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

КВАЛІФІКАЦІЙНА РОБОТА

Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»»
Назва теми

Рівень вищої освіти *другий (магістерський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 240114.24.12.15 ПЗ

Виконав здобувач II курсу, група КІ2м-24-1 — Підпис — Андрій ЖАНДРА (Ініціали, прізвище)

Керівник — канд.-техн. наук, доцент (Науковий ступінь, учене звання) — Підпис — Світлана САЧЕНКО (Ініціали, прізвище)

Нормоконтролер — д. техн. наук, професор (Науковий ступінь, учене звання) — Підпис — Сергій ЛИСЕНКО (Ініціали, прізвище)

До захисту допускаю:
завідувач кафедри КІІС — підпис — Ольга ПАВЛОВА (Ініціали, прізвище)
«_5_» _травня_ 2026 р.
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти ДРУГИЙ (МАГІСТЕРСЬКИЙ)

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
_____ Ольга ПАВЛОВА

" 12 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Жандра Андрій Ярославович
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»»
Керівник проекту (роботи) Саченко Світлана Іванівна, к.е.н., доц.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
Затверджена наказом ректора університету від 12.01.2026 р. № 6
2. Термін подання здобувачем роботи на кафедру 01.05.2026 р.
3. Вихідні дані до роботи Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз відомих методів та рішень для виявлення та запобігання аварійним ситуаціям в кіберфізичній системі "Розумний будинок"
Вибір компонентів для підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі "Розумний будинок"
Метод та алгоритм діяльності підистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі "Розумний будинок"
Підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі "Розумний будинок"
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийн

7. Дата видачі завдання «_12_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	12.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	12.01.2026	виконано
3	Робота над розділом 1 - аналіз відомих моделей, методів за темою; постановка задачі	20.01.2026	виконано
4	Робота над розділом 2 - розробка моделей для вирішення поставленої задачі	01.02.2026	виконано
5	Робота над науковою статтею	01.03.2026	виконано
6	Робота над розділом 3 - розробка методів для вирішення поставленої задачі	15.03.2026	виконано
7	Робота над розділом 4 - проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.04.2026	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2026	виконано
9	Попередній захист ДРМ	29.04.2026	виконано
10	Захист ДРМ на засіданні ЕК	До 15.05.2026	

Здобувач _____ Андрій Жандра
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Світлана Саченко
Підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Тема кваліфікаційної роботи: Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Автор роботи: Жандра А.Я., студент групи КІ2м-24-1.

Керівник роботи: Саченко С.І., кандидат економічних наук, доцент, доцент кафедри комп'ютерної інженерії та інформаційних систем.

Пояснювальна записка: 120 с., 7 рис., 7 табл., 2 дод., 86 джерел.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: кіберфізична система «Розумний будинок», Інтернет речей (IoT) , контролер ESP32, датчик MQ-7, датчик MQ-4, датчик MQ-2, датчик DS18B20, датчик YI-S, протокол MQTT, ситуаційний аналіз, автоматичне реагування.

Об'єктом дослідження є процес виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Предметом дослідження є метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Метою кваліфікаційної роботи є автоматизація процесу виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», зокрема, автоматизація процесу виявлення витоків чадного газу, природного газу, води, виявлення диму, аномально високих температур.

Методологічний апарат роботи становлять засади системного аналізу, зокрема принципи ієрархічності та декомпозиції, у поєднанні з базовими положеннями загальної теорії систем. Розв'язання дослідницьких завдань забезпечено застосуванням математичного апарату теорії моделювання, теоретико-множинного підходу та інструментарію концептуального проєктування. Додатково залучено методи евристичного оцінювання, підходи до розробки баз знань та логічного виведення.

Наукова новизна отриманих результатів: розроблено метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», що відрізняється від існуючих аналогів прецизійним моніторингом одночасно п'яти

критичних загроз – витоків природного та чадного газів, появи диму, несанкціонованих витоків води та аномальних температурних коливань та забезпечує виконання необхідних дій в автоматичному режимі, спрямованих на попередження та запобігання аварійним ситуаціям (сповіщення користувача, перекривання подачі води/газу, сповіщення екстрених рятувальних служб тощо).

Практична значущість отриманих результатів полягає у реалізації підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок», яка забезпечує високий рівень безпеки завдяки комплексній інтеграції різнопланових сенсорів та алгоритмів обробки даних у реальному часі.

У розділі 1 кваліфікаційної роботи проведений аналіз відомих методів та рішень для виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». У розділі 2 здійснений вибір компонентів для підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». У розділі 3 кваліфікаційної роботи розроблені метод та алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». У розділі 4 спроєктовано підсистему виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

ЗМІСТ

ВСТУП

Сучасне розуміння кіберфізичних систем (КФС) значно еволюціонувало, перетворившись із вузькотехнічного терміна на фундаментальну міждисциплінарну категорію [1, 2]. Сьогодні така система розглядається як складний інтегрований простір, де обчислювальні алгоритми, цифрові сервіси та фізичні пристрої взаємодіють у безперервному циклі. КФС фактично стирає межу між віртуальним та матеріальним світами, об’єднуючи датчики, мікроконтролери та хмарні технології в єдину функціональну мережу [3]. Це яскраве втілення концепції Інтернету речей, яке знаходить застосування в усіх сферах – від промисловості та медицини до створення інтелектуального житлового простору [4].

У контексті «Розумного будинку» кіберфізична система виступає не просто як набір дистанційно керованих гаджетів, а як цілісна екосистема, спрямована на підвищення комфорту, безпеки та енергоефективності. Вона об’єднує управління усіма кероівнаими функціями та комунікаціями будинку в єдиний інтелектуальний контур [5, 6]. Головною перевагою такої структури є здатність автоматизувати рутинні побутові процеси, позбавляючи мешканців необхідності постійного ручного контролю [7]. Система самостійно збирає дані, аналізує їх та приймає рішення згідно із заданими параметрами, забезпечуючи наочність управління та суттєву економію ресурсів.

Важливою рисою КФС «Розумний будинок» є її адаптивність та здатність функціонувати в умовах високої невизначеності. На відміну від класичних систем автоматизації, вона виступає активним суб’єктом прийняття рішень, що базується на глибокому аналізі контексту та сенсорної інформації [8]. Система не лише реагує на подразники, а й розпізнає складні ситуації, вибудовуючи логіку дій без прямого втручання людини. Це стає можливим завдяки здатності до самонавчання – накопичуючи дані про звички користувачів та зовнішні впливи, «Розумний будинок» постійно вдосконалює власні алгоритми реагування, стаючи більш стійким до збоїв.

Архітектурно така система базується на багаторівневій структурі, що охоплює шлях від фізичного рівня (сенсори, актуатори, контролери) до когнітивного висновку на основі функціонування кібернетичного (алгоритмти прийняття рішень, база знань) та комунікаційного (мережі передачі даних) рівнів [9]. Сенсорний рівень відповідає за первинне сприйняття середовища (дим, газ, температура, виток води тощо), тоді як обчислювальний рівень забезпечує фільтрацію та передачу цих даних. Аналітичне ядро, використовуючи алгоритми прийняття рішень, класифікує стани та формує стратегію дій. Завершує цей цикл виконавчий рівень, де актуатори та реле перетворюють цифрові команди у фізичні дії, а когнітивно-комунікаційний модуль забезпечує зв’язок із користувачем через хмарні інтерфейси [10].

Сучасна парадигма КФС відмовляється від запрограмованої лінійної логіки на користь ситуаційної інтелектуалізації [11]. Це означає, що система сприймає дані не як окремі цифри, а як цілісні сценарії реальності [12]. Завдяки впровадженню технологій граничних обчислень (edge computing), обробка інформації відбувається безпосередньо в точках її збору, що мінімізує затримки та гарантує автономність будинку навіть за відсутності інтернету [13]. Модуль ситуаційного аналізу дозволяє виявляти аномалії в життєритмі оселі, відрізняючи стандартні побутові процеси від потенційних загроз або аварійних випадків.

Особливою складністю проектування таких систем у житловому секторі є вплив людського фактора, який позбавлений жорсткого детермінізму. Тому КФС «Розумний будинок» має відповідати вимогам систем реального часу, де швидкість реакції на критичні події вимірюється частками секунди [14]. Вона повинна бути онтологічно відкритою, дозволяючи легко інтегрувати нові пристрої та сценарії без перебудови всієї архітектури. Зрештою, така система трансформується з технічного засобу в інтелектуального агента, що поєднує інженерну точність із когнітивною гнучкістю для забезпечення безпеки життєдіяльності.

Актуальність розробки підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» зумовлена стрімкою цифровізацією побутового простору та ускладненням інженерних мереж, що

потребує автоматизованого контролю в режимі реального часу. Сучасне помешкання насичене великою кількістю енергоємних приладів, розгалуженими системами водопостачання та газозабезпечення, де найменша несправність або вихід параметрів за межі норми можуть призвести до катастрофічних наслідків, таких як пожежі, затоплення чи вибухи. У сучасному помешканні критично важливо забезпечити не просто моніторинг, а здатність системи миттєво ідентифікувати аномалії в роботі електромереж, водопостачання чи газового обладнання ще на стадії зародження проблеми, що дозволяє уникнути катастрофічних наслідків, таких як пожежі або затоплення.

Традиційні методи та засоби захисту, що базуються на автономних датчиках без централізованого інтелектуального управління, часто виявляються недостатніми, оскільки вони лише констатують факт аварії, не маючи можливості вчасно її попередити або мінімізувати збитки через превентивні дії. Впровадження кіберфізичних підходів дозволяє об’єднати фізичні процеси з обчислювальними алгоритмами, забезпечуючи не тільки моніторинг, а й глибокий аналіз даних для прогнозування потенційних загроз ще до їх фактичного виникнення, перетворюючи пасивне спостереження на активне запобігання через автоматичне перекриття клапанів чи знеструмлення небезпечних ділянок. Особливої ваги це набуває в умовах нестабільної роботи енергосистем та зростання ризиків техногенного характеру, де швидкість реакції системи вимірюється мілісекундами, що критично для збереження життя мешканців та цілісності майна.

Крім того, актуальність підсистеми підкріплюється економічним аспектом, адже вартість ліквідації наслідків аварій значно перевищує витрати на розробку та впровадження інтелектуальних засобів захисту, які здатні самостійно перекрити подачу води чи газу в разі витоку. Розвиток технологій Інтернету речей та штучного інтелекту відкриває нові можливості для створення адаптивних систем, що здатні до самонавчання на основі поведінкових патернів користувачів, що робить таку підсистему фундаментом безпеки сучасного інтелектуального житла шляхом розпізнавання найменших відхилень від норми, які людина може не помітити.

Соціальна значущість підсистеми полягає у створенні безпечного та комфортного середовища для вразливих груп населення, таких як люди похилого віку або особи з обмеженими можливостями, для яких автоматизоване запобігання аваріям є життєво необхідною функцією, перетворюючи «Розумний будинок» з просто комфортного середовища на надійний інтелектуальний щит, здатний до самостійної діагностики та оперативного реагування в екстремальних умовах.

Таким чином, створення ефективної підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» є пріоритетним завданням, що відповідає сучасним тенденціям розвитку безпечних будинків та інтелектуальних систем життєзабезпечення.

Метою кваліфікаційної роботи є автоматизація процесу виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», зокрема, автоматизація процесу виявлення витоків чадного газу, природного газу, води, виявлення диму, аномально високих температур.

Поставлена мета досягається розв’язанням таких основних *задач*:

1) аналіз відомих методів та рішень для виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

2) вибір компонентів для підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

3) розроблення методу та алгритму функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

4) розроблення архітектури підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

5) проведення експериментів із використанням розробленої підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Об’єктом дослідження є процес виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Предметом дослідження є метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Наукова новизна отриманих результатів: розроблено метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», що відрізняється від існуючих аналогів прецизійним моніторингом одночасно п'яти критичних загроз – витоків природного та чадного газів, появи диму, несанкціонованих витоків води та аномальних температурних коливань та забезпечує виконання необхідних дій в автоматичному режимі, спрямованих на попередження та запобігання аварійним ситуаціям (сповіщення користувача, перекривання подачі води/газу, сповіщення екстрених рятувальних служб тощо).

Практична значущість отриманих результатів полягає у реалізації підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок», яка забезпечує високий рівень безпеки завдяки комплексній інтеграції різнопланових сенсорів та алгоритмів обробки даних у реальному часі.

Методи дослідження. Методологічний апарат роботи становлять засади системного аналізу, зокрема принципи ієрархічності та декомпозиції, у поєднанні з базовими положеннями загальної теорії систем. Розв’язання дослідницьких завдань забезпечено застосуванням математичного апарату теорії моделювання, теоретико-множинного підходу та інструментарію концептуального проєктування. Додатково залучено методи евристичного оцінювання, підходи до розробки баз знань та логічного виведення.

За темою кваліфікаційної роботи опублікована одна стаття у фаховому науковому журналі України категорії Б (додаток А):

1) Войчур Ю.О., Медзатий Д.М., Жандра А.Я. Підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». *Вісник Хмельницького національного університету. Серія «Технічні науки»*. 2026. №1. С. _______.

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ ТА РІШЕНЬ ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АВАРІЙНИМ СИТУАЦІЯМ В КІБЕРФІЗИЧНІЙ СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

1.1 Відомі кіберфізичні системи виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

Проведемо огляд відомих методів та рішень щодо виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок».

Якщо надзвичайна ситуація трапляється вдома у літньої людини, яка проживає сама, початок надання невідкладної допомоги може бути відкладено, що призводить до ще гірших наслідків для цієї групи населення. Розумні системи екстреного виклику вдома (HECS) можуть виявляти падіння та автоматично запускати екстрений сигнал тривоги, потенційно скорочуючи час до надання невідкладної допомоги та покращуючи результати. Окрім стандартної системи HECS з базовою станцією та портативним радіопередавачем, розумна система HECS включає датчики, які можуть виявляти падіння та автоматично вмикати сигнал тривоги [15, 16].

У статті [17] описано системи, спеціально розроблені для підвищення безпеки та незалежності людей з інвалідністю та людей похилого віку, які проживають вдома. Для таких людей негайна допомога в надзвичайній ситуації має вирішальне значення. Коротко обговорюється технічний стан систем екстреного виклику, спеціально розроблених для використання людьми похилого віку, зокрема добре відома радіокнопка екстреного виклику, за допомогою якої можна вручну активувати сигнал тривоги. Однак ця система не забезпечує належної безпеки у всіх надзвичайних ситуаціях. Тому пропонуються альтернативні або додаткові системи, призначені для автоматичного ввімкнення сигналу тривоги на основі запису та оцінки так званих життєво важливих параметрів. Крім того, в середовищі «Розумного будинку» з мережевими пристроями можна використовувати додаткові параметри – так звані параметри середовища. Виявлено, що ідентифікація надзвичайної ситуації стає більш надійною зі збільшенням кількості використовуваних параметрів.

Для літніх людей, які живуть самі, технічні рішення для виявлення надзвичайних ситуацій є важливими для швидкого отримання допомоги, коли це необхідно. Автори [18] представляють новий метод виявлення надзвичайних ситуацій у приватних домогосподарствах, який виявляє надзвичайно тривалі періоди бездіяльності та може обробляти помилкову або невизначену інформацію про активність. Вводиться показник неактивності, який забезпечує ймовірнісне зважування періодів бездіяльності на основі надійності вимірювань датчиків. Аналізуючи історичні показники неактивності, можна виявити аномалії, які потенційно представляють собою надзвичайну ситуацію.

Захист житлових районів все ще здійснюється за допомогою охоронців, які контролюють стан кожного будинку. Однак охоронці можуть охороняти лише зовнішню частину будинку, не знаючи про умови всередині. Тим часом система «Розумного будинку» є однією з технологій, яка продовжує розвиватися для моніторингу умов у будинку. У роботі [19] створено систему, яка може фактично контролювати стан кожного будинку, шляхом інтеграції технології та використання трьох основних датчиків – датчиків вогню, газу та руху. Ця система має переваги з точки зору встановлення гнучкого обладнання, яке можна налаштувати відповідно до потреб. Крім того, охоронці також можуть дізнаватися про умови в кожному будинку, а також отримувати актуальні сповіщення через розроблений застосунок. Система в будинку здатна надсилати інформацію про умови в ньому під час активації, включаючи небезпечні умови для активації сигналізації. З тестування обладнання видно, що чутливість вузла датчика вогню сильно залежить від кольору вогню, величини пожежі та відстані виявлення. Крім того, вузли датчиків газу можуть забезпечити швидку реакцію, якщо їх встановити поблизу джерела витоку.

У статті [20] описується проектування та впровадження пристрою Інтернету речей на базі ESP32-S3, який інтегрує моніторинг безпеки газу в режимі реального часу з голосовим помічником на базі штучного інтелекту, що забезпечує покращений зворотний зв'язок з користувачем та розмовний контекст. Основною метою системи є поєднання голосової взаємодії в режимі "вільні руки" з великою мовною моделлю (LLM) та реальним виявленням газу MQ-2 для моніторингу безпеки навколишнього

середовища. Прототип продемонстрував надійну продуктивність в обробці голосових запитів з контекстною пам'яттю та моніторингом навколишнього середовища. Ця робота ілюструє економічно ефективний та адаптивний підхід до розробки багатофункціональних рішень шляхом поєднання ESP 32 із сучасними хмарними сервісами штучного інтелекту та комплексними механізмами зворотного зв'язку з користувачами. Одночасно система проводить моніторинг навколишнього середовища за допомогою газового датчика MQ-2. При виявленні рівня газу, що перевищує заздалегідь визначений поріг, система запускає локальне голосове сповіщення через свій динамік, активує зумер та надсилає сповіщення через Telegram та мобільну панель керування Blynk, забезпечуючи своєчасне локальне та віддалене сповіщення.

В останні роки прогрес у технологіях «Розумного будинку» підкреслив необхідність розробки систем раннього виявлення пожежі та диму для підвищення безпеки та захисту. Традиційні методи виявлення пожежі, що базуються на теплових або димових датчиках, мають обмеження щодо часу реагування та адаптивності до навколишнього середовища. Для вирішення цих проблем у статті [21] представлено модель багатомасштабного інформаційного трансформатора–DETR (MITI-DETR), яка включає багатомасштабну ідентифікацію ознак на основі трансформатора, спеціально розроблені для виявлення пожежі в розумних будинках. Ця робота пропонує надійне рішення для раннього виявлення пожежі в розумних будинках, поєднуючи високу точність з можливістю розгортання в режимі реального часу.

Проєкт, описаний у [22], мав на меті впровадити застосування інтелектуальної пожежної сигналізації Arduino в реальних життєвих ситуаціях. Проєкт розпочався з дослідження та проєктування архітектури системи перед створенням прототипу. Далі відбувалась розробка прототипу з використанням відповідних датчиків. Далі відбувалось програмування системи, де команди записуються у вигляді коду та виконуються для запуску прототипу. Було проведено чотири експерименти для перевірки ефективності прототипу пристрою, призначеного для моніторингу температури, вологості та концентрації газу в навколишньому середовищі. Система використовує різні датчики для виявлення пожеж та реагування на них у режимі

реального часу, швидко їх локалізуючи та сповіщаючи служби екстреної допомоги. Запропонований метод є економічно ефективним та пропонує ефективне рішення для запобігання пожежам у «Розумних будинках».

Дослідження [23] зосереджено на розробці мобільного застосунку для системи «Розумного будинку» на базі Інтернету речей, здатного керувати побутовою технікою та подавати сигнал тривоги у разі пожежі та витоку газу. Дослідники використовували безкоштовний інструмент для створення веб-застосунків під назвою MIT App Inventor для створення застосунку та його функцій. Також для підключення застосунку до системи «Розумного будинку» використовувалась хмарна база даних Firebase. Кінцевим продуктом дослідження став мобільний застосунок для Android-пристроїв, здатний вмикати або вимикати побутову техніку та діяти як сигнал тривоги у разі пожежі або витоку газу в будинку.

