значно підвищити доступність та зручність використання системи [25, с. 35].

Масштабування системи також є ключовим аспектом її вдосконалення. Однією з можливостей для масштабування є підключення великої кількості датчиків до мережі. Система повинна бути спроектована таким чином, щоб легко інтегрувати нові датчики без значних змін у загальній архітектурі. Для цього важливо використовувати модульну структуру, яка дозволить безперешкодно додавати нові елементи і розширювати функціональність системи.

Також можливим напрямком масштабування є розширення кількості підключених об'єктів. У разі потреби можна збільшити кількість точок контролю на об'єкті, підключити нові зони охорони або навіть створювати декілька незалежних підсистем для різних частин об'єкта. Це дозволить організувати гнучке управління і налаштування системи в залежності від вимог замовника.

Для покращення масштабованості та ефективності системи можна застосувати технології хмарних обчислень, що дозволяють зберігати дані на

віддалених серверах і забезпечувати доступ до них через інтернет. Хмарні технології також дозволяють реалізувати резервне копіювання даних та автоматичне оновлення програмного забезпечення, що забезпечить високу надійність і безперебійність роботи системи. Перспективи вдосконалення системи також включають використання більш потужних мікроконтролерів з більшими обчислювальними ресурсами та більшою кількістю входів/виходів. Наприклад, використання новітніх моделей мікроконтролерів може забезпечити швидшу обробку даних, покращити швидкість реагування на сигнали та дозволити підключати більше датчиків одночасно, що є важливим при масштабуванні системи.

Інтеграція з іншими протоколами зв'язку, такими як LoRa або NB-IoT, також відкриває нові можливості для розширення системи. Ці технології дозволяють здійснювати бездротову передачу даних на великі відстані з мінімальними енергетичними витратами, що важливо для віддалених об'єктів, де немає можливості підключити систему до традиційної мережі Wi-Fi.

Для підвищення ефективності системи можна також вбудовувати додаткові алгоритми машинного навчання або штучного інтелекту, що дозволить автоматично аналізувати великі обсяги даних і виявляти аномалії або потенційні загрози. Використання таких алгоритмів дозволить системі працювати більш автономно, зменшуючи необхідність у ручному втручанні та підвищуючи її ефективність.

Покращення продуктивності також може бути досягнуте за допомогою вдосконалення алгоритмів обробки сигналів, таких як фільтрація шуму та усунення помилок в вимірюваннях. Це дозволить підвищити точність даних, що надходять від датчиків, і забезпечить більш надійну роботу всієї системи.

Перспективи вдосконалення системи можуть включати й автоматизацію процесу обслуговування та налаштування системи. Це може бути реалізовано через додавання функцій для віддаленого діагностування та оновлення програмного забезпечення, що дозволить зменшити час, витрачений на технічне обслуговування, і покращити загальну ефективність системи.

Також важливою складовою розвитку є адаптація системи до нових стандартів безпеки. Постійний розвиток технологій безпеки вимагає від системи здатності реагувати на нові загрози, такі як кібер-атаки. Для цього необхідно регулярно оновлювати систему шифрування та використовувати сучасні методи аутентифікації користувачів для запобігання несанкціонованому доступу.

Масштабування системи також передбачає можливість її використання в різних сферах, наприклад, для захисту великих підприємств, промислових об'єктів, а також житлових комплексів. Це дозволяє створити універсальну систему охорони, яка може бути адаптована під будь-які потреби користувачів, незалежно від розміру об'єкта [26, с. 42].

Іншою важливою складовою вдосконалення є зниження витрат на експлуатацію системи. Для цього можна використовувати більш енергоефективні мікроконтролери, а також оптимізувати програмне забезпечення таким чином, щоб зменшити вимоги до ресурсів і знизити енергоспоживання при збереженні високої продуктивності. У майбутньому можна розглянути можливість впровадження додаткових функцій, таких як інтеграція з системами розпізнавання осіб або автентифікації за допомогою біометричних даних. Це дозволить значно підвищити рівень безпеки, забезпечуючи доступ тільки авторизованим користувачам.