У статті [24] пропонується система «Розумного будинку» на основі нечіткої логіки, яка виявляє ймовірність пожежі та активує екстрені сповіщення та дії. Система інтегрує принципи нечіткої логіки з інтелектуальними методами сенсорного зондування та прийняття рішень, які зменшують небезпеку пожежі в режимі реального часу. Ефективність та надійність системи демонструються за допомогою експериментів та оцінки. Результати досліджень підкреслюють потенціал використання підходів на основі нечіткої логіки для підвищення безпеки житлових приміщень та зменшення кількості інцидентів, пов'язаних з пожежами.

У дослідженні [25] автори пропонують нову структуру федеративного навчання (FL) для вирішення проблеми швидкого виявлення диму під час пожежі на межі середовищ «Розумного будинку». Запропонована структура використовує три різні алгоритми FL для глобальної агрегації прогнозів машинного навчання на основі даних з різних датчиків Інтернету речей. Ця структура дозволяє здійснювати раннє прогнозування, використовуючи обчислювальні можливості на межі, тим самим покращуючи швидкість реагування та ефективність систем пожежної безпеки.

Автори [26] розробили ефективне рішення для виявлення пожежі в «Розумних будинках» за допомогою методів обробки зображень та машинного навчання. FireD витягує ознаки з фотографій та захоплених відеокадрів за допомогою згорткової

нейронної мережі (CNN) та надсилає їх до нейронної мережі, яка реалізує алгоритм кластеризації, відомий як Yolov5, щоб забезпечити можливість класифікації зображень як з пожежею та без пожежі. Після виявлення пожежі модель надсилає зображення до хмари Heroku, яка служить контейнерною хмарною платформою як послуга (PaaS) для доступу, розгортання та управління зображеннями. Про виявлення пожежі сповіщення надсилається до Telegram через Telegram-бот.

У роботі [27] представлено системну модель проєктування та впровадження системи пожежної сигналізації, інтегрованої з Інтернетом речей (IoT) для раннього виявлення пожежі та реагування. Основною метою цієї роботи є покращення заходів пожежної безпеки шляхом використання технології IoT для виявлення пожеж на ранніх стадіях, що дозволяє оперативно діяти, мінімізуючи пошкодження майна та рятуючи життя. Запропонована система включає кілька датчиків, стратегічно розміщених у середовищі розумного будинку, для постійного контролю температури, рівня диму та CO. Реалізована модель включає ряд датчиків разом з візуальним індикатором на OLED та гучним зумером для попередження мешканців про потенційну пожежну небезпеку. Крім того, система запускає автоматичну систему водяного спринклера для гасіння пожежі на попередніх стадіях. Інтеграція технології IoT дозволяє здійснювати моніторинг у режимі реального часу та дистанційний доступ до системи пожежної сигналізації. Зібрані дані з датчиків можуть бути передані на централізовану станцію моніторингу або доступні через мобільний застосунок, що полегшує дистанційний моніторинг, аналіз та контроль пожежної небезпеки. Результати дослідження демонструють потенціал системи пожежної сигналізації на базі IoT у покращенні заходів пожежної безпеки.

Аналіз сучасних методів та рішень у сфері виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» свідчить про перехід від простих автономних датчиків до комплексних інтелектуальних систем, які поєднують моніторинг фізичних параметрів із просунутою аналітикою. Особлива увага в дослідженнях приділяється створенню систем екстреного виклику, що є критично важливим для безпеки літніх людей та осіб з інвалідністю. Розробки охоплюють широкий спектр технологій – від ймовірнісного зважування сенсорних даних до

інтеграції голосових помічників на базі великих мовних моделей (LLM) та мультисенсорних вузлів для контролю витоків газу й вогню. Сучасні архітектури все частіше використовують мобільні застосунки та хмарні сервіси, такі як Telegram або Blynk, для миттєвого віддаленого сповіщення користувачів та охоронних структур про виникнення загрози. Важливим вектором розвитку є впровадження методів штучного інтелекту, зокрема нечіткої логіки, федеративного навчання та згорткових нейронних мереж (CNN) для візуального розпізнавання пожеж у реальному часі. Використання моделей типу MITI-DETR або алгоритмів Yolov5 дозволяє значно підвищити точність детектування диму та вогню, мінімізуючи хибні спрацьовування та скорочуючи час реакції порівняно з традиційними тепловими детекторами. Крім того, спостерігається тенденція до створення закритих циклів реагування, де система не лише сповіщає про небезпеку, а й самостійно активує виконавчі механізми, такі як автоматичні спринклерні системи гасіння. Таким чином, сучасні кіберфізичні рішення трансформуються у когнітивні екосистеми, що здатні до багаторівневого аналізу середовища, забезпечуючи високу стійкість житла до техногенних та побутових аварій.

Значна кількість наукових робіт зосереджена на створенні систем пожежної безпеки в концепції «Розумного дому», де для виявлення загрози використовуються IoT-рішення з датчиками температури, диму та вогню, інтегрованими в хмарні середовища [28-31]. Технологічні рішення включають використання електрохімічних сенсорів для запобігання займанням на кухні [32], оптичні методи аналізу середовища за допомогою дифракційних елементів [33] та мережеве моделювання безпеки пристроїв у Cisco Packet Tracer [34]. У контексті промислового та міського управління пропонуються системи моніторингу лісових пожеж через CC-IoT [35], методи керування енергоспоживанням у промисловості для зменшення пікових навантажень [36] та розробка архітектур для «розумних міст» (Smart City) на базі наступного покоління IoT [37].

Окремо розглядаються системи віддаленого моніторингу стану пацієнтів у реальному часі для покращення якості медичного обслуговування [38], а також

критичний аналіз ризиків конфіденційності, де технології «Розумного дому» можуть стати інструментом для здійснення домашнього насильства [39].

Чимало запропонованих рішень зосереджені на створенні інтелектуальних систем безпеки «Розумного дому», зокрема через розробку IoT-платформ з голосовим керуванням для проактивного виявлення витоків газу та миттєвого сповіщення за допомогою ШІ [40], а також впровадження мультиагентних систем і графів знань для комплексного управління газовими мережами в житлових приміщеннях [41]. Технологічна база включає використання п’єзоелектричних сенсорів та мікроконтролерів для моніторингу навколишнього середовища [42-44], доповнену системами інтелектуального керування освітленням через мобільні додатки [45]. Для підвищення точності аналізу пропонуються методи нечіткої логіки в оцінці ризиків [46] та спеціалізовані інформаційні системи для обробки даних у локальних мережах [47]. Окремі архітектурні рішення описують застосування електрохімічних датчиків для запобігання пожежам на кухні [48], нейромережеве прогнозування енергоспоживання для оптимізації навантажень у будинках [49], а також використання дифузійних оптичних елементів для покращення роботи сенсорних вузлів [42]. Глобальний підхід до автоматизації базується на поєднанні хмарних обчислень і стандартів IoT наступного покоління для створення безпечного та енергоефективного житлового простору [40].

Запропоновані рішення для забезпечення безпеки кіберфізичної системи «Розумний будинок» охоплюють широкий спектр технологій від наносенсорів до хмарних платформ, де особлива увага приділяється інтегрованим системам моніторингу витоків газу та пожежної безпеки на базі мікроконтролерів і бездротових сенсорних мереж [50-52]. Для раннього виявлення загроз пропонується використання високочутливих самовідновлюваних нанокомпозитних датчиків, здатних розпізнавати небезпечні концентрації газів у реальному часі [53], а також впровадження інтелектуальних систем керування енергоспоживанням, які запобігають перевантаженням мережі та аваріям через прогнозування попиту на основі нейронних мереж [54, 55]. Архітектурні рішення включають застосування туманних та хмарних обчислень (Fog-Cloud) для забезпечення низької затримки при

передачі критичних сповіщень про аварії [56], використання мобільних додатків для віддаленого контролю стану середовища [51, 57] та впровадження автоматизованих систем відключення приладів при виявленні відхилень від нормальних показників [52, 57]. Важливим компонентом є також використання мультиагентних підходів для інтелектуального аналізу даних з різних вузлів системи, що дозволяє мінімізувати хибні спрацювання та забезпечує живучість кіберфізичної інфраструктури при виникненні локальних інцидентів [55, 56].

Запропоновані рішення для забезпечення безпеки та запобігання аваріям у кіберфізичних системах «розумного будинку» базуються на впровадженні інтелектуальних IoT-платформ, які використовують алгоритми глибокого навчання (CNN, LSTM) для моніторингу активності мешканців та виявлення аномальних станів, що можуть свідчити про небезпеку [58, 59]. Для запобігання пожежам та витокам газу пропонуються багаторівневі системи детекції на основі хмарних технологій та мікроконтролерів, які забезпечують миттєве автоматичне перекриття подачі ресурсів та сповіщення користувачів у реальному часі [60, 61]. Окрему увагу приділено надійності зв'язку в критичних ситуаціях через використання відмовостійких мережевих протоколів та технологій туманних обчислень (Fog computing) для мінімізації затримок при передачі екстрених даних [62]. У контексті кібербезпеки розглядаються методи блокчейн та адаптивної аутентифікації для захисту від несанкціонованого втручання в роботу датчиків і актуаторів, що запобігає спробам віддаленого саботажу системи [63, 64]. Крім того, досліджуються гібридні моделі оцінки екологічних та техногенних ризиків у житлових приміщеннях, які поєднують дані сенсорів навколишнього середовища з предиктивною аналітикою для раннього попередження про можливі аварійні ситуації [65, 66].

Запропоновані рішення для виявлення та запобігання аваріям у кіберфізичній системі «Розумний будинок» охоплюють багаторівневий підхід, що включає інтелектуальні IoT-системи для детекції витоків газу та пожежної безпеки з миттєвим сповіщенням через інтерактивні мобільні додатки [67], а також застосування технології блокчейн для захисту даних пожежних станцій і забезпечення цілісності команд керування в мережі IoT [68]. Для критично важливого моніторингу в

реальному часі пропонується гібридна архітектура туманних та периферійних обчислень (fog-edge), яка мінімізує затримки передачі сигналів і підвищує стійкість до кіберзагроз у системах медичного та побутового спостереження [69], тоді як для виявлення аномалій у складних кіберфізичних процесах застосовуються рекурентні нейронні мережі (RNN), здатні ідентифікувати приховані збої та сторонні втручання [70, 71]. Методи запобігання пожежам базуються на алгоритмах злиття даних від декількох сенсорів з використанням нейронних мереж зворотного поширення помилки (BP Neural Network), що дозволяє здійснювати раннє попередження з високою точністю [72]. Стійкість енергетичної інфраструктури «розумного будинку» та міста забезпечується через проактивне управління відмовами у розумних мережах (Smart Grids) [73], використання захищених протоколів на основі штучного інтелекту для електромереж [74] та впровадження методів навчання з підкріпленням для аналізу безпеки й протидії атакам на рівні актуаторів [71]. Окрему увагу приділено моніторингу систем водопостачання через використання далекобійного протоколу LoRaWAN, який забезпечує ефективне виявлення витоків води та мінімізацію збитків у масштабах житлових комплексів [75].

Аналіз існуючих рішень дозволяє виділити кілька критичних недоліків, які обмежують їхнє масове впровадження та ефективність у реальних умовах. Головним бар'єром залишається висока вартість інтелектуальних систем, особливо тих, що використовують складні нейромережеві моделі, дороге серверне обладнання або спеціалізовані когнітивні датчики, що робить повну автоматизацію безпеки недоступною для пересічного споживача. Крім того, більшість представлених на ринку та в наукових працях рішень мають вузькоспеціалізований характер, зосереджуючись на вирішенні лише однієї конкретної проблеми – наприклад, виключно на пожежній сигналізації. Такий фрагментарний підхід змушує власників житла встановлювати кілька незалежних підсистем від різних виробників, які часто несумісні між собою, створюють надмірне навантаження на мережу та потребують окремого обслуговування. Саме тому постає гостра науково-технічна потреба у розробці єдиної комплексної підсистеми, яка б функціонувала як цілісний організм у межах кіберфізичного простору. Актуальним є створення універсального рішення,

здатного одночасно здійснювати прецизійний моніторинг множини критичних параметрів – концентрації природного та чадного газів, появи диму, несанкціонованих витоків води, а також фіксації аномальних температурних коливань. Така багатофункціональність дозволить не лише знизити загальну вартість володіння системою, а й забезпечить синергетичний ефект, коли дані з одного датчика (наприклад, температури) допомагають підтвердити показники іншого (наприклад, диму), суттєво підвищуючи достовірність виявлення аварійних ситуацій. Проєктування такої комплексної підсистеми і є метою даного дослідження.

1.2 Параметри виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

Вчасне виявлення відхилень у параметрах життєзабезпечення оселі є критичним чинником, що визначає межу між керованою побутовою ситуацією та масштабною техногенною катастрофою. У сучасному високотехнологічному помешканні, насиченому інженерними комунікаціями, швидкість фізичних процесів під час аварії часто перевищує здатність людини до адекватної реакції. Саме тому перехід від простого моніторингу до інтелектуального прогнозування стає фундаментальною вимогою до безпеки сучасного житла. Ефективність кіберфізичної системи «Розумний будинок» у контексті безпеки безпосередньо залежить від точності та оперативності моніторингу ключових фізичних параметрів середовища. Кожен тип потенційної аварії має власні унікальні характеристики, які потребують специфічних методів детектування та відповідних алгоритмів реагування для запобігання катастрофічним наслідкам.

Параметр концентрації чадного газу вимагає особливої уваги через свою підступність: відсутність органолептичних ознак робить його виявлення на ранніх стадіях життєво необхідним. Навіть незначне перевищення норми впродовж тривалого часу може спричинити незворотні наслідки для здоров'я, тому система повинна ідентифікувати загрозу ще до появи перших симптомів отруєння у мешканців. Постійний контроль цього показника є базовим елементом захисту в

будинках із пічним або газовим опаленням. Виявлення чадного газу (CO) є одним із найбільш критичних завдань, оскільки цей газ не має кольору та запаху, що робить його непомітним для людини. Основним параметром тут виступає концентрація газу в повітрі, що вимірюється в частках на мільйон (ppm). Для надійної роботи системи «золотим стандартом» є напівпровідниковий датчик MQ-7, який здатен фіксувати небезпечні рівні CO у діапазоні від 10 до 1000 ppm.

Виявлення витоків природного газу є пріоритетним через високий ризик миттєвого вибуху при досягненні критичної концентрації паливно-повітряної суміші. Вчасна фіксація появи метану в повітрі дозволяє системі не лише попередити людей, а й здійснити превентивні дії, як-от примусову вентиляцію або перекриття магістралі. Це радикально знижує ймовірність руйнування будівельних конструкцій та виникнення супутніх пожеж. Моніторинг витоків природного газу (метану, CH_4) базується на фіксації концентрації горючих речовин, що можуть призвести до вибуху при досягненні нижньої межі вибуховості. Для цього параметру «золотим стандартом» бюджетних систем є датчик MQ-4, який має високу селективність саме до метану. Оскільки метан легший за повітря, критично важливо враховувати геометричний параметр розміщення датчика у верхній частині приміщення.

Моніторинг параметрів задимлення дозволяє розпізнати пожежу на стадії тління, коли концентрація продуктів горіння ще не є летальною. Раннє виявлення частинок диму дає дорогоцінний час для евакуації або локалізації джерела вогню за допомогою автоматичних засобів гасіння. В умовах використання сучасних синтетичних матеріалів в інтер’єрі, швидкість поширення токсичного диму робить кожну секунду затримки критичною. Параметр задимленості є ключовим індикатором зародження пожежі, особливо на стадії тління матеріалів. Використання датчика MQ-2 дозволяє не лише виявляти дим, а й створювати мультисенсорний контур разом із детекторами газів, що значно здешевлює апаратну частину системи. Це забезпечує комплексний підхід до пожежної безпеки, де задимлення аналізується як динамічний показник зміни прозорості та хімічного складу повітря.

Контроль температурного фону є універсальним індикатором, що дозволяє верифікувати пожежні ситуації та виявляти несправності в роботі електромереж.

Аномальне зростання температури часто передує появі відкритого полум'я, сигналізуючи про перегрів кабелів або порушення цілісності термоізоляції приладів. Вчасна реакція на зміну цього параметра дозволяє запобігти займанню ще до моменту виникнення пожежі. Температурний моніторинг виступає не лише як самостійний параметр контролю мікроклімату, а й як засіб верифікації пожежних ситуацій. Використання цифрового датчика DS18B20 дозволяє фіксувати аномальні стрибки температури понад 60°C. Такий тепловий параметр у поєднанні з даними про задимлення дає системі можливість майже зі стовідсотковою впевненістю ідентифікувати реальну пожежу, відсікаючи помилкові спрацювання від кухонних парів чи пилу.

Параметри витоку води потребують негайного реагування для мінімізації матеріальних збитків та запобігання короткому замиканню в електромережі. Навіть невеликий розлив рідини може призвести до пошкодження майна декількох поверхів та руйнування оздоблювальних матеріалів. Автоматизоване розпізнавання присутності вологи на підлозі дозволяє системі миттєво ізолювати пошкоджену ділянку водопроводу. Виявлення витоків води базується на параметрі електропровідності рідкого середовища. Зондовий датчик YI-S фіксує замикання контактів при появі вологи, що є сигналом про прорив водопроводу або несправність побутової техніки. Для запобігання помилковим тривогам через підвищену вологість алгоритм системи передбачає часовий параметр фільтрації – сигнал вважається аварійним лише при його стабільності протягом 1-2 секунд.

Актуальність одночасного відстеження всіх цих показників полягає у синергетичному ефекті, коли дані з різних джерел доповнюють одне одного. Це створює умови для ситуаційної інтелектуалізації, де система розуміє контекст подій і не реагує на випадкові одиничні сплески. Такий комплексний підхід підвищує загальну стійкість оселі до мультифакторних впливів та складних аварійних сценаріїв.

Соціальний параметр актуальності підсистеми полягає у створенні безпечного середовища для вразливих верств населення. Для людей похилого віку автоматичне запобігання аваріям є життєво необхідною функцією, оскільки вони не завжди можуть вчасно зреагувати на запах газу чи появу води. Система фактично виконує роль

«інтелектуального щита», який бере на себе функцію постійної діагностики оселі. Для вразливих верств населення, таких як самотні літні люди, вчасне виявлення цих параметрів є соціально значущою функцією, що компенсує зниження сенсорного сприйняття. Автоматизована діагностика середовища перетворює помешкання на надійний інтелектуальний щит, здатний захистити людину в екстремальних умовах. Це забезпечує незалежність та безпеку проживання без потреби в постійній присутності сторонніх осіб.

Параметр адаптивності забезпечується здатністю системи до самонавчання на основі історичних даних про стан середовища. Кіберфізична система аналізує звичні патерни використання енергоносіїв та води, що дозволяє виявляти аномалії навіть при значеннях, які формально не виходять за межі загальних нормативів. Це підвищує інтелектуальність захисту та робить його більш персоналізованим. Онтологічна відкритість є параметром, що дозволяє системі еволюціонувати без заміни базової архітектури. Користувач може додавати нові датчики або розширювати перелік сценаріїв реагування залежно від власних потреб чи змін в інженерних мережах будинку. Такий підхід забезпечує довговічність інвестицій у безпеку житла.

Вартість розробки та впровадження інтелектуальних механізмів контролю є значно нижчою за потенційні витрати на ліквідацію наслідків аварій. Вчасне запобігання пожежі чи вибуху газу зберігає не лише матеріальні активи, а й найвищу цінність – людське життя. Таким чином, інвестиції в цифрові системи безпеки є економічно виправданими та стратегічно необхідними для будь-якого сучасного домогосподарства.