Нарешті, важливо враховувати екологічні аспекти вдосконалення системи. Використання екологічно чистих технологій, таких як сонячні панелі для живлення мікроконтролерів або датчиків, може значно знизити вплив на навколишнє середовище і зробити систему більш стійкою в умовах відсутності традиційних джерел енергії.

ВИСНОВКИ

Автоматизовані системи охоронної сигналізації на базі мікроконтролера ESP8266 демонструють високу ефективність, гнучкість і економічність у порівнянні з традиційними охоронними рішеннями. Застосування Wi-Fi технології дозволяє зменшити витрати на прокладання комунікацій, а також забезпечити швидке та масштабоване розгортання системи на різних об’єктах. Це особливо актуально в умовах обмежених ресурсів або необхідності оперативної установки.

Мікроконтролер ESP8266 має широкі можливості інтеграції з сенсорними пристроями, підтримку протоколів передачі даних, що робить його ідеальним для реалізації рішень IoT, зокрема – у сфері безпеки. Розроблене програмне забезпечення дозволяє в реальному часі зчитувати інформацію з датчиків, обробляти її та оперативно передавати на веб-сервер, що відкриває доступ до даних з будь-якої точки світу. Це значно підвищує ефективність прийняття рішень та своєчасність реагування на потенційні загрози.

Важливим компонентом системи є інтерфейс користувача – інтуїтивно зрозумілий, адаптивний до різних пристроїв і платформ. Він дозволяє оперативно відслідковувати зміни в параметрах охоронюваного об'єкта та своєчасно реагувати на події. Особливу увагу в системі приділено питанням безпеки – впровадження сучасних методів шифрування, таких як SSL/TLS, гарантує захист переданої інформації від несанкціонованого доступу.

Загалом, результати дослідження підтверджують доцільність використання ESP8266 у проєктуванні систем охорони з передачею даних на веб-сервер. Це не лише дозволяє створити надійну систему з високим рівнем безпеки, а й забезпечує її адаптивність, масштабованість і відповідність сучасним технологічним вимогам. Упровадження таких рішень відкриває широкі перспективи для розвитку інтелектуальних систем охорони в різних галузях, включно з побутовим, промисловим та військовим застосуванням.

Крім того, система охоронної сигналізації з використанням ESP8266 відзначається високою енергоефективністю, що дозволяє зменшити витрати на

живлення пристроїв, особливо в умовах автономної роботи. Завдяки широкій спільноті розробників та наявності великої кількості бібліотек для ESP8266, процес розробки та налагодження програмного забезпечення значно спрощується. Важливо також, що дана система є легко модернізованою – її можна доповнювати новими сенсорами, модулями зв’язку або функціональними можливостями без потреби повної заміни обладнання. Такий підхід відповідає сучасним тенденціям сталого розвитку та повторного використання електронних компонентів. У майбутньому ця система може бути інтегрована до більш складних екосистем розумного будинку або індустріального IoT середовища, що значно розширить сферу її застосування та підвищить ефективність управління об'єктами.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Курков М. Д. Інтеграція мікроконтролерного Wi-Fi модуля ESP8266 до системи автоматизації на базі DSC LabView за протоколом Modbus TCP/IP. 2021. URL: https://krs.chmnu.edu.ua/jspui/bitstream/123456789/ 1859/1/%d0%90 %d0%b2%d1%82%d0%be%d1%80%d0%b5%d1%84%d0%b5%d1%80%d0%b0%d1%82%20%d0%9a%d1%83%d1%80%d0%ba%d0%be%d0%b2%20471%20%d0%b3%d1%80..pdf (дата звернення: 16.04.2025).

2. Черноус Я. В. Мікроконтролерний пристрій охоронної сигналізації для Smart House. 2024. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/96446/1/Chernous_bachelors_thesis.pdf (дата звернення: 16.04.2025).