Аналіз розглянутих наукових праць свідчить, що моніторинг параметрів у кіберфізичних системах «Розумний будинок» базується на багатофакторному аналізі фізичних та середовищних показників для вчасного запобігання аваріям. Ключовими параметрами виявлення небезпек є концентрація горючих і токсичних газів, зокрема чадного газу (CO) та метану [76, 77], рівень задимленості приміщення [77, 78], а також критичні показники температури та вологості, що вказують на зародження пожежі або несправність кліматичних систем [79-81]. Для запобігання затопленням відстежуються параметри наявності води на поверхнях та рівень рідини в резервуарах

[77, 78]. Особлива увага приділяється параметрам споживання електроенергії та моніторингу електричних навантажень для ідентифікації аномалій, що можуть призвести до короткого замикання [82, 83]. У контексті пожежної безпеки аналізуються візуальні ознаки вогню та диму через обробку зображень у реальному часі [84, 85], а також параметри якості повітря (PM2.5, VOC) як непрямі індикатори аварійних станів [81]. Дослідження також виділяють акустичні параметри для детектування розбиття скла або незвичних шумів [86] та параметри цілісності мережі й затримок передачі даних, що критично для систем реального часу при виникненні надзвичайних ситуацій [76, 79].

Кіберфізична система, що працює в режимі реального часу, здатна адаптуватися до динамічного середовища та приймати рішення в умовах неповноти даних. Це виводить безпеку на новий рівень, де будинок самостійно оцінює ризики та діє як активний суб'єкт захисту. Впровадження таких рішень є пріоритетним кроком у розвитку концепції безпечного міста та інтелектуальних систем життєзабезпечення майбутнього. Підсумовуючи, інтеграція параметрів моніторингу газу, диму, води та температури в єдину кіберфізичну структуру створює якісно новий рівень захисту. Комплексний аналіз цих показників дозволяє перетворити «Розумний будинок» з просто комфортного приміщення на керовану екосистему, здатну ефективно протидіяти техногенним викликам сучасності.

1.3 Висновки. Постановка задачі

Дослідження підтвердило, що сучасні кіберфізичні системи еволюціонували від простих дистанційно керованих пристроїв до складних інтегрованих екосистем. У розділі обґрунтовано, що такі системи стирають межу між віртуальним та матеріальним світами, об’єднуючи обчислювальні алгоритми, цифрові сервіси та фізичні пристрої в єдиний функціональний контур, що працює в безперервному циклі збору та аналізу даних.

Встановлено, що ідентифікація надзвичайних ситуацій стає значно надійнішою при збільшенні кількості параметрів моніторингу. Окрім аналізу життєво важливих

показників людини, критично важливим є врахування параметрів середовища, таких як температура, вологість, наявність диму чи газу, що дозволяє системі приймати більш зважені рішення на основі багатокритеріального аналізу.

Виявлено, що традиційні методи охорони житла, які базуються на зовнішньому спостереженні, є недостатніми, оскільки вони не дають інформації про умови всередині будинку. Розділ демонструє перевагу внутрішнього моніторингу за допомогою інтегрованих датчиків вогню, газу та руху, що дозволяє охоронним службам та власникам отримувати актуальні сповіщення про реальний стан об'єкта в режимі реального часу.

Аналіз існуючих технічних рішень виявив стрімкий розвиток інтелектуальних пристроїв на базі сучасних мікроконтролерів (зокрема ESP32-S3), які поєднують моніторинг безпеки з голосовими помічниками на базі великих мовних моделей (LLM). Це забезпечує якісно новий рівень взаємодії користувача з системою безпеки, роблячи її більш адаптивною та контекстно-залежною.

У розділі детально розглянуто прогрес у методах виявлення пожеж. Традиційні теплові та димові датчики мають обмеження щодо часу реагування, тому запропоновано використання моделей на основі багатомасштабних інформаційних трансформаторів (DETR) та згорткових нейронних мереж (CNN). Такі підходи дозволяють розпізнавати ознаки вогню та диму на відеокадрах із високою точністю та в режимі реального часу.

Значну увагу приділено методам обробки даних в умовах невизначеності. Використання нечіткої логіки та федеративного навчання дозволяє системам «Розумного будинку» ефективно працювати з помилковою або неповною інформацією від датчиків. Це особливо важливо для виявлення аномальних періодів бездіяльності мешканців або прогнозування пожежі на межі мережевих середовищ.

Критичний огляд існуючих систем виявив їхні суттєві недоліки: високу вартість розгортання та вузьку спеціалізацію на одній конкретній проблемі. Більшість рішень зосереджені або лише на пожежній безпеці, або лише на медичному моніторингу, що змушує користувачів інсталювати кілька непов'язаних між собою систем, здорожуючи загальну інфраструктуру.

За результатами аналізу обґрунтовано необхідність розробки саме комплексної підсистеми безпеки. Така підсистема має об'єднувати моніторинг витоків чадного та природного газу, появи диму, води та аномальних температур в межах єдиного апаратного та програмного рішення. Це дозволить не лише знизити вартість системи, а й забезпечити синергію даних для точнішого розпізнавання загроз.

Підсумовано, що інтеграція параметрів моніторингу в єдину кіберфізичну структуру на базі сучасних протоколів передачі даних та контролерів є найбільш перспективним шляхом. Це дозволяє створити автономну та надійну систему, здатну самостійно оцінювати ризики та діяти як активний суб'єкт захисту, що є важливим кроком до реалізації концепції безпечного міста майбутнього.

Метою кваліфікаційної роботи є автоматизація процесу виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», зокрема, автоматизація процесу виявлення витоків чадного газу, природного газу, води, виявлення диму, аномально високих температур.

Поставлена мета досягається розв’язанням таких основних *задач*:

1) аналіз відомих методів та рішень для виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

2) вибір компонентів для підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

3) розроблення методу та алгритму функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

4) розроблення архітектури підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;

5) проведення експериментів із використанням розробленої підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Об’єктом дослідження є процес виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Предметом дослідження є метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

2 ВИБІР КОМПОНЕНТІВ ДЛЯ ПІДСИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АВАРІЙНИМ СИТУАЦІЯМ В КІБЕРФІЗИЧНІЙ СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

2.1 Вибір датчиків для нижнього рівня підсистеми

Отже, основні параметри, які виявлятиме підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»:

1) наявність чадного газу;
2) наявність витоку природного газу;
3) наявність диму;
4) наявність витоку води;
5) наявність аномально високих температур.

Для побудови комплексної підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» важливо обрати датчики, які поєднують точність, довговічність та прийнятну ціну.

Датчики чадного газу (CO) працюють на різних принципах – напівпровідникові (дешевші, але споживають більше енергії) та електрохімічні (високоточні, ідеальні для автономних систем). У Таблиці 2.1 представлені результати порівняльного аналізу датчиків чадного газу.

Таблиця 2.1 – Порівняльний аналіз датчиків чадного газу

Модель датчика	Тип	Діапазон вимірювання (ppm)	Переваги	Недоліки	Орієнтовна вартість
MQ-7	Напівпро-відниковий	10 – 1000	Дуже низька ціна, простота підключен-	Потребує циклічного нагріву, високе енерго-	Низька

Продовження таблиці 2.1

			ня до Arduino/ESP32	споживання, чутливий до вологості	
MQ-9	Напівпровідниковий	10 – 1000	Комбінований – реагує на CO та горючі гази (CH4, LPG)	Менша точність саме по чадному газу порівняно з MQ-7	Низька
MG-811	Електрохімічний / Хімічний	350 – 10000	Висока чутливість, стабільність роботи	Висока ціна, складніша схема підключення	Середня
ME2-CO	Електрохімічний	0 – 1000	Висока точність, лінійна залежність сигналу, низьке енергоспоживання	Обмежений термін служби електроліту (2-5 років)	Середня

Кінець таблиці 2.1

FIGARO TGS5042	Електро-хімічний	0 – 10000	Промисло-вий стандарт, висока селектив-ність, довгий термін служби (до 10 років)	Висока вартість, потребує якісної обв'язки	Висока

Для розробки бюджетної, але надійної системи «Розумного будинку» для широкого вжитку, оптимальним вибором є MQ-7 (для прототипів та систем з живленням від мережі). Оскільки метою є побудова комплексної системи, то більше підходять датчики серії MQ, які мають схожу логіку підключення, що спростить проєктування плати для моніторингу газу, диму та витоків одночасно.

Датчик MQ-7 (рис. 2.1) є спеціалізованим напівпровідниковим пристроєм, призначеним для детектування концентрації чадного газу (CO) у навколишньому середовищі в діапазоні від 10 до 1000 ppm. Його робота базується на зміні провідності шару діоксиду олова (SnO_2) при контакті з молекулами газу, що робить його чутливим і надійним інструментом для побутових систем безпеки. Завдяки низькій вартості та простоті інтеграції з популярними платформами, такими як Arduino або ESP32, цей сенсор вважається оптимальним вибором для створення прототипів комплексних систем «Розумного будинку».

Особливістю функціонування MQ-7 є необхідність циклічного нагріву для забезпечення точності вимірювань. Датчик працює у двох фазах: спочатку нагрівальний елемент споживає 5 В для очищення сенсора від адсорбованих частинок, а потім напруга знижується до 1,4 В для безпосереднього зчитування концентрації CO. Це зумовлює вище енергоспоживання порівняно з

електрохімічними аналогами, проте забезпечує стабільну роботу при живленні від стаціонарної мережі.

У складі комплексної кіберфізичної системи датчик MQ-7 відіграє роль критичного вузла моніторингу, оскільки чадний газ не має кольору та запаху, що робить його виявлення на ранніх стадіях життєво необхідним. Використання цього сенсора дозволяє перетворити звичайний сповіщувач на інтелектуальний агент безпеки, який через контролер ESP32 передає дані за протоколом MQTT, гарантуючи вчасне інформування користувача про небезпеку. Правильне калібрування та програмна обробка сигналу дозволяють мінімізувати вплив вологості повітря на точність показників.

Рисунок 2.1 – Датчик CO чадного газу MQ-7 5B

Для моніторингу природного газу (метану CH4) найчастіше використовують напівпровідникові датчики, які змінюють свій опір при контакті з молекулами газу. Оскільки метан легший за повітря, при проєктуванні системи слід враховувати, що ці датчики мають розміщуватися у верхній частині приміщення. У Таблиці 2.2

наведені результати порівняльного аналізу датчиків природного газу, які найкраще підходять для інтеграції в кіберфізичну систему «Розумний будинок».

Таблиця 2.2 – Порівняльний аналіз датчиків природного газу

Модель датчика	Тип	Діапазон детектування (ppm)	Особливості	Енерго-споживання	Вартість
MQ-4	Напівпро-відникo-вий (SnO2)	200 – 10000	Висока чутливість саме до метану (CH4), низька чутливість до диму	Високе	Низька
MQ-5	Напівпро-відникo-вий	200 – 10000	Більш універсаль-ний – реагує на метан та пропан-бутан (LPG)	Високе	Низька
MQ-9	Напівпро-відникo-вий	100 – 10000	Гібридний – виявляє метан та чадний газ, проте з меншою точністю	Середнє	Низька

Кінець таблиці 2.2

			порівняно з MQ-7		
TGS2611	Напівпровідниковий	500 – 10000	Висока селективність до метану, компактний розмір	Середнє	Висока
MiCS-5524	MEMS (напівпровідниковий)	1000 – 10000	Сучасна технологія, дуже компактний, придатний для портативних пристроїв	Низьке	Середня

MQ-4 є «золотим стандартом» для бюджетних комплексних систем безпеки. Його головна перевага – вузька спеціалізація на метані, що зменшує кількість хибних спрацьовувань, коли на кухні готується їжа або використовуються миючі засоби. MQ-5 доцільно обирати лише в тому випадку, якщо в будинку використовується і природний газ (магістральний), і балонний (пропан), оскільки він ефективно «бачить» обидва види палива. TGS2611 рекомендується для систем преміум-класу, де пріоритетом є довговічність та стабільність показань без частих калібрувань. Отже, для нашої підсистеми оберемо в якості датчику природного газу саме датчик MQ-4 (рис. 2.2).

Рисунок 2.2 – Датчик природного газу MQ-4

Датчик MQ-4 є спеціалізованим напівпровідниковим пристроєм, який вважається «золотим стандартом» для бюджетних комплексних систем безпеки завдяки своїй високій чутливості до природного газу, зокрема метану (CH4). Його робота базується на зміні провідності чутливого шару з діоксиду олова (SnO_2) при контакті з молекулами горючого газу. Ключовою перевагою цієї моделі є вузька спеціалізація, що дозволяє мінімізувати кількість хибних спрацьовувань від сторонніх подразників, таких як кухонні запахи, дим або миючі засоби.

Технічні характеристики датчика дозволяють детектувати метан у широкому діапазоні від 200 до 10000 ppm, що є достатнім для виявлення небезпечних концентрацій задовго до досягнення нижньої межі вибуховості. Оскільки природний газ легший за повітря і має тенденцію накопичуватися під стелею, при проектуванні кіберфізичної системи важливо враховувати геометричний параметр розміщення сенсора у верхній частині приміщення. Датчик потребує постійного

нагріву внутрішнього елемента для підтримки стабільної працездатності, що зумовлює його відносно високе енергоспоживання.

У структурі інтелектуального «Розумного будинку» MQ-4 інтегрується як важливий елемент локального рівня збору даних під керуванням контролера ESP32. Аналоговий сигнал від сенсора зчитується контролером, після чого інформація передається за протоколом MQTT для подальшого ситуаційного аналізу. Це дозволяє не лише констатувати факт витоку, а й реалізувати сценарії автоматичного перекриття магістральних клапанів подачі газу, що є критично важливим для збереження життя мешканців та цілісності майна.

Для комплексної системи безпеки вибір датчика диму є критичним, оскільки саме вони відповідають за раннє виявлення пожежі. У сучасних кіберфізичних системах використовуються переважно два типи – іонізаційні (швидко реагують на відкрите полум’я) та оптичні/фотоелектричні (краще розпізнають тління та густий дим). У Таблиці 2.3 представлені результати порівняльного аналізу датчиків диму, які можна інтегрувати в систему «Розумний будинок».

Таблиця 2.3 – Порівняльний аналіз датчиків диму

Модель датчика	Тип	Чутливість	Переваги	Недоліки	Ціна
MQ-2	Напівпро-відніко-вий	Дим, LPG, пропан, водень	Універсаль-ність, дуже низька ціна, простота обробки сигналу	Високе енергоспо-живання	Низька
GP2Y1010 AU0F	Оптичний (інфрачер-воний)	Дрібні частки пилу та диму	Дуже низьке енергоспо-живання, висока	Потребує захисту від зовнішнього світла,	Середня

Кінець таблиці 2.3

			швидкість реакції, компактність	чутливий до звичайного пилу	
MAX30105	Оптичний (Particle Sensor)	Дим, дихання, частки	Надзвичайна точність (використо-вує ІЧ, червоний та зелений світлодіоди)	Складний протокол зв'язку (I2C), вища ціна	Висока
MQ-303A	Напівпрові дниковий (MEMS)	Дим, пари спирту	Мініатюрний розмір, низьке енергоспо-живання порівняно з серією MQ	Менша площа контакту з повітрям, потребує калібрування	Середня
DSM501A	Оптичний	Дим, пил (PM2.5)	Здатний розрізняти розмір часток	Габаритний корпус, потребує вертикаль-ного встановлення	Середня

MQ-2 (рис. 2.3) – це оптимальний вибір для комплексного бюджетного рішення, оскільки він дозволяє одним модулем «закрити» питання і диму, і витоку горючих газів. Це значно здешевлює конструкцію, що відповідає вимозі щодо подолання дороговизни існуючих систем. Якщо ж пріоритетом є точність та

уникнення хибних спрацювань, варто інтегрувати оптичний датчик типу GP2Y1010AU0F або DSM501A. Вони аналізують фізичну наявність часток у повітрі, а не хімічний склад, що робить їх надійнішими. Отже, для нашої підсистеми оберемо в якості датчику диму саме датчик MQ-2.

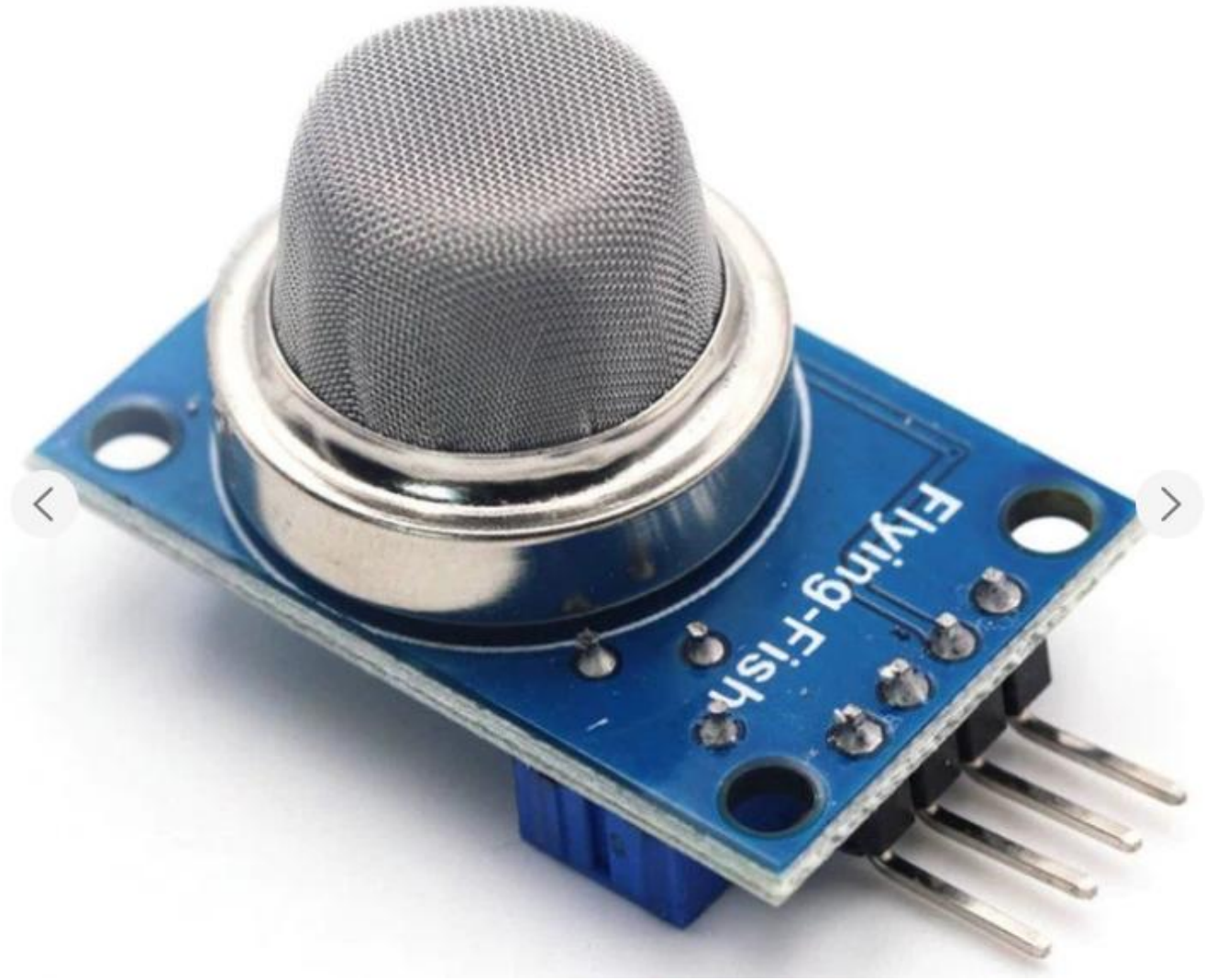


Рисунок 2.3 – Датчик диму MQ-2

Датчик MQ-2 є універсальним напівпровідниковим пристроєм, який широко використовується в кіберфізичних системах для виявлення задимлення та широкого спектра горючих газів, таких як зріджений нафтовий газ (LPG), пропан, бутан та водень. Його робота базується на зміні опору чутливого шару з діоксиду олова (SnO_2) при контакті з молекулами диму або газу, що дозволяє системі реагувати на небезпеку на ранніх стадіях тління або витоку. Завдяки своїй низькій

вартості та простоті обробки сигналу, цей сенсор є оптимальним вибором для побудови бюджетних комплексних систем безпеки «Розумного будинку».

У межах розроблюваної підсистеми датчик MQ-2 виконує роль багатофункціонального модуля, який дозволяє одним пристроєм закрити питання детектування як диму, так і витоку горючих газів. Це значно здешевлює загальну конструкцію системи, що відповідає ключовій вимозі подолання дороговизни існуючих комерційних рішень. Використання напівпровідникової технології забезпечує швидку реакцію, хоча й потребує постійного підігріву чутливого елемента, що підвищує загальне енергоспоживання вузла.

Інтеграція MQ-2 у кіберфізичну систему на базі контролера ESP32 дозволяє реалізувати принцип ситуаційної інтелектуалізації через перехресну верифікацію даних. Наприклад, при фіксації задимлення датчиком MQ-2, аналітичне ядро системи зіставляє ці дані з показниками температури від датчика температури; якщо обидва параметри демонструють аномальне зростання, система з високою точністю ідентифікує пожежу. Такий підхід мінімізує кількість хибних спрацювань від кухонних парів або пилу, забезпечуючи надійну роботу системи в реальному часі.

Для комплексної системи безпеки датчик витоку води є одним із найпростіших, але водночас критично важливих елементів. На відміну від газових сенсорів, вони зазвичай споживають мінімум енергії, оскільки працюють за принципом замикання контактів через провідне середовище (воду). У Таблиці 2.4 представлені результати порівняльного аналізу датчиків витоку води, які допоможуть запобігти затопленню.

Таблиця 2.4 – Порівняльний аналіз датчиків витоку води

Модель датчика	Тип	Принцип роботи	Переваги	Недоліки	Ціна
HW-038 (Rain/	Контакт-ний	Вимірювання опору	Надзвичайно низька ціна,	Швидка корозія	Дуже низька

Кінець таблиці 2.4

Water Level)	(резис-тивний)		сумісність з усіма мікроконтро лерами	контактів (електроліз), потребує частої заміни	
YI-S (Зондовий) WL400 Water Level Sensor	Контакт-ний (щуповий)	Два металеві щупи, що замикаються водою	Стійкість до корозії, легкість очищення, довговічність	Потребує безпосеред-нього контакту з калюжею певної глибини	Низька
Non-contact (Безкон-тактний)	Ємнісний	Виявлення води через стінку труби або резервуара	Не контактує з водою (немає корозії), висока надійність	Складніше налаштувати для виявлення розливу на підлозі	Середня
Optical Liquid Level	Оптичний	Відбиття/зал омлення світла всередині призми	Висока точність, миттєва реакція, працює роками	Складніший у монтажі на пласкі поверхні (підлогу)	Середня
XKC-Y25-T12V	Індуктив-ний / Ємнісний	Детектуван-ня рідини без прямого контакту	Безпека, ідеально для агресивних середовищ	Чутливий до товщини поверхні, через яку «дивиться»	Висока

Найдешевшим є датчик HW-038, проте для реальної експлуатації в «Розумному будинку» він не підходить через швидке руйнування контактів під дією струму та вологи. Тому оптимальним вибором для комплексної підсистеми є зондові датчики (YI-S) з нержавіючими щупами або контактними пластинами, покритими золотом/нікелем – WL400 Water Level Sensor (рис. 2.4). Вони дешеві, надійні та легко інтегруються в загальний аналітичний модуль. Щоб уникнути помилкових тривог через високу вологість, у програмне забезпечення комплексної системи варто додати алгоритм перевірки – сигнал вважається аварійним лише тоді, коли рівень сигналу з датчика тримається стабільно високим протягом 1-2 секунд.

Рисунок 2.4 – Датчик витоку води WL400 Water Level Sensor

Зондовий датчик YI-S є критично важливим елементом підсистеми виявлення аварійних ситуацій, що відповідає за моніторинг витоків води та запобігання затопленню приміщень. На відміну від газових сенсорів, він працює за кондуктометричним принципом, де замикання двох металевих щупів через провідне середовище (воду) призводить до різкої зміни електричного опору, що фіксується контролером як сигнал тривоги. Вибір саме зондової моделі

обумовлений її високою стійкістю до корозії та довговічністю, оскільки щупи часто виготовляються з нержавіючої сталі або покриваються захисними шарами золота чи нікелю. Цей датчик має характерну конструкцію з нержавіючими контактними щупами, що забезпечує його стійкість до корозії при постійному контакті з вологою. Така форма дозволяє надійно фіксувати наявність води на поверхні підлоги або в піддонах побутової техніки, замикаючи електричний контур при контакті рідини з обома електродами.

У порівнянні з дешевшими резистивними платами (наприклад, HW-038), датчик YI-S демонструє кращу експлуатаційну надійність у реальних умовах «Розумного будинку», оскільки він менше схильний до швидкої деградації контактів під дією електролізу. Це робить його оптимальним вибором для комплексної підсистеми, де пріоритетом є тривала робота без необхідності частого обслуговування чи заміни компонентів. Датчик легко інтегрується в загальний аналітичний модуль на базі ESP32, забезпечуючи миттєву реакцію на появу рідини в критичних зонах, таких як місця підключення пральних машин або вузли водопостачання.

Для підвищення достовірності роботи системи та уникнення помилкових тривог через випадкові бризки або високу вологість повітря, дані з датчика YI-S обробляються спеціальним алгоритмом. Програмне забезпечення контролера підтверджує аварійний стан лише у випадку, якщо рівень сигналу з сенсора залишається стабільно високим протягом 1–2 секунд. Такий підхід у поєднанні з низькою вартістю та простотою монтажу дозволяє створити надійний бар'єр проти затоплення, який є невід'ємною частиною інтелектуального «щита» безпеки сучасного помешкання.

Для комплексної системи безпеки датчик температури відіграє подвійну роль – він не лише забезпечує клімат-контроль, а й слугує критичним верифікатором пожежі. Якщо датчик диму фіксує задимлення, а температурний сенсор одночасно показує стрімке зростання температури більше 60°C, система може з майже 100% впевненістю ідентифікувати реальну пожежу, уникаючи помилкових тривог. В

Таблиці 2.5 представлені результати порівняльного аналізу датчиків температури, придатних для детектування аномальних температур.

Таблиця 2.5 – Порівняльний аналіз датчиків температури

Модель датчика	Тип	Діапазон температур	Точність	Переваги для системи безпеки	Вартість
DHT11 / DHT22	Цифровий (містить ємнісний сенсор вологості)	-40°C ... +80°C	±0.5 - 2°C	Вимірює і вологість, низька ціна	Низька
DS18B20	Цифровий (1-Wire)	-55°C ... +125°C	±0.5°C	Герметичний корпус (можна занурювати у воду), висока перешкодо-стійкість	Середня
LM35	Аналоговий	-55°C ... +150°C	±0.25°C	Пряма лінійна залежність 10 мВ/1°C, надзвичайно швидка реакція	Низька
BMP280 / BME280	Цифровий (I2C)	-40°C ... +85°C	±1°C	Додатково вимірює тиск, що	Середня

Кінець таблиці 2.5

				дозволяє фіксувати зворотну тягу в димоходах	
MLX90614	ІЧ-пірометр (безконтактний)	-70°C ... +380°C	±0.5°C	Дистанційне виявлення джерел тепла (може «побачити» вогонь здалеку)	Висока

Для виявлення (веріфікації) пожежі найкращим вибором є DS18B20. Завдяки цифровому інтерфейсу 1-Wire, можна підключити десятки таких датчиків до одного піна мікроконтролера, розмістивши їх у кожній кімнаті. Його здатність працювати до +125°C дозволяє системі продовжувати передавати дані навіть у розпал аварії.

Цифровий датчик температури DS18B20 є високоточним пристроєм, який у комплексній системі безпеки відіграє критичну роль верифікатора пожежних ситуацій. На відміну від аналогових терморезисторів, він використовує протокол передачі даних 1-Wire, що дозволяє підключати велику кількість таких сенсорів до одного цифрового піна контролера ESP32, розміщуючи їх у кожній кімнаті для повного охоплення будинку. Датчик має широкий діапазон вимірювання від –55°C до +125°C із високою точністю ±0,5°C, що дозволяє йому стабільно функціонувати та передавати дані навіть у розпал аварійної ситуації.

У межах розробленої архітектури цей датчик забезпечує реалізацію принципу перехресної перевірки: якщо газові сенсори фіксують задимлення, а DS18B20 одночасно показує стрімке зростання температури понад 60°C, система з

майже 100% впевненістю ідентифікує реальну пожежу. Це дозволяє ефективно відсікати помилкові тривоги, що виникають через кухонну пару або пил, підвищуючи загальну надійність кіберфізичної системи. Герметичне виконання корпусу деяких модифікацій датчика також дозволяє використовувати його у вологих середовищах, що розширює можливості моніторингу.

Завдяки цифровій природі сигналу, DS18B20 (рис. 2.5) забезпечує високу перешкодостійкість, що є критичним для систем «Розумного будинку», де працює багато побутових електроприладів. Після зчитування температурного параметра контролер ESP32 передає дані через протокол MQTT на верхній аналітичний рівень для прийняття рішень. Така інтеграція робить датчик не просто термометром, а повноцінним компонентом когнітивного вузла безпеки, здатним адаптуватися до мінливих умов середовища та забезпечувати автономний захист житла.

Рисунок 2.5 – Датчик детектування аномальної температури DS18B20

Отже, основними компонентами нижнього рівня підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» є:

1) датчик чадного газу MQ-7;
2) датчик природного газу MQ-4;
3) датчик диму MQ-2;
4) датчик витоку води YI-S WL400 Water Level Sensor;
5) датчик аномально високих температур DS18B20.

2.2 Вибір компонентів для середнього рівня підсистеми

Для інтеграції обраного набору датчиків (MQ-7, MQ-4, MQ-2, YI-S WL400 Water Level Sensor та DS18B20) контролер повинен мати достатню кількість аналогових входів (для серії MQ) та цифрових інтерфейсів, а також підтримувати бездротовий зв'язок для миттєвого сповіщення користувача. У Таблиці 2.6 представлені результати порівняльного аналізу популярних платформ для створення кіберфізичних систем.

Таблиця 2.6 – Порівняльний аналіз контролерів

Характе-ристика	Arduino Uno (R3/R4)	ESP8266 (NodeMCU)	ESP32 (DevKit V1)	STM32 (Black Pill)	Raspberry Pi Zero 2 W
Процесор	ATMega328P (8-біт)	ESP8266 (32-біт)	Dual-core (32-біт)	Cortex-M4	ARM Cortex-A53
Аналогові входи (ADC)	6 (10-біт)	1 (10-біт)	15+ (12-біт)	10 (12-біт)	Немає (потрібен АЦП)
Бездрото-вий зв'язок	Немає	Wi-Fi	Wi-Fi + Bluetooth	Немає	Wi-Fi + Bluetooth

Кінець таблиці 2.6

Енергоспо-живання	Низьке	Середнє	Середнє (є Deep Sleep)	Низьке	Високе
Обсяг пам'яті (Flash)	32 KB	4 MB	4 MB - 16 MB	512 KB	Залежить від SD-карти
Вартість	Низька	Дуже низька	Низька/ Середня	Середня	Висока (дефіцит)

Для нашої комплексної підсистеми найкращим вибором є ESP32, оскільки він має велику кількість АЦП для датчиків MQ-7, MQ-4, MQ-2, що видають аналоговий сигнал. На відміну від ESP8266 (де вхід лише один) або Arduino (де їх 6, але низька розрядність), ESP32 дозволяє підключити всі газові датчики одночасно з високою точністю зчитування. ESP32 має вбудований Wi-Fi та Bluetooth, що є критично важливим для «Розумного будинку», оскільки не потрібно купувати додаткові модулі, щоб надсилати сповіщення про витоки газу чи пожежу на смартфон через мобільний застосунок або протокол MQTT. ESP32 має двоядерний процесор, який дозволяє розділити завдання – одне ядро займається постійним опитуванням датчиків у реальному часі, а інше – обробкою Wi-Fi з’єднання та шифруванням даних. ESP32 відмінно працює з протоколом 1-Wire (датчик DS18B20), тобто датчик температури можна підключити до будь-якого вільного цифрового піна. При високій потужності ESP32 залишається доступним за ціною, що відповідає концепції подолання дороговизни систем безпеки.

Усі параметри з дачиків збираються контролером ESP32 (рис. 2.6), який виступає центральним вузлом обробки на локальному рівні. Завдяки вбудованому 12-бітному АЦП, контролер перетворює аналогові сигнали від датчиків серії MQ у цифрові значення з високою точністю. Це дозволяє системі не просто фіксувати перетин порогу, а відстежувати динаміку зміни параметрів у часі для прогнозування розвитку аварії.

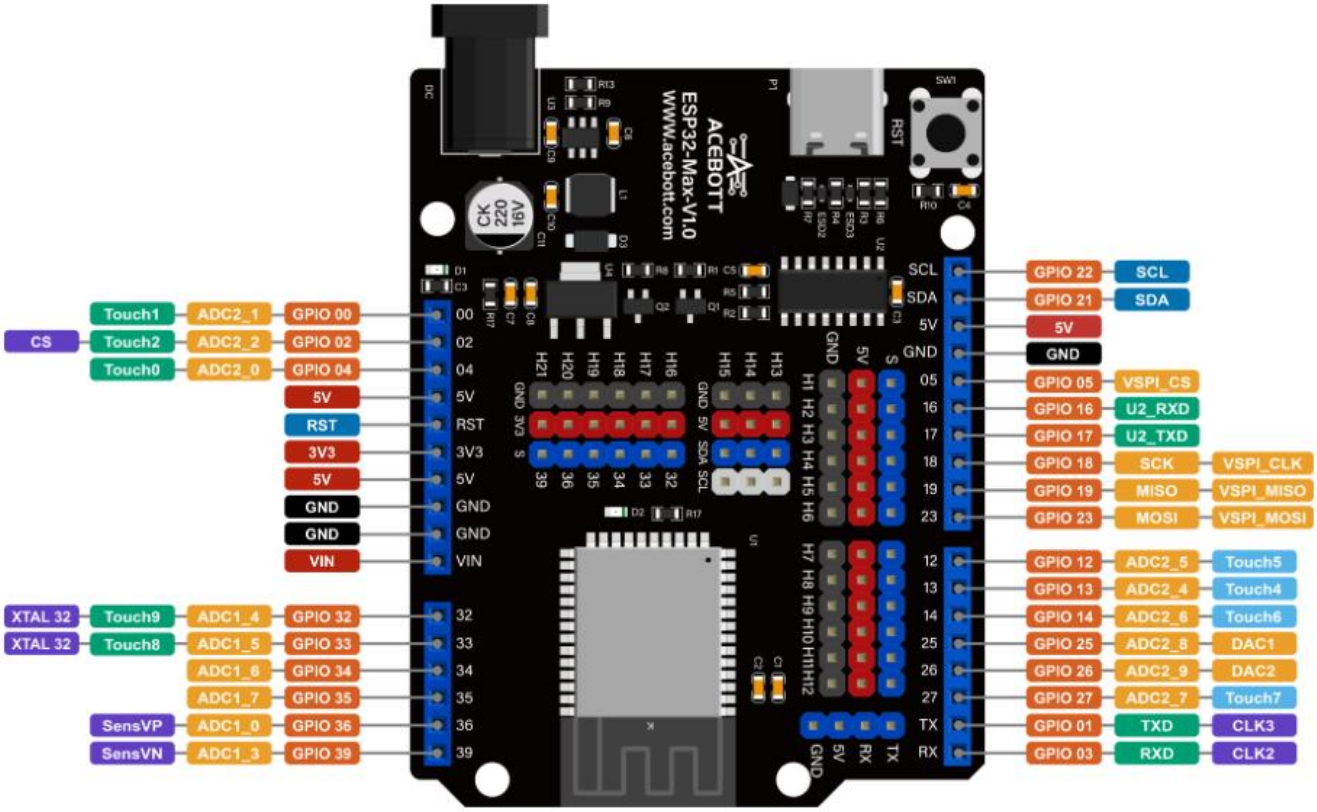


Рисунок 2.6 – Плата контролера ESP32

Контролер ESP32 (зокрема у версії DevKit V1) є високопродуктивною 32-бітною системою на кристалі (SoC), яка виступає центральним обчислювальним ядром для сучасних кіберфізичних систем «Розумного будинку». Головною перевагою цього контролера є наявність двоядерного процесора, що дозволяє ефективно розділяти завдання: одне ядро забезпечує постійне опитування сенсорів (MQ-7, MQ-4, MQ-2, DS18B20 та YI-S WL400 Water Level Sensor) у реальному часі, тоді як інше відповідає за мережеву комунікацію та шифрування даних. Це гарантує високу швидкість обробки інформації та миттєву реакцію на виникнення аварійних ситуацій.

Для підсистеми безпеки критично важливим є вбудований 12-бітний аналогово-цифровий перетворювач (АЦП), який підтримує понад 15 каналів зчитування. Це дозволяє підключати всю лінійку напівпровідникових газових датчиків одночасно з високою точністю, що неможливо для простіших платформ на кшталт Arduino чи ESP8266 через обмежену кількість або низьку розрядність їхніх входів. Крім того, ESP32 підтримує цифрові інтерфейси, необхідні для роботи

з прецизійними термометрами DS18B20 через протокол 1-Wire, що робить його універсальним вузлом для збору різнопланових параметрів середовища.

Інтегровані модулі Wi-Fi та Bluetooth роблять ESP32 автономним комунікаційним мостом, який не потребує додаткових дорогих шлюзів для виходу в інтернет. Використання цього контролера дозволяє реалізувати передачу даних за протоколом MQTT, забезпечуючи надійне сповіщення користувача про витоки газу чи води безпосередньо на смартфон через мобільний застосунок. При високій потужності та широкому функціоналі ESP32 залишається доступним за ціною, що повністю відповідає концепції створення бюджетних, але високоефективних систем безпеки для широкого вжитку.

Для комплексної підсистеми кіберфізичної системи «Розумний будинок», яка базується на контролері ESP32 та групі датчиків безпеки, вибір стандарту передачі даних є критичним. Система має бути надійною, працювати в реальному часі та легко інтегруватися з мобільними пристроями. У Таблиці 2.7 представлені результати порівняльного аналізу основних стандартів передачі даних.

Таблиця 2.7 – Порівняльний аналіз стандартів передачі даних

Стандарт	Радіус дії	Енерго-споживання	Пропускна здатність	Переваги	Недоліки
Wi-Fi (IEEE 802.11)	Середній (30-50 м)	Високе	Дуже висока	Пряме підключення до роутера та інтернету, не потрібен хаб	Залежність від стабільності роутера, енерго-залежність
Zigbee / Z-Wave	Середній (10-100 м)	Дуже низьке	Низька	Стійка mesh-мережа, ідеально для	Потребує спеціальний шлюз (Gateway),

Кінець таблиці 2.7

				датчиків на батарейках	вища ціна модулів
Bluetooth LE (BLE)	Малий (10-20 м)	Низьке	Середня	Економний, прямий зв'язок зі смартфоном	Обмежений радіус дії, складно керувати віддалено без шлюзу
LoRaWAN	Великий (до 5-15 км)	Дуже низьке	Дуже низька	Величезна дальність, робота в підвалах/ бетонних спорудах	Повільна передача даних, складна інфраструк-тура

Для розроблюваної підсистеми оптимальним рішенням є використання протоколу MQTT (Message Queuing Telemetry Transport), що працює поверх Wi-Fi. Оскільки обраний контролер ESP32 вже має вбудований Wi-Fi модуль, це дозволяє реалізувати систему без додаткових витрат на шлюзи (як у випадку з Zigbee). Це повністю відповідає вимозі щодо бюджетності рішення. Wi-Fi забезпечує достатню швидкість для передачі великої кількості даних від багатьох датчиків одночасно. Протокол MQTT – це «золотий стандарт» для IoT-систем завдяки своїм особливостям: легкість (протокол мінімізує обсяг переданих даних, що важливо для швидкої реакції системи), надійність (MQTT має рівні якості обслуговування (QoS – Quality of Service); наприклад, для датчика газу можна встановити рівень «QoS 1», який гарантує, що повідомлення про аварію точно дійде до користувача), модель «Видавець-Підписник» (датчики публікують дані в певні «топіки» (наприклад, home/safety/gas), а смартфон або сервер негайно отримує їх), затримка

передачі даних складає мілісекунди, що критично для запобігання пожежам чи вибухам.