3. Артюхов, В. Г. Локальне позиціонування по Wi-Fi з використанням мікроконтролерів. Таврійський науковий вісник. Серія: Технічні науки. 2022. URL: https://journals.ksauniv.ks.ua/index.php/tech/article/view/213/198 (дата звернення: 16.04.2025).

4. Кучменко В. Г. IoT системи на основі мікроконтролерів ESP: концепція мережі та програмне забезпечення: кваліфікаційна робота магістра. – 2021. –. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/85050/1/Kuchmenko_mag_rob.pdf (дата звернення: 16.04.2025).

5. Ареф’єв М. О. Моделювання системи IoT пристроїв на платформі одноплатного комп'ютера 2024. URL: https://ela.kpi.ua/server/api/core/bitstreams/c65b8d24-2e3a-4c38-8099-fb6dd337aede/content (дата звернення: 16.04.2025).

6. Єрмоленко В. Р. Система тихого розумного будинку. 2021. URL: https://ela.kpi.ua/server/api/core/bitstreams/238d39d3-1c56-4a5b-997e-ea5ed40e1fba/content (дата звернення: 16.04.2025).

7. Кубасов А. С. Дослідження та розробка автоматизованої охоронної та протипожежної системи. 2023. URL: https://dspace.znu.edu.ua/jspui/bitstream/12345/17407/1/Kubasov_A_S.pdf (дата звернення: 16.04.2025).

8. Макаренко Д. В. Моделювання системи IoT пристроїв на базі мікроконтролера ATMEGA328. 2024. URL: https://ela.kpi.ua/server/api/core/bitstreams/d314f90d-1295-4aa9-8111-a63f03850fb4/content (дата звернення: 16.04.2025).

9. Зеленський, К. К. Система керування внутрішнім середовищем розумного будинку на базі мікроконтролерів : кваліфікаційна робота магістра. – 2024. – URL: https://elartu.tntu.edu.ua/bitstream/lib/44850/1/2024_KRM_SNnm-61_Zelenskiy%20K.K.pdf (дата звернення: 16.04.2025).

10. Підгородецький М. В. Система розумний карниз : кваліфікаційна робота бакалавра, Тернопільський національний технічний університет імені Івана Пулюя. 2021. URL: https://elartu.tntu.edu.ua/bitstream/lib/35587/2/%d0%9f%d1%96%d0%b4%d0%b3%d0%be%d1%80%d0%be%d0%b4%d0%b5%d1%86%d1%8c%d0%ba%d0%b8%d0%b9.pdf (дата звернення: 16.04.2025).

11. Гаврада Д. М. Комп'ютеризована система збору та логування показників сенсорів для пожежної сигналізації : бакалавр. робота, Тернопільський національний технічний університет імені Івана Пулюя. 2024. URL: https://elartu.tntu.edu.ua/bitstream/lib/45995/2/Dmytro_Havrada.pdf (дата звернення: 16.04.2025).

12. Томенко В. І. Лабораторний практикум із дисципліни «Системи протипожежного захисту». 2024. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/24801/1/Лабпрактикум%20СПЗ_2024.pdf (дата звернення: 16.04.2025).

13. Шишкр А. Т., Кулешов Д. С. IoT-рішення для автоматизації виробничого приміщення на базі ESP8266 та Веб-сервера. 2023. URL: https://openarchive.nure.ua/server/api/core/bitstreams/c5d95ea7-80d3-4772-8b36-7204eb09119b/content (дата звернення: 16.04.2025).

14. Лиска Д. М. Система керування тепличним господарством на базі мікроконтролерів : кваліфікаційна робота магістра. 2023. URL: https://eir.zp.edu.ua/server/api/core/bitstreams/02f92321-6963-47c6-aa02-27d52129b16e/content (дата звернення: 16.04.2025).

15. Лобода В. С. Реалізація мікроконтролерних систем моніторингу та керування на базі web серверів : магіст. робота. 2020. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/80089/1/Loboda.pdf (дата звернення: 16.04.2025).