Швидкість передачі даних є критичним параметром для систем реального часу, де затримка може вимірюватися мілісекундами. Використання протоколу MQTT поверх Wi-Fi забезпечує мінімальний мережевий трафік та швидку доставку інформації про стан об'єкта. Параметр якості обслуговування QoS 1 гарантує, що кожне повідомлення про зміну аварійних показників буде доставлене брокеру принаймні один раз.

Ситуаційний аналіз на верхньому рівні архітектури дозволяє об’єднувати розрізнені параметри в єдині сценарії реальності. Система перестає бути набором окремих датчиків і перетворюється на когнітивного агента, який розуміє контекст подій. Наприклад, одночасне зростання концентрації CO та температури може свідчити про несправність опалювального приладу, що потребує негайного знеструмлення.

Економічний параметр розробки є вирішальним для масового впровадження системи. Використання доступних напівпровідникових та цифрових компонентів робить підсистему в кілька разів дешевшою за промислові аналоги. Це дозволяє забезпечити комплексний захист навіть для бюджетних домогосподарств, де раніше автоматизація безпеки була недоступною.

Важливим параметром функціонування є автономність системи, що реалізується через технології граничних обчислень. ESP32 здатна приймати базові рішення про перекриття клапанів навіть за умови втрати зв’язку з хмарним сервісом чи зовнішньою мережею. Це гарантує безперервність захисту в екстремальних умовах, коли зовнішня інфраструктура може бути пошкоджена.

На основі проведеного аналізу можна зробити висновок, що сформований перелік апаратних засобів є оптимальним для створення комплексної, бюджетної та високоефективної підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Обрана конфігурація дозволяє подолати головні недоліки існуючих рішень – їхню високу вартість та вузьку спеціалізацію. Використання лінійки датчиків MQ-7, MQ-4 та MQ-2 у поєднанні з

DS18B20 та YI-S WL400 Water Level Sensor дозволяє системі одночасно контролювати п'ять критичних загроз – чадний газ, природний газ, задимлення, аномально висока температура та витоки води. Це перетворює підсистему з простого детектора на повноцінний когнітивний вузол безпеки. Комбінація датчика диму MQ-2 та прецизійного термометра DS18B20 реалізує принцип перехресної перевірки. Це мінімізує кількість хибних спрацювань, що є ключовим показником надійності для кіберфізичних систем. Вибір ESP32 як обчислювального центру є найбільш виправданим. Завдяки вбудованому 12-бітному АЦП для точного зчитування аналогових сигналів газу та інтегрованому Wi-Fi модулю, контролер забезпечує високу швидкість обробки даних та миттєву передачу тривожних сигналів без потреби в дорогому додатковому обладнанні. Використання стандарту Wi-Fi у поєднанні з протоколом MQTT гарантує низьку затримку (low latency) та високу надійність доставки повідомлень (QoS). Це критично для систем реального часу, де кожна секунда зволікання при аварії може мати серйозні наслідки.

Застосування напівпровідникових та резистивних сенсорів у поєднанні з доступним контролером ESP32 робить підсистему в кілька разів дешевшою за промислові аналоги, зберігаючи при цьому необхідний рівень точності для побутового використання.

Отже, запропонований апаратний стек створює надійний фундамент для підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок», яка здатна адаптуватися до мінливих умов середовища, забезпечувати автономний захист житла та надавати користувачу повний контроль над безпекою через сучасні цифрові канали зв'язку.

2.3 Висновки

У другому розділі проведено ґрунтовний порівняльний аналіз та обґрунтовано вибір сенсорного обладнання, що дозволяє системі одночасно контролювати п'ять критичних загроз: чадний газ (MQ-7), природний газ (MQ-4), задимлення (MQ-2), витоки води (YI-S WL400 Water Level Sensor) та аномальні

температури (DS18B20). Обрана лінійка напівпровідникових та цифрових датчиків забезпечує оптимальний баланс між прецизійною точністю вимірювань та економічною доступністю, що є ключовим для подолання високої вартості існуючих комерційних рішень. Особливо важливою є реалізація принципу перехресної верифікації подій, де, наприклад, температурний сенсор виступає підтверджуючим фактором для детектора диму, що радикально знижує ймовірність хибних спрацювань.

Центральним елементом архітектури визначено контролер ESP32, який завдяки двоядерному процесору та вбудованому 12-бітному АЦП забезпечує високу швидкість обробки аналогових сигналів та надійне шифрування даних у реальному часі. Вибір стандарту Wi-Fi у поєднанні з протоколом MQTT та рівнем якості обслуговування QoS 1 («At least once») гарантує гарантовану доставку критичних повідомлень про аварії на кінцевий пристрій користувача з мінімальними затримками. Це дозволяє інтегрувати підсистему в єдину мережу будинку без потреби у використанні додаткових дорогих шлюзів, підтримуючи концепцію бюджетності.

Проєктована архітектура має чітку трирівневу структуру: від нижнього рівня безпосереднього зчитування параметрів середовища до середнього рівня первинної обробки на базі ESP32 та верхнього аналітичного рівня, де розміщено модуль ситуаційного аналізу. Такий підхід трансформує підсистему з простого набору датчиків у когнітивний вузол безпеки, здатний до автономного прийняття рішень, таких як автоматичне перекриття подачі води чи газу. Впровадження технологій граничних обчислень забезпечує живучість системи та її здатність функціонувати навіть за відсутності стабільного інтернет-з’єднання.

3 МЕТОД ТА АЛГОРИТМ ФУНКЦІОНУВАННЯ ПІДСИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АВАРІЙНИМ СИТУАЦІЯМ В КІБЕРФІЗИЧНІЙ СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

3.1 Метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

На основі розробленої архітектури та обраного апаратного стека (ESP32, сенсори серії MQ, DS18B20 та YI-S WL400 Water Level Sensor), підсистема реалізуватиме низку сценаріїв, що базуються на ситуаційному аналізі та перехресній верифікації даних.

Множина основних сценаріїв роботи підсистеми має вигляд:

$$SDPE = \{ sdpe_1, .., sdpe_8 \} = \{ ngld, rcmp, cmlrt, nglrt, srt, wld, ao, lc \},$$

де *ngld* – виявлення витоку природного газу (датчик MQ-4 фіксує концентрацію метану (CH_4) вище заданого безпечного порогу (> 1000 ppm)), *rcmp* – загроза отруєння чадним газом (датчик MQ-7 детектує підвищення рівня чадного газу, що часто трапляється при несправності пічного опалення або камінів), *cmlrt* – виток чадного газу та збільшення температури (датчик MQ-7 детектує підвищення рівня чадного газу та дачтик DS18B20 детектує аномальне підвищення температури, що свідчить про критичну несправність опалювального приладу), *hglrt* – виток природного газу та збільшення температури (датчик MQ-4 детектує підвищення рівня природного газу та дачтик DS18B20 детектує аномальне підвищення температури, що свідчить про критичну несправність опалювального приладу), *srt* – поява диму та збільшення температури (верифікація пожежі) (датчик MQ-2 фіксує задимлення та датчик DS18B20 одночасно реєструє стрімке зростання температури понад 60°C або датчик MQ-2 фіксує задимлення та датчик DS18B20 одночасно реєструє стрімке зростання температури +5ºC на хвилину), *wld* – виявлення витоку води (загроза затоплення) (зондовий датчик YI-S WL400 Water Level Sensor фіксує стабільний контакт із водою протягом більше ніж 1–2 секунд (захист від випадкових бризок)), *ao* – аномальний перегрів (загроза пожежі) (датчик DS18B20 фіксує перевищення температурного порогу без ознак диму (наприклад,

перегрів електрощитової)), *lc* – втрата зв'язку (edge computing) (відсутність підключення до Wi-Fi або хмарного брокера MQTT).

Множина відповідних сценаріїв реагування підсистеми має вигляд:

$$CRS = \{ crs_1,..,crs_{15} \} = \{ iscap, lava, somgv, aowv, isha, iscaf, ses, deab, aafs, iscaft, acsvw, nufh, apco, sadmm, mlfpa \},$$

де *iscap* – негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Небезпека отруєння», *lava* – активація локальної звукової та світлової сигналізації, *somgv* – автоматичне подання сигналу на сервопривід для перекриття магістрального газового крана, *aowv* – автоматичне відкриття віконних приводів або заслінок припливної вентиляції для провітрювання, *isha* – негайне вимкнення опалювального приладу, *iscaf* – негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Пожежа», *ses* – надсилання сигналу екстреним службам (через хмарні сервіси або Telegram-бот), *deab* – знеструмлення відповідної зони будинку для запобігання коротким замиканням, *aafs* – активація автоматичної системи пожежогасіння (спринклерів) у зоні займання, *iscaft* – негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Загроза затоплення», *acsvw* – автоматичне закриття електромагнітного клапана на вході водопроводу до приміщення, *hufh* – сповіщення користувача про загрозу пожежі, *apco* – автоматичне знеструмлення перегрітої ділянки ланцюга для запобігання займанню, *sadmm* – перехід контролера ESP32 в автономний режим прийняття рішень (обробка логіки безпосередньо на пристрої), *mlfpa* – збереження локальної працездатності фізичних актуаторів (перекриття кранів при спрацюванні датчиків незалежно від наявності Інтернету).

Всі сценарії базуються на ієрархічній моделі, де локальний рівень (ESP32) відповідає за збір даних, а верхній рівень (база знань) – за фінальний аналіз та вибір оптимальної дії.

Тоді метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» базується на багаторівневій структурі, що забезпечує

перехід від фізичного сприйняття середовища до інтелектуального прийняття рішень, і складається з таких етапів:

1) етап первинного сенсорного моніторингу – безпосереднє зчитування параметрів навколишнього середовища за допомогою обраних датчиків. Фізичні компоненти (датчики диму, газу, температури та витоку води) збирають первинну інформацію, яка є фундаментом для всього подальшого аналізу. Частота виконання етапу первинного сенсорного моніторингу є критичним параметром, оскільки від неї залежить швидкість реакції всієї кіберфізичної системи на загрозу. Опитування датчиків має відбуватися в режимі реального часу з високою інтенсивністю. Зчитування параметрів навколишнього середовища обраними датчиками (MQ-7, MQ-4, MQ-2, DS18B20, YI-S WL400 Water Level Sensor) має виконуватися постійно та безперервно для того, щоб система виступала активним суб'єктом прийняття рішень і не пропустила момент зародження аварійної ситуації. Таким чином, перший етап виконується циклічно з частотою кілька разів на секунду, що забезпечує миттєву ідентифікацію аномалій ще на стадії їх зародження;

2) етап збору та попередньої обробки даних – зібрані дані передаються на середній рівень, де центральним елементом виступає контролер ESP32. Контролер виконує роль мосту та первинного процесора: він отримує сигнали від датчиків, проводить їх фільтрацію та готує до передачі;

3) етап комунікаційної передачі – після первинної обробки контролер використовує мережеві протоколи (Wi-Fi та MQTT) для ефективної передачі даних на верхній аналітичний рівень. Це забезпечує мінімальний мережевий трафік та надійну інтеграцію пристроїв у єдину мережу будинку. Для критично важливих повідомлень встановлюється рівень якості QoS 1, що гарантує доставку інформації;

4) етап ситуаційного аналізу та прийняття рішень – на цьому етапі розміщується аналітичне ядро підсистеми. Тут відбувається фінальний аналіз отриманих комплексних даних та застосовуються методи для розпізнавання поточних ситуацій. Система визначає оптимальні дії відповідно до заздалегідь заданих правил, що містяться в базі знань. Важливою особливістю є перехресна

верифікація (наприклад, підтвердження пожежі одночасно за димом та температурою) для мінімізації хибних спрацювань;

5) етап автоматичного реагування та запобігання – виконання необхідних дій в автоматичному режимі, спрямованих на нейтралізацію загрози:

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_1 = ngld$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$;

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_2 = rcmp$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$;

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_3 = cmlrt$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$;

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_4 = nglrt$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$;

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_5 = srt$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_6 = iscaf$, $crs_7 = ses$, $crs_8 = deab$, $crs_9 = aafs$, $crs_2 = lava$;

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_6 = wld$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_{10} = iscaft$, $crs_{11} = acsvw$, $crs_2 = lava$;

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_7 = ao$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_{12} = nufh$, $crs_{13} = apco$;

– якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_8 = lc$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_{14} = sadmm$, $crs_{15} = mlfpa$;

6) етап адаптації та зворотного зв'язку – завдяки здатності до самонавчання, система накопичує дані про зовнішні впливи та звички користувачів. Це дозволяє постійно вдосконалювати алгоритми реагування, роблячи «Розумний будинок» більш стійким до збоїв та здатним розпізнавати найменші відхилення від норми.

Розроблений метод виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» базується на багаторівневій структурі, що забезпечує логічний перехід від фізичного сприйняття середовища до інтелектуального прийняття рішень. Його архітектура охоплює шість послідовних етапів, починаючи від безпосереднього зчитування параметрів обраними датчиками й завершуючи етапом адаптації та зворотного зв'язку. Така системність дозволяє перетворити звичайний набір сенсорів на когнітивну екосистему, здатну не лише реагувати на загрози, а й аналізувати контекст їх виникнення.

Ключовою перевагою методу є етап первинного сенсорного моніторингу, який виконується циклічно з частотою кілька разів на секунду. Постійне та безперервне зчитування параметрів чадного газу, метану, диму, температури та

витоків води гарантує миттєву ідентифікацію аномалій ще на стадії їх зародження. Це дозволяє системі виступати активним суб’єктом захисту, випереджаючи швидкість фізичних процесів під час аварії, яка часто перевищує реакцію людини.

Важливою особливістю розробки є етап ситуаційного аналізу та прийняття рішень, де реалізовано принцип перехресної верифікації. Наприклад, підтвердження пожежі відбувається одночасно за показниками диму та температури, що радикально мінімізує кількість хибних спрацювань. Такий синергетичний ефект підвищує достовірність виявлення небезпек і забезпечує надійність системи в умовах реального житлового простору.

Комунікаційний етап методу використовує мережеві протоколи Wi-Fi та MQTT, що забезпечує мінімальний трафік та надійну інтеграцію пристроїв. Встановлення рівня якості обслуговування QoS 1 для критичних повідомлень гарантує обов'язкову доставку інформації користувачу. Це робить систему стійкою до мережевих збоїв і дозволяє мешканцям отримувати миттєві сповіщення через мобільні додатки в будь-якій точці світу.

Етап автоматичного реагування передбачає виконання заздалегідь визначених сценаріїв для нейтралізації конкретних загроз. Метод дозволяє системі самостійно здійснювати такі дії, як перекриття подачі води чи газу, активацію звукової сигналізації та сповіщення екстрених служб. Така автономність є критично важливою для вразливих верств населення, зокрема літніх людей, які не завжди можуть вчасно зреагувати на небезпеку.

Значною перевагою методу є його економічна доступність, оскільки він орієнтований на використання недорогих датчиків серії MQ та контролера ESP32. Це дозволяє подолати головний бар’єр – високу вартість інтелектуальних систем безпеки – і зробити повну автоматизацію захисту доступною для пересічного споживача. Таким чином, інвестиції в дану систему є стратегічно виправданими для будь-якого домогосподарства.

До недоліків методу можна віднести залежність від стабільності електроживлення та Wi-Fi з’єднання на етапі комунікаційної передачі. Хоча протокол MQTT та рівень QoS 1 підвищують надійність, повна відсутність мережі

може обмежити можливості віддаленого моніторингу та сповіщення. Також напівпровідникові датчики потребують періодичного калібрування через схильність до деградації чутливого шару з часом.

Можливості використання даного методу охоплюють не лише приватні будинки, а й багатоквартирні житлові комплекси, де ризики техногенних аварій є особливо високими. Метод може бути масштабований для моніторингу промислових приміщень або об'єктів критичної інфраструктури, де необхідний прецизійний контроль концентрації газів та температурних режимів. Його онтологічна відкритість дозволяє легко інтегрувати нові типи датчиків без перебудови базової архітектури.

Перспективи розвитку методу пов'язані з етапом адаптації та зворотного зв'язку, що базується на здатності до самонавчання. Система може накопичувати дані про звички користувачів та зовнішні впливи, постійно вдосконалюючи алгоритми розпізнавання відхилень від норми. Це відкриває шлях до впровадження предиктивної аналітики, яка зможе прогнозувати аварію ще до моменту її фактичного виникнення.

Додатковим вектором розвитку є впровадження технологій туманних обчислень (fog computing) для забезпечення низької затримки при передачі екстрених даних. Це дозволить системі зберігати повну функціональність навіть при тимчасових збоях хмарних сервісів. Також актуальним є інтеграція з технологією блокчейн для забезпечення цілісності команд керування та захисту від несанкціонованого втручання.

Розроблений метод перетворює помешкання на надійний інтелектуальний щит, здатний до самостійної діагностики. Це забезпечує мешканцям новий рівень комфорту та безпеки, позбавляючи їх потреби в постійному ручному контролі побутових приладів. Соціальна значущість методу полягає у створенні захищеного середовища, що компенсує зниження сенсорного сприйняття у людей похилого віку.

На завершення, інтеграція параметрів моніторингу газу, диму, води та температури в єдину кіберфізичну структуру за даним методом створює якісно

новий рівень захисту. Комплексний аналіз показників дозволяє системі ефективно протидіяти техногенним викликам сучасності, зберігаючи матеріальні активи та людські життя. Дана розробка є пріоритетним кроком у розвитку інтелектуальних систем життєзабезпечення майбутнього.

3.2 Алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

Алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» базується на циклічному використанні шести послідовних етапів, що забезпечують перехід від збору фізичних даних до виконання автономних захисних дій. Логіка роботи побудована таким чином, щоб мінімізувати час реакції та гарантувати достовірність виявлення загроз.

Алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»:

Етап 1. Циклічне зчитування параметрів.

Система безперервно з високою інтенсивністю (кілька разів на секунду) опитує датчики MQ-7, MQ-4, MQ-2, DS18B20 та YI-S WL400 Water Level Sensor для фіксації найменших відхилень від норми.

Етап 2. Первинна обробка на ESP32.

Отримані сигнали передаються на контролер, який виконує роль мосту, проводить фільтрацію шумів та готує дані для мережевого обміну.

Етап 3. Мережева передача даних.

Контролер використовує Wi-Fi та протокол MQTT для передачі інформації на верхній рівень, застосовуючи рівень якості QoS 1 для гарантованої доставки критичних сповіщень.

Етап 4. Ситуаційний аналіз та верифікація.

Аналітичне ядро порівнює отримані дані із заздалегідь заданими правилами бази знань і проводить перехресну перевірку (наприклад, зіставлення диму та температури) для відсікання хибних тривог.

Етап 5. Виконання сценаріїв реагування.

У разі ідентифікації аварії система автоматично активує відповідні заходи: перекриття клапанів, знеструмлення ділянок, увімкнення сирени та сповіщення користувача.

Етап 6. Адаптація та самонавчання.

Система накопичує дані про звички користувачів та зовнішні впливи, що дозволяє вдосконалювати алгоритми та розпізнавати аномалії в умовах високої невизначеності.

Цей алгоритм забезпечує автономність будинку, оскільки завдяки технологіям граничних обчислень основні захисні дії можуть виконуватися контролером ESP32 навіть за умови тимчасової відсутності зв'язку з хмарним сервісом.

Алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям базується на суворій ієрархічній структурі, що забезпечує безперервний цикл від збору фізичних даних до виконання автономних захисних дій. Його головна перевага полягає у високій інтенсивності опитування датчиків, що відбувається в режимі реального часу кілька разів на секунду. Це дозволяє системі ідентифікувати аномалії, такі як витоки газів або задимлення, ще на стадії їх зародження, випереджаючи швидкість поширення фізичної загрози.

Важливою аналітичною перевагою алгоритму є впровадження перехресної верифікації параметрів на етапі прийняття рішень. Завдяки зіставленню даних від різних сенсорів, наприклад, підтвердженню задимлення аномальним зростанням температури, система радикально знижує ймовірність хибних спрацювань. Такий підхід робить «Розумний будинок» надійним когнітивним агентом, який розуміє контекст подій і не реагує на випадкові одиничні сплески показників.

Використання протоколу MQTT з рівнем якості QoS 1 у структурі алгоритму забезпечує гарантовану доставку критичних сповіщень користувачу. Це означає, що навіть у разі нестабільного мережевого з'єднання інформація про витік газу або води буде доставлена брокеру принаймні один раз. Така мережева стійкість є критично важливою для систем безпеки, де затримка або втрата пакету даних може призвести до катастрофічних наслідків.

Алгоритм надає можливість повної автономізації захисних функцій через автоматичне виконання сценаріїв реагування. Система не просто інформує власника, а самостійно активує виконавчі механізми: перекриває електромагнітні клапани подачі газу та води, знеструмлює небезпечні ділянки електромережі та вмикає вентиляцію. Це перетворює помешкання на «інтелектуальний щит», здатний захистити майно та життя навіть за відсутності людини.

З точки зору можливостей використання, цей алгоритм є універсальним фундаментом для побудови безпечного середовища в приватних будинках і квартирах. Завдяки орієнтації на доступну апаратну базу, таку як контролер ESP32 та датчики серії MQ, алгоритм дозволяє створювати високоефективні рішення з низькою вартістю впровадження. Це відкриває шлях до масової автоматизації безпеки, яка раніше була доступна лише в дорогому преміальному сегменті.

Для вразливих верств населення, зокрема літніх людей, алгоритм виконує соціально значущу функцію компенсації сенсорного сприйняття. Оскільки люди похилого віку можуть не відчути запах газу або не помітити воду на підлозі, автоматизована діагностика середовища бере на себе функцію постійного нагляду. Це забезпечує їм вищий рівень незалежності та безпеки проживання без потреби в постійній присутності сторонніх осіб.

Основним недоліком алгоритму на поточному етапі є його залежність від стабільності живлення та наявності Wi-Fi для віддаленого сповіщення. Хоча локальне реагування може відбуватися автономно на рівні контролера, повноцінний вихід у хмарне середовище потребує безперебійної роботи мережевої інфраструктури. Також алгоритм вимагає періодичної перевірки точності датчиків,

оскільки напівпровідникові сенсори схильні до поступової деградації під впливом зовнішніх чинників.

Перспективи розвитку алгоритму лежать у площині етапу адаптації та самонавчання. Накопичення історичних даних про стан середовища дозволяє системі виявляти аномалії навіть у межах формально нормальних значень, аналізуючи звичні патерни використання енергоносіїв. Це підвищує інтелектуальність захисту, роблячи його персоналізованим і здатним прогнозувати аварії ще до появи явних фізичних ознак.

Впровадження технологій граничних та туманних обчислень (Fog Computing) дозволить алгоритму ще ефективніше розподіляти навантаження та мінімізувати затримки. Це забезпечить миттєву обробку критичних сигналів безпосередньо на місці виникнення, що особливо важливо для запобігання вибухам газу чи стрімкому поширенню вогню. Така архітектурна гнучкість дозволяє системі еволюціонувати без заміни базового обладнання.

Ще одним вектором розвитку є розширення онтологічної відкритості методу для додавання нових типів датчиків, наприклад, акустичних для детектування розбиття скла або вібраційних для аналізу цілісності конструкцій. Це дозволить алгоритму охоплювати нові домени безпеки, включаючи захист від несанкціонованого проникнення. У результаті «Розумний будинок» трансформується у повноцінну когнітивну екосистему.

Економічна виправданість алгоритму підтверджується тим, що витрати на його розробку та впровадження є значно нижчими за потенційні збитки від пожежі чи затоплення. Збереження матеріальних активів і, найголовніше, людських життів робить цей алгоритм стратегічно необхідним елементом сучасного житлового простору. Це створює надійний фундамент для побудови безпечного міста та інтелектуальних систем майбутнього.

Підсумовуючи, розроблений алгоритм пропонує комплексний і надійний підхід до вирішення проблем побутової безпеки. Він долає фрагментарність існуючих рішень, об’єднуючи моніторинг різних типів загроз у єдиний функціональний цикл. Завдяки поєднанню швидкості реакції, інтелектуального

аналізу та автономності, цей алгоритм виводить концепцію «Розумного будинку» на якісно новий рівень стійкості до техногенних викликів.

3.3 Висновки

Розроблений у розділі метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» базується на багаторівневій структурі, яка забезпечує логічний перехід від фізичного збору даних за допомогою сенсорів до інтелектуального прийняття рішень та автономного реагування. Така системність перетворює звичайний набір датчиків на когнітивну екосистему, здатну аналізувати не лише факт загрози, а й контекст її виникнення.

Ключовою перевагою методу виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» є етап первинного моніторингу, що виконується в режимі реального часу з високою інтенсивністю (кілька разів на секунду). Це дозволяє ідентифікувати аномалії, такі як витоки газів або задимлення, ще на стадії їх зародження, випереджаючи швидкість поширення фізичної небезпеки.

Встановлено, що використання принципу перехресної верифікації параметрів радикально підвищує точність системи. Наприклад, підтвердження пожежі одночасно за показниками диму та температури дозволяє мінімізувати кількість хибних спрацювань від побутових чинників, таких як кухонна пара або пил.

Обґрунтовано вибір комунікаційного стека на основі Wi-Fi та протоколу MQTT із рівнем якості QoS 1. Це забезпечує мінімальний мережевий трафік та гарантовану доставку критичних сповіщень про аварії на смартфон користувача, що є життєво необхідним для систем екстреного реагування.

У розділі розроблено також алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», який забезпечує високий рівень автономності будинку. Завдяки технологіям граничних обчислень на базі ESP32, основні захисні дії (перекриття клапанів,

знеструмлення ділянок) можуть виконуватися локально навіть за умови тимчасової втрати зв'язку з хмарними сервісами.

Розроблена множина сценаріїв реагування охоплює всі критичні типи аварій: витоки природного та чадного газів, пожежі, затоплення та аномальні перегріви обладнання. Для кожного випадку визначено чіткі заходи – від автоматичного провітрювання до негайного вимкнення потенційно небезпечних опалювальних приладів.

Підкреслено соціальну значущість розробки для вразливих верств населення, зокрема літніх людей. Автоматизована діагностика середовища компенсує зниження їхнього сенсорного сприйняття, забезпечуючи безпечне та незалежне проживання без потреби в постійному сторонньому нагляді.

Аналіз економічного аспекту засвідчив перевагу методу за рахунок орієнтації на доступну апаратну базу (датчики серії MQ та контролер ESP32). Це дозволяє реалізувати багатофункціональну систему безпеки з низькою вартістю впровадження, що робить її доступною для масового споживача.

Визначено перспективи розвитку системи, що лежать у площині адаптації та самонавчання. Накопичення історичних даних дозволить у майбутньому реалізувати предиктивну аналітику, здатну прогнозувати аварії на основі аналізу звичних патернів використання енергоносіїв.

Інтеграція всіх параметрів моніторингу в єдиний функціональний цикл створює якісно новий рівень стійкості оселі до техногенних викликів. Розроблений алгоритм долає фрагментарність існуючих рішень і є надійним фундаментом для побудови інтелектуальних систем життєзабезпечення майбутнього.

4 ПІДСИСТЕМА ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АВАРІЙНИМ СИТУАЦІЯМ В КІБЕРФІЗИЧНІЙ СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

4.1 Підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

Отже, основні елементи підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»:

1) датчик чадного газу MQ-7;
2) датчик природного газу MQ-4;
3) датчик диму MQ-2;
4) датчик витоку води YI-S WL400 Water Level Sensor;
5) датчик аномально високих температур DS18B20;
6) контролер ESP32;
7) стандарт передачі даних – протокол MQTT, що працює поверх Wi-Fi.

Архітектура підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» складається з локального рівня – контролер ESP32 збирає дані з датчиків MQ-7, MQ-4, MQ-2, DS18B20 та YI-S WL400 Water Level Sensor, протоколу передачі – MQTT-клієнт на ESP32, хмарного/локального брокера – Mosquitto або безкоштовні хмарні сервіси (Adafruit IO, HiveMQ), кінцевий пристрій – смартфон із мобільним застосунком.

На нижньому рівні відбувається безпосереднє зчитування параметрів навколишнього середовища обраними датчиками. Ці фізичні компоненти збирають первинну інформацію, яка є основою для подальшого аналізу.

Зібрані дані передаються на середній рівень, центральним елементом якого є контролер ESP32. Контролер виконує роль мосту та первинного процесора – він отримує дані від датчиків. Після первинної обробки та перевірки, контролер використовує Wi-Fi-зв'язок та протокол MQTT для ефективної передачі даних на верхній рівень, що забезпечує мінімальний мережевий трафік та надійну інтеграцію у мережу будинку. Для всіх критично важливих повідомлень, що стосуються

імплементації рішень, було встановлено рівень якості обслуговування QoS 1 (At least once).

На верхньому рівні розміщуються методи прийняття рішень та керування, які є аналітичним ядром та модулем ситуаційного аналізу підсистеми. Тут відбувається фінальний аналіз отриманих комплексних даних – застосовуються методи для розпізнавання поточних ситуацій та для визначення оптимальних дій відповідно до заздалегідь заданих правил, що містяться в розділі правил бази знань. Завершальним етапом роботи підсистеми є виконання необхідних дій в автоматичному режимі, спрямованих на попередження та запобігання аварійним ситуаціям. Це включає сповіщення користувача, перекривання подачі води/газу, сповіщення екстрених рятувальних служб тощо.

Спроєктуємо архітектуру підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» – рис. 4.1.

Розроблена підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» забезпечує високий рівень безпеки завдяки комплексній інтеграції різнопланових сенсорів та алгоритмів обробки даних у реальному часі. Головними перевагами такої архітектури є її багатофункціональність, що дозволяє одночасно контролювати витоки газів, води та виникнення пожеж, а також економічна доступність за рахунок використання контролера ESP32 та недорогих напівпровідникових датчиків. Використання протоколу MQTT з рівнем якості QoS 1 гарантує надійність доставки критичних повідомлень, а багаторівнева структура прийняття рішень мінімізує вплив людського фактора та забезпечує оперативне автоматичне реагування на загрози. Разом з тим, система має певні обмеження, пов'язані із залежністю від стабільності Wi-Fi-з’єднання та необхідністю регулярного калібрування напівпровідникових сенсорів серії MQ, які схильні до деградації з часом і чутливі до змін вологості повітря. Проте, завдяки впровадженню методів ситуаційного аналізу та перехресної верифікації даних, підсистема трансформує житловий простір у когнітивне середовище, здатне ефективно запобігати техногенним аваріям та забезпечувати надійний захист майна і життя мешканців.

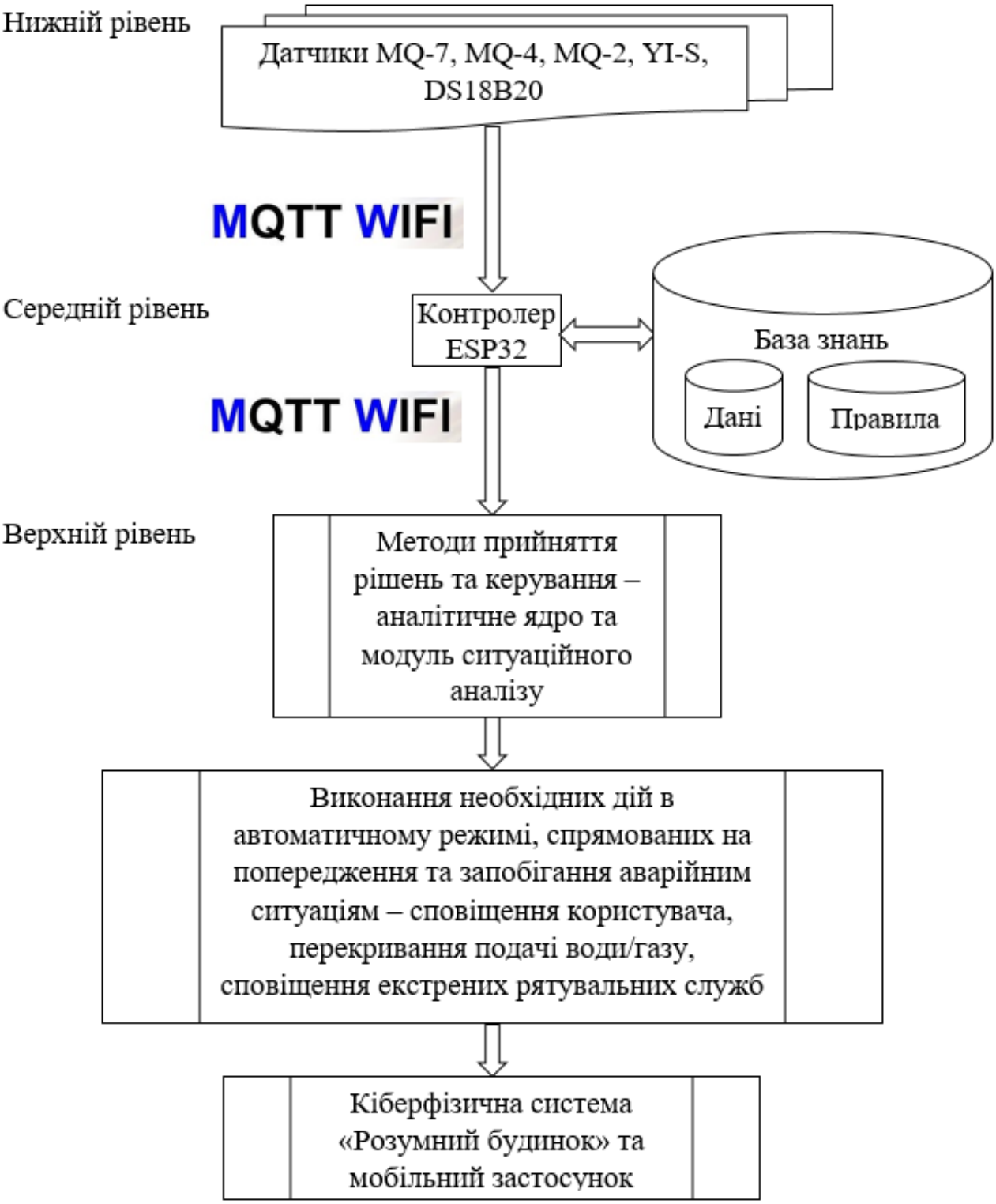


Рисунок 4.1 – Архітектура підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»

Розроблена підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» представляє собою цілісну інженерну

екосистему, яка базується на інтеграції доступних, але високопродуктивних апаратних засобів та інтелектуальних алгоритмів обробки даних. Її архітектура побудована за ієрархічним принципом, що включає три функціональні рівні: нижній (сенсорний), середній (процесорний) та верхній (аналітичний), що дозволяє системі еволюціонувати від простого збору інформації до автономного прийняття рішень.

Фундаментом системи є набір спеціалізованих сенсорів, що охоплюють моніторинг п'яти ключових типів загроз: чадного газу (MQ-7), природного газу (MQ-4), диму (MQ-2), витоків води (YI-S WL400 Water Level Sensor) та аномальних температур (DS18B20). Таке поєднання датчиків дозволяє контролювати практично всі основні техногенні ризики, властиві сучасному житлу, в єдиному функціональному контурі.

Головною перевагою підсистеми є її здатність до ситуаційного аналізу та перехресної верифікації даних. Наприклад, ідентифікація пожежі відбувається лише за умови одночасного підтвердження від датчика диму та сенсора температури, що радикально знижує ймовірність хибних спрацювань від кухонних парів чи пилу. Це робить систему надійним когнітивним агентом, який "розуміє" контекст подій у реальному часі.

Використання контролера ESP32 як центрального вузла середнього рівня забезпечує високу швидкість обробки аналогових і цифрових сигналів. Завдяки потужному процесору контролер виконує роль первинного фільтра та мосту, готуючи дані для передачі на верхній рівень, що гарантує оперативну реакцію на загрози, яка вимірюється мілісекундами.

Комунікаційна складова підсистеми базується на протоколі MQTT, що працює поверх Wi-Fi, забезпечуючи мінімальний мережевий трафік та високу надійність. Впровадження рівня якості обслуговування QoS 1 (At least once) гарантує, що жодне критичне повідомлення про аварію не буде втрачено в мережі, забезпечуючи обов'язкову доставку інформації до користувача.

Підсистема забезпечує повну автономність через виконання автоматичних сценаріїв реагування. Вона здатна самостійно перекривати магістральні клапани

подачі газу та води, знеструмлювати небезпечні зони будинку та активувати системи пожежогасіння. Це перетворює помешкання на «інтелектуальний щит», який бере на себе функцію постійної діагностики оселі, що особливо важливо для літніх людей та осіб з інвалідністю.

Економічна доступність є ще одним вагомим аргументом на користь даної розробки. Використання недорогих напівпровідникових датчиків серії MQ та масового контролера ESP32 дозволяє створити високоефективну систему за ціною, значно нижчою за промислові чи комерційні аналоги, роблячи безпеку доступною для широкого загалу.

Незважаючи на численні переваги, підсистема має певні обмеження, як-от залежність від стабільності Wi-Fi та електроживлення для віддаленого сповіщення. Крім того, напівпровідникові датчики схильні до поступової деградації та чутливі до змін вологості, що зумовлює необхідність їх періодичного калібрування для підтримки точності вимірювань.

Можливості використання підсистеми виходять далеко за межі приватних будинків; вона може бути успішно масштабована для багатоквартирних комплексів, готелів або офісних приміщень. Онтологічна відкритість архітектури дозволяє легко інтегрувати нові типи датчиків або розширювати перелік сценаріїв реагування відповідно до специфічних потреб об'єкта.

Перспективи розвитку системи лежать у площині впровадження предиктивної аналітики на основі машинного навчання. Накопичення історичних даних дозволить системі розпізнавати аномалії на ранніх стадіях ще до досягнення критичних порогів, аналізуючи звичні патерни використання ресурсів мешканцями.

Впровадження технологій граничних (edge computing) та туманних обчислень (fog computing) дозволить ще більше знизити затримки передачі екстрених даних та забезпечити повну працездатність актуаторів навіть за відсутності доступу до хмарних сервісів. Це зробить систему ще більш відмовостійкою та надійною в критичних умовах.

У підсумку, розроблена підсистема трансформує житловий простір у когнітивне середовище, здатне ефективно протистояти техногенним та побутовим викликам. Вона забезпечує якісно новий рівень захисту життя та майна, що є пріоритетним кроком у розвитку концепції «розумного міста» та інтелектуальних систем життєзабезпечення майбутнього.

4.2 Приклади функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»

Розглянемо приклади функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» на конкретних сценаріях, що базуються на синергії датчиків та інтелектуальних алгоритмів реагування.