16. Квасніков В. П., Квашук Д. М., Катаєва М. О. Розробка інформаційно-вимірювальної системи діагностики робочих характеристик електродвигунів. *Збірник наукових праць Одеської державної академії технічного регулювання та якості*. 2021. №1 (18). URL: https://www.odatrya.org.ua/index.php/osatrq/article/view/260/274 (дата звернення: 16.04.2025).

17. Платформі ESP32 на. Бібліотека графічного інтерфейсу користувача для мікроконтролера ESP8266. *Наука – виробництву*. 2018. С. 36. URL: https://old.kntu.kr.ua/doc/zbirnyki/teachers/2018/2.pdf#page=36 (дата звернення: 16.04.2025).

18. Зікратий В. С. «Розумний дім» на базі мікроконтролера ESP8266. 2018. С. 24. URL: http://www.konferenciaonline.org.ua/data/downloads/file_1633679936.pdf#page=24 (дата звернення: 16.04.2025).

19. Назаревич О. Б., Шикульський І. М. Управління розумним будинком на базі мікроконтролера ESP8266. *Матеріали Міжнародної науково-технічної конференції «Фундаментальні та прикладні проблеми сучасних технологій»*. 2018. С. 223–225. URL: https://elartu.tntu.edu.ua/bitstream/lib/25395/2/MNTK_2018_2018_Nazarevich_O_B-Managing_smart_home_based_223.pdf (дата звернення: 16.04.2025).

20. Колодич В. П. Пристрій регулювання параметрів приміщень на базі мікроконтролера ESP8266. 2020. URL: https://krs.chmnu.edu.ua/jspui/bitstream/123456789/1514/1/автореферат%20Колодич%20405з.pdf (дата звернення: 16.04.2025).

21. Козак Д. М., Стадник Н. Б. Дослідження стандартів фізичного рівня Wi-Fi // Матеріали XII науково-технічної конференції «Інформаційні моделі, системи та технології». 2024. С. 133–135. URL: https://elartu.tntu.edu.ua/bitstream/

lib/47273/2/IMST_2024_Kozak_D_M-Research_of_Wi_Fi_physical_133.pdf (дата звернення: 16.04.2025).

22. Гарист А. В. Аналіз захищеності Wi-Fi мереж // Вчені записки. 2021. № 2 (част. 1). С. 105–108. URL: https://tech.vernadskyjournals.in.ua/journals/2021/2_2021/part_1/2-1_2021.pdf#page=105 (дата звернення: 16.04.2025).

23. Бабій Д. С. Портативний Wi-Fi роутер. 2023. URL: https://ela.kpi.ua/server/api/core/bitstreams/5a810eb6-7cdd-45c7-afcd-211eec7da750/content (дата звернення: 16.04.2025).

24. Фодченко А. В. Шифрування Wi-Fi 6-мереж. 2024. URL: https://openarchive.nure.ua/server/api/core/bitstreams/091db2d1-770e-4a2f-a657-302e228b0d53/content#page=169 (дата звернення: 16.04.2025).