Розглянемо приклад1 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – безпосереднє зчитування параметрів навколишнього середовища за допомогою обраних датчиків (датчики диму, газу природного та чадного, аномальної температури та витоку води) – виконується циклічно з частотою кілька разів на секунду. Етап збору та попередньої обробки даних – зібрані дані постійно передаються на середній рівень, де центральним елементом виступає контролер ESP32. Етап комунікаційної передачі – після первинної обробки контролер постійно використовує мережеві протоколи (Wi-Fi та MQTT) для ефективної передачі даних на верхній аналітичний рівень. Етап ситуаційного аналізу та прийняття рішень – на цьому етапі відбувається постійний аналіз отриманих комплексних даних та застосовуються методи для розпізнавання поточних ситуацій. Етап автоматичного реагування та запобігання – в автоматичному режимі виконуються необхідні дії, спрямовані на нейтралізацію загрози.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила одночасну появу

диму та збільшення температури – датчик MQ-2 зафіксував задимлення та датчик DS18B20 одночасно зареєстрував стрімке зростання температури понад 60°C.

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_5 = srt$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_6 = iscaf$, $crs_7 = ses$, $crs_8 = deab$, $crs_9 = aafs$, $crs_2 = lava$, тобто відбувається негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Пожежа», відбувається надсилання сигналу екстреним службам (через хмарні сервіси або Telegram-бот), відбувається знеструмлення відповідної зони будинку для запобігання коротким замиканням, відбувається активація автоматичної системи пожежогасіння (спринклерів) у зоні займання, а також відбувається активація локальної звукової та світлової сигналізації.

На етапі адаптації та зворотного зв'язку система накопичує дані про зовнішні впливи та звички користувачів.

Розглянемо приклад2 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – зняття показників середовища за допомогою встановлених детекторів диму, природного та чадного газів, аномального тепла й підтоплень – відбувається безперервними циклами з високою інтенсивністю, а саме декілька разів на секунду. Етап збору та попередньої обробки даних – отримана інформація постійно спрямовується на середній рівень системи, ядром якого є контролер ESP32. Етап комунікаційної передачі – після завершення первинної обробки контролер у безперервному режимі залучає протоколи Wi-Fi та MQTT для трансляції даних на верхній аналітичний рівень. Етап ситуаційного аналізу та прийняття рішень – постійна аналітична обробка масивів комплексних даних у ядрі системи. Етап автоматичного реагування та запобігання – система в автономному режимі здійснює заздалегідь визначені заходи, метою яких є повна нейтралізація виявленої загрози.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила витік природного газу – датчик MQ-4 зафіксував концентрацію метану (CH4), рівною 1050 ppm, що є вище заданого безпечного порогу (> 1000 ppm).

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_1 = ngld$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$, тобто відбувається негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Небезпека отруєння», відбувається активація локальної звукової та світлової сигналізації, здійснюється автоматичне подання сигналу на сервопривід для перекриття магістрального газового крана, здійнюється автоматичне відкриття віконних приводів або заслінок припливної вентиляції для провітрювання, відбуваєься негайне вимкнення опалювального приладу.

У процесі адаптації та зворотного зв'язку відбувається акумуляція відомостей щодо поведінкових патернів мешканців та динаміки зовнішніх чинників.

Розглянемо приклад3 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – безперервне отримання даних про стан середовища через розгорнуту мережу детекторів (чадного та природного газів, диму, температури та протікання води) – циклічне опитування з високою інтенсивністю (кілька транзакцій на секунду). Етап збору та попередньої обробки даних – постійна трансляція отриманих сигналів на середній рівень ієрархії, де базовим обчислювальним модулем є контролер ESP32. Етап комунікаційної передачі – використання мережевих протоколів Wi-Fi та MQTT для стабільного передавання підготовленої інформації до аналітичного ядра верхнього рівня. Етап ситуаційного аналізу та прийняття рішень – безперервне оцінювання вхідного потоку даних в межах аналітичного ядра підсистеми. Етап автоматичного

реагування та запобігання – автономне виконання алгоритмів, націлених на локалізацію та усунення джерел небезпеки.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила витік чадного газу – датчик MQ-7 детектував підвищення рівня чадного газу.

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_2 = rcmp$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$, тобто відбувається негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Небезпека отруєння», відбувається активація локальної звукової та світлової сигналізації, здійснюється автоматичне подання сигналу на сервопривід для перекриття магістрального газового крана, здійнюється автоматичне відкриття віконних приводів або заслінок припливної вентиляції для провітрювання, відбуваєься негайне вимкнення опалювального приладу.

Система постійно збирає базу даних про щоденні звички користувачів та параметри навколишнього середовища для подальшого аналізу та налаштування.

Розглянемо приклад4 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – безперервне отримання фізичних показників середовища через розгорнуту мережу детекторів (чадного та природного газів, диму, температури та протікання води) – високоінтенсивне циклічне опитування (кілька транзакцій на секунду). Етап збору та попередньої обробки даних – постійна трансляція отриманих сигналів на середній рівень ієрархії, де базовим обчислювальним модулем є контролер ESP32. Етап комунікаційної передачі – використання мережевих протоколів Wi-Fi та MQTT для стабільного передавання підготовленої інформації до аналітичного ядра верхнього рівня. Етап ситуаційного аналізу та прийняття рішень – безперервне оцінювання вхідного потоку даних.

Етап автоматичного реагування та запобігання – автономне виконання алгоритмів, націлених на локалізацію та усунення джерел небезпеки.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила витік води – зондовий датчик YI-S WL400 Water Level Sensor зафіксував стабільний контакт із водою протягом більше ніж 1–2 секунд (захист від випадкових бризок).

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_6 = wld$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_{10} = iscaft$, $crs_{11} = acsvw$, $crs_2 = lava$, тобто відбувається негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Загроза затоплення», здійснюється автоматичне закриття електромагнітного клапана на вході водопроводу до приміщення, а також відбувається активація локальної звукової та світлової сигналізації.

Завдяки механізму зворотного зв'язку підсистема реєструє та зберігає інформацію про зовнішні впливи й типові дії людей у домі для забезпечення гнучкості керування.

Розглянемо приклад5 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – безперервний збір фізичних показників за допомогою розподіленої мережі сенсорів (газових, термічних та гідравлічних) – в режимі реального часу з інтервалом у кілька зчитувань на секунду. Етап збору та попередньої обробки даних – постійна трансляція сигналів до обчислювального вузла на базі ESP32. Етап комунікаційної передачі – використання стека Wi-Fi та протоколу MQTT для перенесення обробленої інформації до аналітичного центру. Етап ситуаційного аналізу та прийняття рішень – реалізується аналітичним ядром системи, яке в режимі 24/7 проводить оцінку комплексних показників. Етап автоматичного реагування та запобігання – негайна активація програмних сценаріїв, спрямованих на купірування небезпеки в автоматичному режимі.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила аномальний перегрів – датчик DS18B20 зафіксував перевищення температурного порогу без ознак диму (перегрів електрощитової).

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_7 = ao$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_{12} = nufh$, $crs_{13} = apco$, тобто відбувається сповіщення користувача про загрозу пожежі, а також здійснюється автоматичне знеструмлення перегрітої ділянки ланцюга для запобігання займанню.

На етапі адаптації та зворотного зв'язку відбувається формування бази знань про динаміку зовнішніх впливів та типову активність користувачів у помешканні.

Розглянемо приклад6 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – безпосереднє зчитування показників навколишнього середовища за допомогою відповідних датчиків – циклічно з частотою кілька разів на секунду. Етап збору та попередньої обробки даних – отримані дані безперервно передаються на середній рівень системи, ключовим елементом якого є контролер ESP32. Етап комунікаційної передачі – після початкової обробки контролер постійно використовує мережеві протоколи (Wi-Fi та MQTT) для надійної передачі даних на верхній аналітичний рівень. Етап ситуаційного аналізу та прийняття рішень – безперервна обробка сукупності даних із застосуванням відповідних методів для ідентифікації поточних ситуацій. Етап автоматичного реагування та запобігання – виконання необхідних дій у автоматичному режимі з метою усунення або мінімізації потенційної загрози.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила втрату зв’язку – відсутність підключення до Wi-Fi.

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_8 = lc$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_{14} = sadmm$, $crs_{15} = mlfpa$, тобто відбувається перехід контролера ESP32 в автономний режим прийняття рішень (обробка логіки безпосередньо на пристрої), а також здійснюється збереження локальної працездатності фізичних актуаторів (перекриття кранів при спрацюванні датчиків незалежно від наявності Інтернету).

На етапі адаптації та зворотного зв'язку система накопичує дані про зовнішні впливи та звички користувачів.

Розглянемо приклад7 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – безперервне зчитування параметрів довкілля за допомогою відповідних датчиків (диму, природного та чадного газу, температури й витоку води) – циклічно, кілька разів на секунду. Етап збору та попередньої обробки даних – всі отримані дані регулярно передаються на середній рівень системи, де їх обробку забезпечує контролер ESP32. Етап комунікаційної передачі – використання контролером мережевих протоколів (Wi-Fi та MQTT) для стабільної передачі оброблених даних до верхнього рівня аналітики. Етап ситуаційного аналізу та прийняття рішень – постійна обробка комплексних даних із застосуванням відповідних методів для виявлення та інтерпретації поточних станів. Етап автоматичного реагування та запобігання – виконання системою необхідних дій у режимі реального часу з метою усунення або запобігання загрозам.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила виток чадного газу та збільшення температури – датчик MQ-7 задетектував підвищення рівня чадного газу та дачтик DS18B20 задетектував аномальне підвищення температури.

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_3 = cmlrt$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$, тобто тобто відбувається негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Небезпека отруєння», здійснюється активація локальної звукової та світлової сигналізації, здійснюється автоматичне подання сигналу на сервопривід для перекриття магістрального газового крана, відбувається автоматичне відкриття віконних приводів або заслінок припливної вентиляції для провітрювання, відбувається негайне вимкнення опалювального приладу.

На етапі адаптації та зворотного зв'язку система накопичує дані про зовнішні впливи та звички користувачів.

Розглянемо приклад8 функціонування підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Етап первинного сенсорного моніторингу – регулярне зчитування показників навколишнього середовища за допомогою відповідних датчиків – періодично з інтервалом у кілька разів на секунду. Етап збору та попередньої обробки даних – всі зафіксовані значення безперервно передаються до середнього рівня системи, де ключову роль відіграє мікроконтролер ESP32. Етап комунікаційної передачі – використання контролером мережевих технологій (Wi-Fi і MQTT) для оперативної передачі оброблених даних на рівень аналітики. Етап ситуаційного аналізу та прийняття рішень – постійне опрацювання отриманих даних із застосуванням відповідних підходів для визначення поточного стану системи. Етап автоматичного реагування та запобігання – самостійне виконання необхідних дій, спрямованих на запобігання небезпеці або її мінімізацію.

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила виток природного газу та збільшення температури – датчик MQ-4 задетектував підвищення рівня

природного газу та дачтик DS18B20 задетектував аномальне підвищення температури, що свідчить про критичну несправність опалювального приладу.

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію $sdpe_4 = nglrt$, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: $crs_1 = iscap$, $crs_2 = lava$, $crs_3 = somgv$, $crs_4 = aowv$, $crs_5 = isha$, тобто тобто відбувається негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Небезпека отруєння», здійснюється активація локальної звукової та світлової сигналізації, здійснюється автоматичне подання сигналу на сервопривід для перекриття магістрального газового крана, відбувається автоматичне відкриття віконних приводів або заслінок припливної вентиляції для провітрювання, відбувається негайне вимкнення опалювального приладу.

На етапі адаптації та зворотного зв'язку система накопичує дані про зовнішні впливи та звички користувачів.

4.3 Висновки

Четвертий розділ присвячений практичній реалізації та проєктуванню архітектури підсистеми виявлення аварійних ситуацій.

У розділі успішно спроєктовано та візуалізовано архітектуру підсистеми, яка має чітку трирівневу структуру: нижній рівень (сенсорний), середній рівень (контролер ESP32) та верхній рівень (аналітичне ядро). Такий підхід забезпечує логічний поділ функцій між безпосереднім збором даних, їхньою попередньою обробкою та високорівневим прийняттям рішень у межах єдиної кіберфізичної системи.

Обраний склад апаратного забезпечення, до якого увійшли датчики серії MQ (MQ-7, MQ-4, MQ-2), зондовий сенсор витоку води YI-S та прецизійний термометр DS18B20, дозволив створити багатофункціональне рішення, здатне одночасно

контролювати п'ять критичних техногенних ризиків – концентрацію чадного та природного газів, наявність диму, прориви водопроводу та температурні аномалії.

Обраний центральний обчислювальний вузол системи контролер ESP32 завдяки вбудованому 12-бітному АЦП забезпечує високу швидкість та точність обробки аналогових сигналів від газових сенсорів. Двоядерна архітектура контролера дозволяє ефективно розділяти завдання реального часу: одне ядро відповідає за безперервне опитування датчиків, а інше – за мережеву комунікацію та шифрування.

Підтверджено ефективність використання протоколу MQTT, що працює поверх Wi-Fi, як основного стандарту передачі даних. Встановлення рівня якості обслуговування QoS 1 (At least once) гарантує надійну доставку критичних повідомлень про аварії до смартфона користувача, що виключає втрату інформації в мережі.

Практичне функціонування підсистеми базується на багаторівневій обробці, де перший етап – сенсорний моніторинг – виконується циклічно з високою частотою кілька разів на секунду. Це дозволяє системі виступати активним суб’єктом захисту, виявляючи аномалії ще на стадії їх зародження.

Особливу увагу приділено методу перехресної верифікації даних, що став ключовим інструментом підвищення надійності. Наприклад, ідентифікація пожежі (сценарій *srt*) відбувається лише за умови одночасної фіксації задимлення датчиком MQ-2 та стрімкого зростання температури понад 60°C датчиком DS18B20, що мінімізує хибні тривоги.

Продемонстровано переваги автоматичного реагування, де система самостійно активує виконавчі механізми (сервоприводи, клапани). Це забезпечує негайне локальне купірування джерела небезпеки, наприклад, перекриття подачі газу при виявленні витоку метану (сценарій *ngld*), ще до втручання мешканців.

Розроблена архітектура демонструє високу живучість завдяки впровадженню технологій граничних обчислень (edge computing). У разі втрати зв'язку (сценарій *lc*) контролер ESP32 переходить в автономний режим, зберігаючи здатність приймати рішення та керувати фізичними актуаторами локально.

Доведено економічну виправданість проєкту, оскільки використання доступних компонентів робить систему значно дешевшою за промислові аналоги. Це відкриває можливості для масового впровадження інтелектуальної безпеки, роблячи захист майна та життя доступним для широкого загалу.

Отже, підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» трансформує житловий простір у когнітивне середовище, здатне до самонавчання через накопичення даних про звички користувачів. Результати розділу підтверджують, що обрана архітектура та алгоритми забезпечують надійний, автономний та оперативний захист, що є пріоритетним для систем життєзабезпечення майбутнього.

ВИСНОВКИ

Актуальність даної кваліфікаційної роботи зумовлена стрімким розвитком концепції «Розумного будинку» та гострою потребою у створенні надійних, комплексних систем забезпечення безпеки житлового простору. Сучасне помешкання насичене складними інженерними комунікаціями, де швидкість фізичних процесів під час аварії часто перевищує здатність людини до адекватної реакції. Особливого значення це набуває для вразливих верств населення, зокрема самотніх літніх людей та осіб з інвалідністю, для яких автоматизоване виявлення загроз є критично важливим чинником збереження життя та здоров'я.

Наукова новизна дослідження полягає у розробці цілісної кіберфізичної екосистеми, яка долає фрагментарність існуючих рішень шляхом одночасного прецизійного моніторингу множини критичних параметрів. Запропонований метод ситуаційного аналізу базується на принципі перехресної верифікації даних від різних типів сенсорів, що дозволяє системі розуміти контекст подій. Такий підхід радикально знижує ймовірність хибних спрацювань, перетворюючи підсистему з простого набору датчиків на когнітивний вузол безпеки, здатний до автономного прийняття рішень.

Практична значущість роботи підтверджується вибором оптимального апаратного стека на базі контролера ESP32 та лінійки доступних напівпровідникових датчиків MQ-7, MQ-4, MQ-2 у поєднанні з DS18B20 та YI-S. Використання протоколу MQTT з рівнем якості QoS 1 гарантує надійну доставку екстрених повідомлень у реальному часі. Розроблене рішення є економічно виправданим, оскільки воно в кілька разів дешевше за промислові аналоги, що робить інтелектуальну безпеку доступною для широкого загалу споживачів.

Перспективи подальшого розвитку системи лежать у площині впровадження предиктивної аналітики на основі машинного навчання та технологій туманних обчислень (Fog computing). Накопичення історичних даних про зовнішні впливи та звички користувачів дозволить системі еволюціонувати та прогнозувати аварійні ситуації ще до моменту їх фізичного виникнення. Таким чином, дана робота є

вагомим внеском у розвиток концепції безпечного міста та інтелектуальних систем життєзабезпечення майбутнього.

У роботі проведено всебічний аналіз відомих методів та технологічних рішень для виявлення й запобігання аваріям у середовищі «Розумного будинку». Дослідження охоплює еволюцію систем від простих автономних сповіщувачів до сучасних когнітивних екосистем, що використовують штучний інтелект, великі мовні моделі (LLM) та нейронні мережі для розпізнавання загроз у реальному часі. Особливу увагу приділено соціальному аспекту – створенню інтелектуальних систем екстреного виклику, які є життєво необхідними для гарантування безпеки та незалежності літніх людей та осіб з інвалідністю.

На основі критичного аналізу існуючих розробок виявлено низку суттєвих недоліків, серед яких головними є висока вартість складних нейромережевих моделей та вузька спеціалізація більшості комерційних продуктів. Фрагментарний підхід до безпеки змушує користувачів комбінувати несумісні пристрої від різних виробників, що створює технічні складнощі та знижує загальну надійність. Обґрунтовано науково-технічну потребу в розробці універсальної, бюджетної та комплексної підсистеми, яка здатна одночасно здійснювати прецизійний моніторинг множини параметрів: концентрації газів, задимлення, витоків води та температурних коливань.

У роботі також реалізовано обґрунтований вибір апаратного забезпечення, що поєднує високу точність моніторингу з економічною доступністю для широкого вжитку. Проведено глибокий порівняльний аналіз наявних на ринку датчиків чадного (CO) та природного (CH4) газів, диму, температури та витоку води, за результатами якого сформовано оптимальний набір компонентів нижнього рівня. До складу підсистеми увійшли напівпровідникові сенсори серії MQ (MQ-7, MQ-4, MQ-2), зондовий датчик YI-S WL400 та цифровий термометр DS18B20, що дозволяє одночасно контролювати п'ять ключових техногенних загроз.

Особливу увагу приділено вибору центрального обчислювального вузла середнього рівня, де на основі зіставлення характеристик різних платформ було обрано контролер ESP32 . Завдяки наявності двоядерного процесора та

вбудованого 12-бітного АЦП з великою кількістю каналів, цей пристрій забезпечує прецизійне зчитування аналогових сигналів від газових датчиків та їхню паралельну обробку в режимі реального часу. Інтегровані модулі Wi-Fi та Bluetooth дозволяють ESP32 функціонувати як автономний комунікаційний міст, усуваючи потребу в дорогому додатковому обладнанні чи шлюзах.

У межах розділу також обґрунтовано використання мережевого протоколу MQTT, що працює поверх Wi-Fi, як найбільш ефективного стандарту для передачі телеметричних даних. Впровадження рівня якості обслуговування QoS 1 («At least once») гарантує надійну доставку критичних повідомлень про аварії, навіть за умов нестабільного з'єднання. Сформований апаратний стек створює надійний фундамент для перетворення підсистеми з простого детектора на повноцінний когнітивний вузол безпеки, здатний до автономного захисту житла.