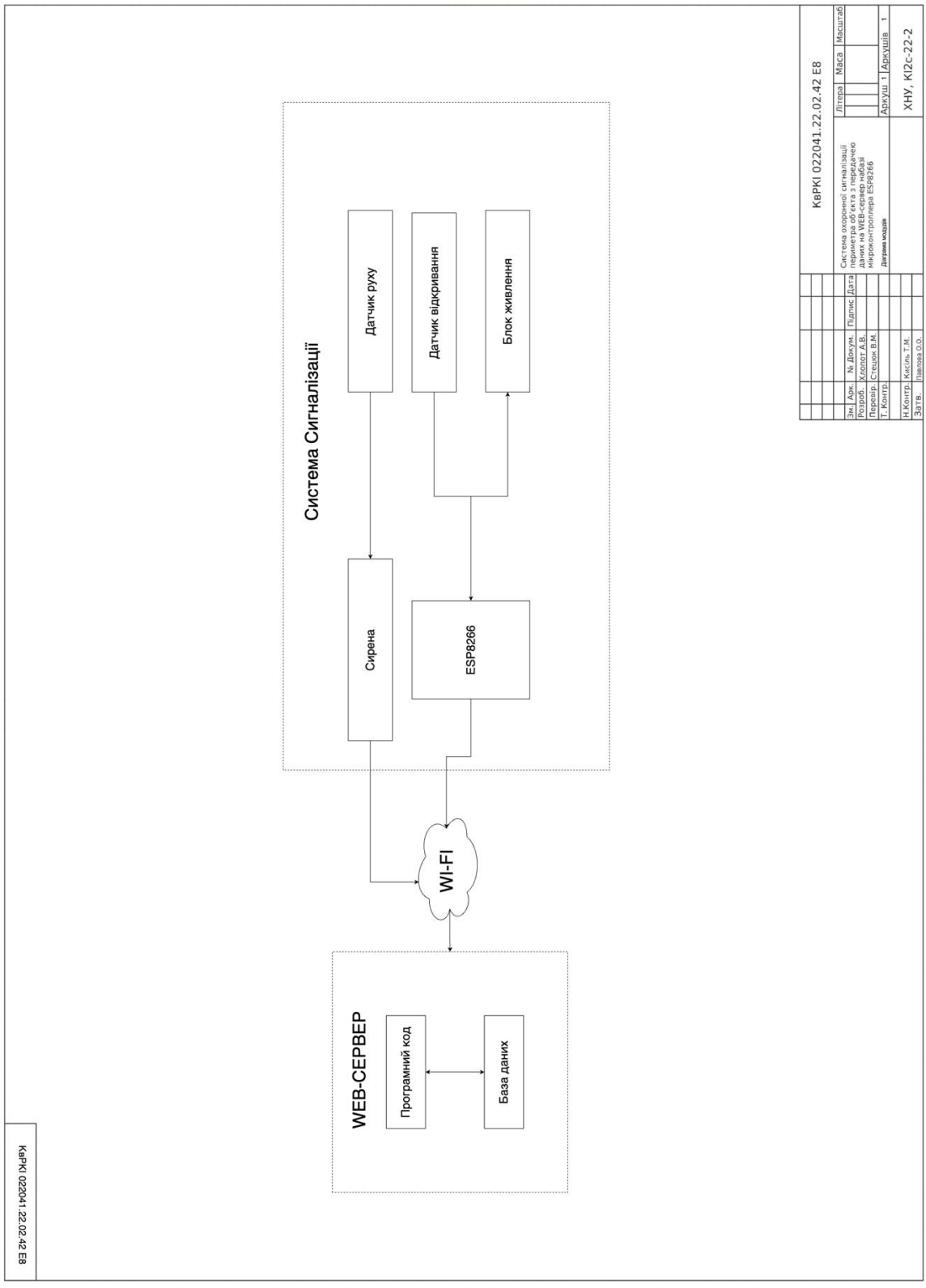
25. Крайник Я. М. Інтеграція набору взаємодіючих Wi-Fi-пристроїв у користувацьке середовище // Матеріали VI Міжнародної науково-технічної конференції «Датчики, прилади та системи–2017». 2017. С. 35. URL: https://er.chdtu.edu.ua/bitstream/ChSTU/820/1/Сборник%20тезисов%20ДПС-2017.pdf#page=35 (дата звернення: 16.04.2025).

26. Воронецький А. В. Комп'ютерна мережа підприємства на базі технології Wi-Fi. 2023. URL: https://er.nau.edu.ua/server/api/core/bitstreams/0909f35c-cb35-47f2-ad52-0a4d4a4f2c7c/content (дата звернення: 16.04.2025).

Додаток А

(обов’язковий)

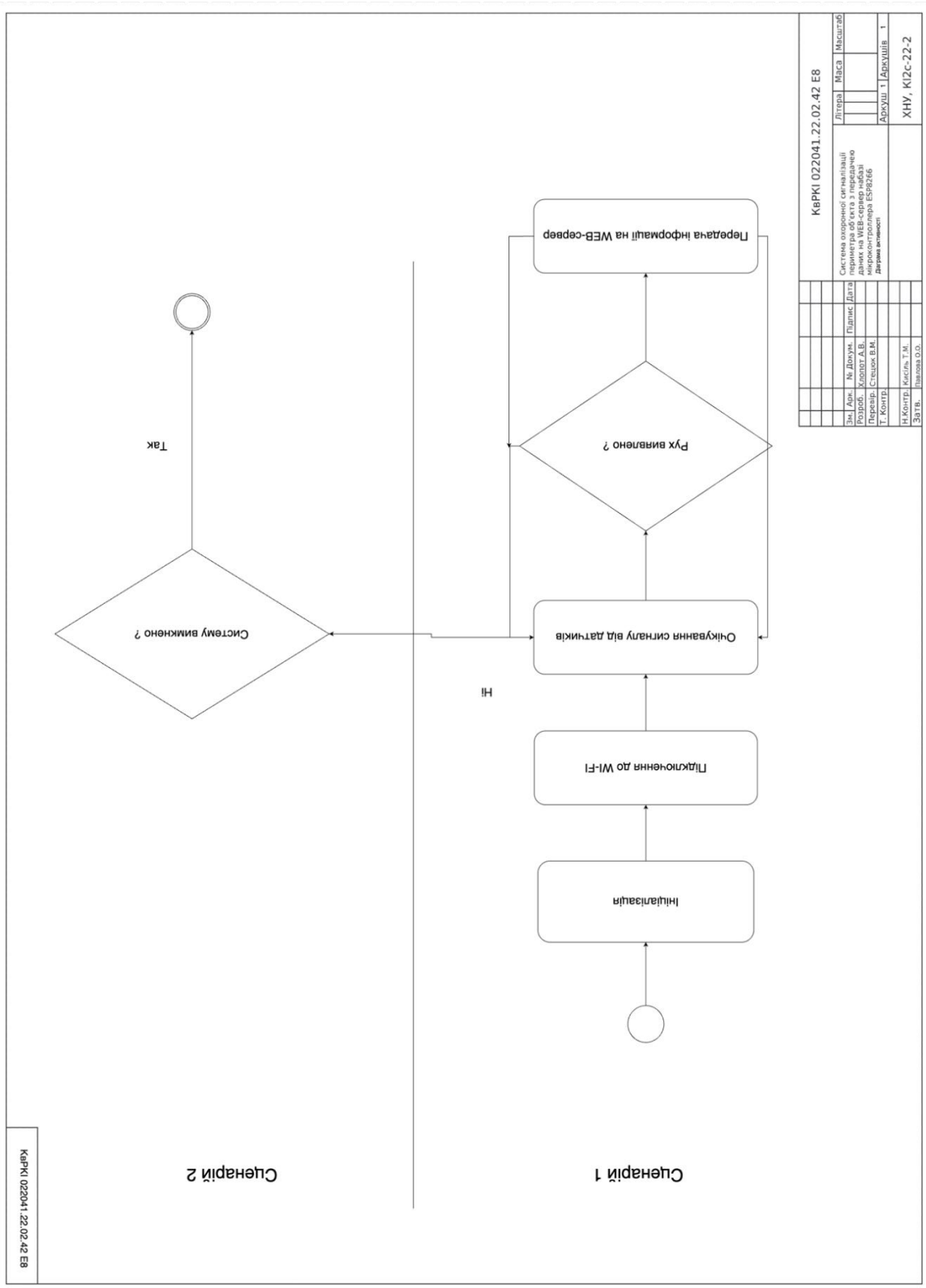
КОПІЯ КРЕСЛЕННЯ «СТРУКТУРНА СХЕМА ПЗ ПРОЄКТУ»



Додаток Б

(обов’язковий)

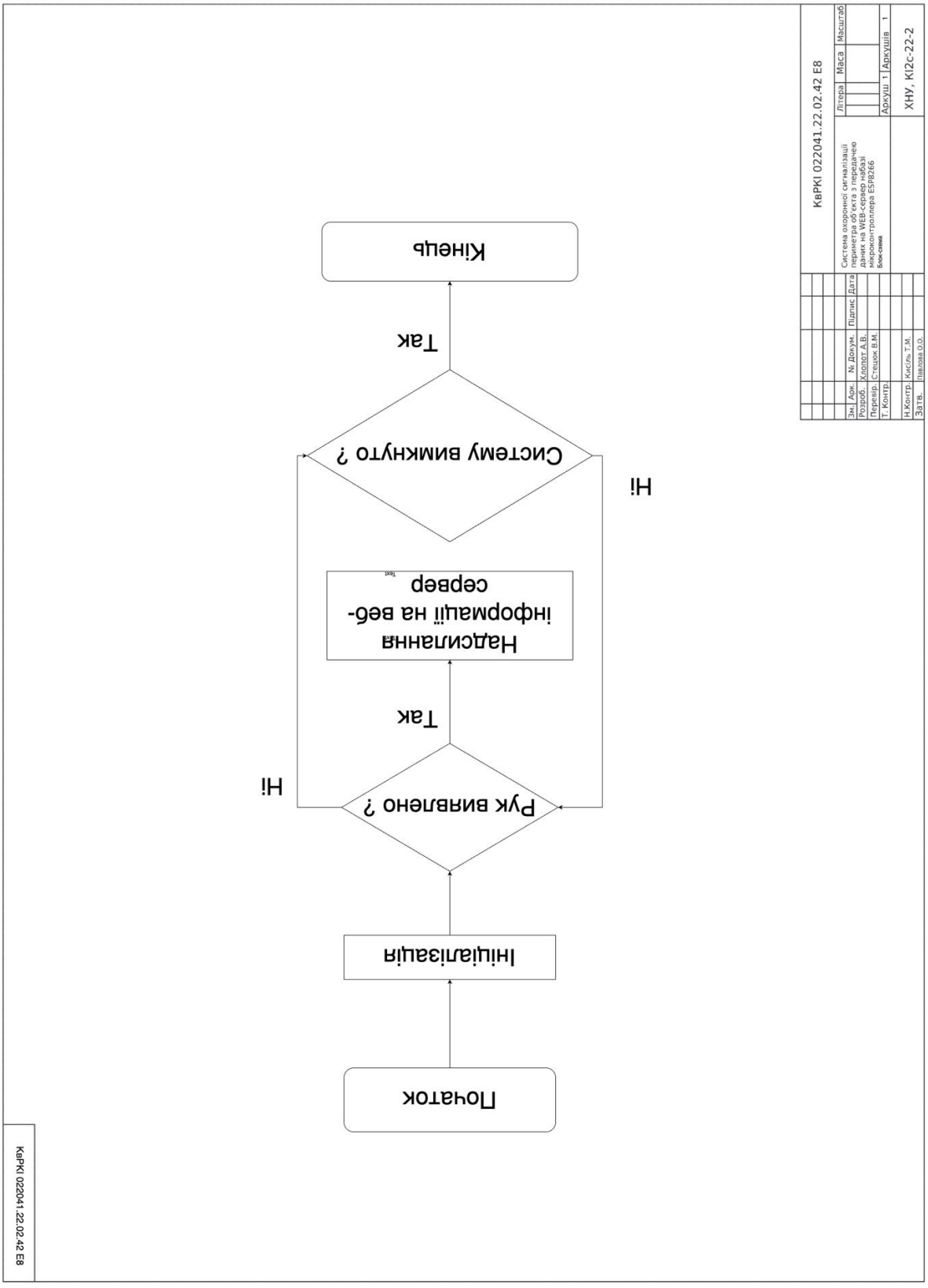
КОПІЯ КРЕСЛЕННЯ «ДІАГРАМА АКТИВНОСТІ»



Додаток В

(обов’язковий)

КОПІЯ КРЕСЛЕННЯ «БЛОК СХЕМА КРЕСЛЕННЯ»



Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Андрій ХЛОПОТ

Співавтор:

Назва: Хлопот_Система охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтроллера ESP8266

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:1.1%

Коефіцієнт подібності 2:0.3%

Мікропробіли: 6

Заміна букв: 2

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-08 07:23:52.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-06-08 Доцент Андрій Нічепорук

Дата експерт

Sun Jun 08 08:06:08 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 26.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 7%**

	Document		Sum coincidence on the DB	
ID: 244092 Title: БКР Система охоронної сигналізації периметра об‘єкта з передачею даних на WEB-сервер на базі мікроконтроллера ESP8266 Added in a DB: 2025-06-08 Authors: Андрій ХЛОПОТ Heads: Василь СТЕЦЮК Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	90345	609	23424 (26%)	159 (26%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes
240797	Title: Звіт з ПДП Система охоронної сигналізації периметра об‘єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266 Added in a DB: 2025-05-04 Authors: А.В. Хлопота Heads: В.М. Стецюк Consultants: Opponents:	23154 (26.0%)	158 (26.0%)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Хлопот Андрій В’ячеславович

Тема: Система охоронної сигналізації периметра об’єкта з передачею даних на WEB-сервер на базі мікроконтроллера ESP8266

Спеціальність**:** 123 «Комп’ютерна інженерія та програмування»

Обсяг кваліфікаційної роботи:

Кількість листів креслень _3__ Кількість сторінок записки ___55___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є розробка системи охоронної сигналізації периметра об’єкта з передачею даних на WEB-сервер на базі мікроконтролера ESP8266. В рамках роботи було створено ефективну систему, яка забезпечує моніторинг периметра об’єкта та відправлення даних на сервер для подальшого аналізу та збереження.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню і досягнуті всі поставлені цілі.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі кваліфікаційної роботи проведено дослідження основних принципів роботи охоронних систем, аналіз сучасних рішень у цій галузі, а також характеристика мікроконтролера ESP8266 та його можливостей для реалізації подібної системи. У другому розділі описано проектування та налаштування основних компонентів системи, включаючи

налаштування датчиків руху, камери та інших охоронних елементів. Описано механізм передачі даних на WEB-сервер через Wi-Fi. У третьому розділі реалізовано програмне забезпечення для управління системою, розроблено серверну частину та інтерфейс користувача для моніторингу стану системи.

4. Позитивні сторони роботи: Система демонструє високу надійність, ефективність та зручність у використанні. Реалізація через мікроконтролер ESP8266 дозволяє знизити вартість проекту і полегшує інтеграцію з іншими сервісами.

5. Негативні сторони роботи: Необхідно додатково врахувати питання масштабованості системи при розширенні периметра та збільшенні кількості підключених пристроїв.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена відповідно до вимог стандартів, графічні матеріали чіткі та наочні.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні, показує високі практичні результати та має значний потенціал для подальшого розвитку та вдосконалення.

8. Інші зауваження: Бажано провести тестування системи на реальному об'єкті для перевірки всіх функцій в умовах реального використання.

9. Оцінка дипломної роботи: добре

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи:_____
Онищко Оксана Григорівна,
доцент каф. ІПЗ, ХНУ

"__"_____2025 р. _____(підпис)

Завідувачу кафедри КІС
д-р. філософії, доц. Ользі ПАВЛОВІЙ

Андрія ХЛОПОТА
ПІБ здобувача вищої освіти

ФІТ, 3 курсу, групи КІ2с-22-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, 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 плагіат оповіщений(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 (Strike-Plagiarism 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.

5.06 2025 року Хлопот. А

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Система охоронної сигналізації периметра об'єкта з передачею даних на WEB-сервер на базі мікроконтроллера ESP8266
Автор Андрій ХЛОПОТ
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський) рівень
Спеціальність 123– Комп'ютерна інженерія
Науковий керівник: старший виклалач, Василь СТЕЦЮК

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	Відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	Не виявлено

Підтвердження:
Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:
1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.
Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 1.1% і адресується до 25 першоджерела; та системою Anti-Plagiarism складає 0.3%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Василь СТЕЦЮК
Гарант ОП _____ Андрій НІЧЕПОРУК
Завідувач кафедри КПС _____ Ольга ПАВЛОВА