У дослідженні розроблено комплексний метод та алгоритм функціонування підсистеми, що базуються на багаторівневій структурі для переходу від фізичного сприйняття середовища до інтелектуального прийняття рішень. Метод охоплює шість послідовних етапів: від високоінтенсивного сенсорного моніторингу (кілька разів на секунду) до автоматичного реагування та етапу адаптації. Така системність дозволяє трансформувати набір датчиків у когнітивну екосистему, здатну аналізувати контекст виникнення загроз.

Важливою складовою розділу є формування множини сценаріїв роботи та відповідних заходів реагування. Визначено вісім ключових ситуацій, серед яких виявлення витоків природного та чадного газів, верифікація пожежі за двома параметрами (дим та температура), загроза затоплення та аномальний перегрів обладнання. Для кожної ситуації розроблено алгоритм дій – від надсилання MQTT-сповіщень із відповідними позначками небезпеки до фізичного керування актуаторами, такими як сервоприводи газових кранів та електромагнітні клапани водопостачання.

Особливу увагу приділено алгоритму автономного функціонування, який забезпечує живучість системи навіть за умови втрати зв'язку з мережею (сценарій *lc*). Завдяки технологіям граничних обчислень на базі ESP32, контролер здатний

переходити в автономний режим прийняття рішень, зберігаючи локальну працездатність фізичних вузлів. Крім того, впроваджений механізм адаптації дозволяє системі накопичувати дані про звички користувачів і зовнішні впливи, що забезпечує постійне вдосконалення логіки захисту та розпізнавання аномалій у складних умовах.

У роботі проведено детальне проєктування архітектури підсистеми виявлення та запобігання аварійним ситуаціям, яка базується на трирівневій моделі функціонування. Нижній рівень забезпечує безпосереднє зчитування фізичних параметрів середовища через обрані датчики MQ-7, MQ-4, MQ-2, DS18B20 та YI-S. Середній рівень, ядром якого є контролер ESP32, здійснює збір, первинну фільтрацію та підготовку даних для подальшої передачі, виконуючи роль інтелектуального мосту між сенсорами та аналітичними модулями.

Особливу увагу приділено реалізації комунікаційного зв’язку на основі протоколу MQTT та стандарту Wi-Fi. Для гарантованої доставки критично важливих повідомлень про загрози було впроваджено рівень якості обслуговування QoS 1 («At least once»), що мінімізує мережевий трафік та забезпечує надійну інтеграцію пристрою у загальну цифрову інфраструктуру будинку.

Верхній рівень архітектури містить аналітичне ядро та модуль ситуаційного аналізу, де на основі правил бази знань відбувається фінальна інтерпретація комплексних даних та вибір оптимальних сценаріїв реагування.

Практична значущість розділу підтверджується описом автоматизованих циклів реагування, які включають миттєве сповіщення користувача через мобільний застосунок, автоматичне перекриття подачі води чи газу та інформування екстрених служб. Розроблена архітектура трансформує звичайне житло у когнітивне середовище, здатне ефективно запобігати техногенним аваріям. Водночас визначено перспективи розвитку системи через впровадження предиктивної аналітики та технологій туманних обчислень для підвищення відмовостійкості системи в критичних умовах.

Наукова новизна отриманих результатів: розроблено метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», що

відрізняється від існуючих аналогів прецизійним моніторингом одночасно п'яти критичних загроз – витоків природного та чадного газів, появи диму, несанкціонованих витоків води та аномальних температурних коливань та забезпечує виконання необхідних дій в автоматичному режимі, спрямованих на попередження та запобігання аварійним ситуаціям (сповіщення користувача, перекривання подачі води/газу, сповіщення екстрених рятувальних служб тощо).

Практична значущість отриманих результатів полягає у реалізації підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок», яка забезпечує високий рівень безпеки завдяки комплексній інтеграції різнопланових сенсорів та алгоритмів обробки даних у реальному часі.

За темою кваліфікаційної роботи опублікована одна стаття у фаховому науковому журналі України категорії Б (додаток А):

1) Войчур Ю.О., Медзатий Д.М., Жандра А.Я. Підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». *Вісник Хмельницького національного університету. Серія «Технічні науки»*. 2026. №1. С. _____.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Resilient Distributed Optimization for Multi-Agent Cyberphysical Systems / M. Yemini et al. *IEEE Transactions on Automatic Control*. 2025. P. 1–16. URL: https://doi.org/10.1109/tac.2025.3532791.

2. Explainable AI for Cyber-Physical Systems: Issues and Challenges / A. Hoenig et al. *IEEE Access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3395444.

3. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook / S. J. Oks et al. *Information Systems Frontiers*. 2022. URL: https://doi.org/10.1007/s10796-022-10252-x.

4. Fuada S., Hendriyana H. UPISmartHome V.2.0 – A Consumer Product of Smart Home System with an ESP8266 as the Basis. *Journal of Communications*. 2022. P. 541–552. URL: https://doi.org/10.12720/jcm.17.7.541-552.

5. Sung W.-T., Hsiao S.-J. Creating Smart House via IoT and Intelligent Computation. *Intelligent Automation & Soft Computing*. 2023. Vol. 35, no. 1. P. 415–430. URL: https://doi.org/10.32604/iasc.2023.027618.

6. Smart Home Personal Assistants: Fueled by Natural Language Processor and Blockchain Technology / S. A. Ansar et al. *2022 Second International Conference on Interdisciplinary Cyber Physical Systems (ICPS)*, Chennai, India, 9–10 May 2022. 2022. URL: https://doi.org/10.1109/icps55917.2022.00029.

7. Yaici W., Entchev E., Longo M. Internet of Things (IoT)-Based System for Smart Home Heating and Cooling Control. 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), Prague, Czech Republic, 28 June – 1 July 2022. 2022. URL: https://doi.org/10.1109/eeeic/icpseurope54979.2022.9854634.

8. Harnessing Real-Time Data for Intelligent Decision-Making in Cyber-Physical Systems / T. Premavathi et al. *Advances in Computer and Electrical Engineering*. 2024. P. 257–286. URL: https://doi.org/10.4018/979-8-3693-5728-6.ch010.

9. Azeri N., Hioual O., Hioual O. Towards an Approach for Modeling and Architecting of Self-Adaptive Cyber-Physical Systems. *2022 4th International*

Conference on Pattern Analysis and Intelligent Systems (PAIS), Oum El Bouaghi, Algeria, 12–13 October 2022. 2022. URL: https://doi.org/10.1109/pais56586.2022.9946921.

10. Cognitive architecture for cognitive cyber-physical systems / J. Al Haj Ali et al. *IFAC-PapersOnLine*. 2024. Vol. 58, no. 19. P. 1180–1185. URL: https://doi.org/10.1016/j.ifacol.2024.09.099.

11. Kluge T. A role-based architecture for self-adaptive cyber-physical systems. *SEAMS '20: IEEE/ACM 15th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, Seoul Republic of Korea. New York, NY, USA, 2020. URL: https://doi.org/10.1145/3387939.3391601.

12. Nota G., Petraglia G. Heritage buildings management: the role of situational awareness and cyber-physical systems. *Journal of Ambient Intelligence and Humanized Computing*. 2024. URL: https://doi.org/10.1007/s12652-023-04750-2.

13. Edge-Computing-Driven Internet of Things: A Survey / L. Kong et al. *ACM Computing Surveys*. 2022. URL: https://doi.org/10.1145/3555308.

14. Design Procedure for Real-Time Cyber–Physical Systems Tolerant to Cyberattacks / C. M. Paredes et al. *Symmetry*. 2024. Vol. 16, no. 6. P. 684. URL: https://doi.org/10.3390/sym16060684.

15. Assessing the effectiveness and cost-effectiveness of a smart home emergency call system: study protocol for a randomised controlled trial in Germany / H. Rehse et al. *BMJ Open*. 2025. Vol. 15, no. 4. P. e092893. URL: https://doi.org/10.1136/bmjopen-2024-092893.

16. Smart Assistance of Elderly Individuals in Emergency Situations at Home / A. R. Reddy et al. *Internet of Things*. Cham, 2021. P. 95–115. URL: https://doi.org/10.1007/978-3-030-63937-2_6.

17. Personennotrufsysteme auf Basis menschlicher vital- und systemtechnischer Parameter in einer Smart-Home-Umgebung / Emergency-call Systems Based on Human Vital and System-technical Parameters in a Smart-home Environment / M. Hampicke et al. *Biomedizinische Technik/Biomedical Engineering*. 2002. Vol. 47, no. 11. P. 278–284. URL: https://doi.org/10.1515/bmte.2002.47.11.278.

18. Wilhelm S., Wahl F. Emergency Detection in Smart Homes Using Inactivity Score for Handling Uncertain Sensor Data. *Sensors*. 2024. Vol. 24, no. 20. P. 6583. URL: https://doi.org/10.3390/s24206583.

19. Pramunanto E., Muhtadin M., Febrian W. Integrated Smart Safety Home System based on Wireless Sensor Network and Internet of Things as Emergency Preventive Efforts in Settlement Areas. *2019 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, Surabaya, Indonesia, 19–20 November 2019. 2019. URL: https://doi.org/10.1109/cenim48368.2019.8973328.

20. Şevik R., Demirci R., Yılmaz Y. IoT-Powered Voice Interaction and Proactive Gas Leak Detection System for Smart Homes with Embedded Gas Sensing and Instant AI Alerts. *2025 Innovations in Intelligent Systems and Applications Conference (ASYU)*, Bursa, Turkiye, 10–12 September 2025. 2025. P. 1–8. URL: https://doi.org/10.1109/asyu67174.2025.11208502.

21. A Multi-Scale Approach to Early Fire Detection in Smart Homes / A. Abdusalomov et al. *Electronics*. 2024. Vol. 13, no. 22. P. 4354. URL: https://doi.org/10.3390/electronics13224354.

22. Development of Arduino based smart home fire alarm system with emergency SOS notification / K. R. Rajinran et al. *PROCEEDINGS OF 5TH INTERNATIONAL CONFERENCE ON SUSTAINABLE INNOVATION IN ENGINEERING AND TECHNOLOGY 2023*, Kuala Lumpur, Malaysia. 2024. P. 020103. URL: https://doi.org/10.1063/5.0229532.

23. Paglinawan C. C., Bagunu R. A. D., Castillo S. T. Mobile Application for IoT-Based Smart Home System for Appliance Control and Fire Alert. *2024 16th International Conference on Computer and Automation Engineering (ICCAE)*, Melbourne, Australia, 14–16 March 2024. 2024. URL: https://doi.org/10.1109/iccae59995.2024.10569777.

24. Chrysafiadi K., Tsichrintzi E.-A., Sakkopoulos E. A smart home fuzzy logic-based cooking fire prevention system addressing human errors due to distraction or minor medical memory lapses. *Procedia Computer Science*. 2024. Vol. 246. P. 3390–3399. URL: https://doi.org/10.1016/j.procs.2024.09.218.

25. A Trustable Federated Learning Framework for Rapid Fire Smoke Detection at the Edge in Smart Home Environments / A. N. Patel et al. *IEEE Internet of Things Journal*. 2024. P. 1. URL: https://doi.org/10.1109/jiot.2024.3439228.

26. Fired:An Image-Based Fire Detector for Smart Homes using Machine Learning Algorithms / G. M. Srinath et al. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, Chikkaballapur, India, 18–19 April 2024. 2024. P. 1–4. URL: https://doi.org/10.1109/ickecs61492.2024.10616511.

27. Debnath S., Gautam J., Rai S. K. IoT Based Smart Home and Office Fire Notification Alert System. *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Gwalior, India, 14–16 March 2024. 2024. URL: https://doi.org/10.1109/iatmsi60426.2024.10503336.

28. IoT-Enabled Fire Detection System for a Smart Home Environment / J. H. V. Reddy et al. *Proceedings of Second International Conference on Computational Electronics for Wireless Communications*. Singapore, 2023. P. 347–357. URL: https://doi.org/10.1007/978-981-19-6661-3_31.

29. Suklabaidya S., Das I. IoT as a Platform: For Smart Home Analysis and Monitoring of Fire Parameters. Adva*nced Computing and Intelligent Technologies*. Singapore, 2021. P. 329–338. URL: https://doi.org/10.1007/978-981-16-2164-2_27.

30. Kang J., Basnet S., Farhad S. M. Smart Fire-Alarm System for Home. *Advances in Intelligent Systems and Computing*. Cham, 2019. P. 474–483. URL: https://doi.org/10.1007/978-3-030-22354-0_42.

31. Harun Al Rasyid M. U., Enda D., Saputra F. A. Smart Home System for Fire Detection Monitoring Based on Wireless Sensor Network. *2019 International Electronics Symposium (IES)*, Surabaya, Indonesia, 27–28 September 2019. 2019. URL: https://doi.org/10.1109/elecsym.2019.8901528.

32. Wireless Kitchen Fire Prevention System Using Electrochemical Carbon Dioxide Gas Sensor for Smart Home / S.-J. Kweon et al. *Sensors*. 2022. Vol. 22, no. 11. P. 3965. URL: https://doi.org/10.3390/s22113965.

33. Liu X., Yan K. Design and implementation of fire alarm module for smart home. *International Conference on Electronic Information Engineering and Data Processing (EIEDP 2023)*, Nanchang, China, 17–19 March 2023 / ed. by V. E. Balas, Z. H. Khan. 2023. URL: https://doi.org/10.1117/12.2682265.

34. Comprehensive Smart Home Automation: Network Setup, Fire Prevention, and Network Security using Cisco Packet Tracer / B. Roy et al. *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*, Chennai, India, 14–15 December 2023. 2023. URL: https://doi.org/10.1109/iccebs58601.2023.10448604.

35. FireDS-IoT: A Fire Detection System for Smart Home Based on IoT Data Analytics / S. K. Bhoi et al. *2018 International Conference on Information Technology (ICIT)*, Bhubaneswar, India, 19–21 December 2018. 2018. URL: https://doi.org/10.1109/icit.2018.00042.

36. Smart Plug 2.0: Solid State Smart Plugs Preventing Fire and Shock Hazards in Smart Homes and Offices / Z. Deng et al. *2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, Detroit, MI, USA, 11–15 October 2020. 2020. URL: https://doi.org/10.1109/ecce44975.2020.9235862.

37. Early Detection System for Gas Leakage and Fire in Smart Home Using Machine Learning / L. Salhi et al. *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 11–13 January 2019. 2019. URL: https://doi.org/10.1109/icce.2019.8661990.

38. Inventive Fire Detection utilizing Raspberry Pi for New Age Home of Smart Cities / M. Sheth et al. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 20–22 August 2020. 2020. URL: https://doi.org/10.1109/icssit48917.2020.9214108.

39. Maalsen S., Sadowski J. The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance. *Surveillance & Society*. 2019. Vol. 17, no. 1/2. P. 118–124. URL: https://doi.org/10.24908/ss.v17i1/2.12925.

40. Şevik R., Demirci R., Yılmaz Y. IoT-Powered Voice Interaction and Proactive Gas Leak Detection System for Smart Homes with Embedded Gas Sensing and

Instant AI Alerts. *2025 Innovations in Intelligent Systems and Applications Conference (ASYU)*, Bursa, Turkiye, 10–12 September 2025. 2025. P. 1–8. URL: https://doi.org/10.1109/asyu67174.2025.11208502.

41. Gas Management in Smart Homes: A Multi-agent and Knowledge Graph Approach / M. Berkani et al. *Lecture Notes in Networks and Systems*. Cham, 2025. P. 21–31. URL: https://doi.org/10.1007/978-3-031-92734-8_3.

42. Design and Implementation of a Smart Home IoT Gas Detection and Alert System / A. H. Matey et al. *African Journal of Applied Research*. 2026. Vol. 12, no. 1. P. 278–300. URL: https://doi.org/10.26437/1xehzg89.

43. Development of a Smart and Cost Effective Gas Leakage and Flame Detection System for Homes and Industries / T. G. Tamara-Tarime et al. *2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON)*, Ado Ekiti, Nigeria, 26–28 November 2024. 2024. P. 1–5. URL: https://doi.org/10.1109/nigercon62786.2024.10927102.

44. Smart Home Gas Sensor Optimization Using Kalman Filter for Data Processing / Somantri et al. *2024 Ninth International Conference on Informatics and Computing (ICIC)*, Medan, Indonesia, 24–25 October 2024. 2024. P. 1–6. URL: https://doi.org/10.1109/icic64337.2024.10956724.

45. LPG Smart Guard: An IoT-Based Solution for Real-Time Gas Cylinder Monitoring and Safety in Smart Homes / D. Balogun et al. *ICSEE 2024*. Basel Switzerland, 2024. P. 9. URL: https://doi.org/10.3390/ecsa-11-20471.

46. SGD: Smart Gas Leakage Detection System for Home Safety / E. M. Saleh et al. *2024 14th International Conference on Advanced Computer Information Technologies (ACIT)*, Ceske Budejovice, Czech Republic, 19–21 September 2024. 2024. P. 581–585. URL: https://doi.org/10.1109/acit62333.2024.10712453.

47. Smart LPG Gas Detection and Automatic Booking System for Home Safety Using IoT Platform / T. Kar et al. *2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, 2–6 October 2023. 2023. URL: https://doi.org/10.1109/khpiweek61412.2023.10312969.

48. Wireless Kitchen Fire Prevention System Using Electrochemical Carbon Dioxide Gas Sensor for Smart Home / S.-J. Kweon et al. *Sensors*. 2022. Vol. 22, no. 11. P. 3965. URL: https://doi.org/10.3390/s22113965.

49. Safaie A. A., Alizadeh Bidgoli M., Javadi S. A multi-objective optimization framework for integrated electricity and natural gas networks considering smart homes in downward under uncertainties. *Energy*. 2022. Vol. 239. P. 122214. URL: https://doi.org/10.1016/j.energy.2021.122214.

50. F. Abbas A., Z. Abdullah M. DESIGN AND IMPLEMENTATION OF A SMART HOME GAS DETECTION BASED ON MOBILE NETWORK SYSTEM. *Journal of Engineering and Sustainable Development*. 2021. Vol. 25, no. 02. P. 9–16. URL: https://doi.org/10.31272/jeasd.25.2.2.

51. Smart Gas Monitoring System for Home and Industries / M. Kavitha et al. *IOP Conference Series: Materials Science and Engineering*. 2020. Vol. 981. P. 022003. URL: https://doi.org/10.1088/1757-899x/981/2/022003.

52. A Study on HT32F1765 MCU-Based in Smart Home Gas Monitoring / D. Y. Qiao et al. *Applied Mechanics and Materials*. 2014. Vol. 644-650. P. 1298–1302. URL: https://doi.org/10.4028/www.scientific.net/amm.644-650.1298.

53. Wireless Self-Powered High-Performance Integrated Nanostructured-Gas-Sensor Network for Future Smart Homes / Z. Song et al. *ACS Nano*. 2021. Vol. 15, no. 4. P. 7659–7667. URL: https://doi.org/10.1021/acsnano.1c01256.

54. Optimal scheduling of gas and electricity consumption in a smart home with a hybrid gas boiler and electric heating system / J. Wang et al. *Energy*. 2020. Vol. 204. P. 117951. URL: https://doi.org/10.1016/j.energy.2020.117951.

55. Mahalakshmi A., Yogalakshmi S. An Evaluation on Gas Spillage Detection and Controlling Framework in Smart Home. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 22–24 January 2020. 2020. URL: https://doi.org/10.1109/iccci48352.2020.9104163.

56. Holistic Privacy for Electricity, Water, and Natural Gas Metering in Next Generation Smart Homes / C. E. Kement et al. *IEEE Communications Magazine*. 2021. Vol. 59, no. 3. P. 24–29. URL: https://doi.org/10.1109/mcom.001.2000263.

57. Early Detection System for Gas Leakage and Fire in Smart Home Using Machine Learning / L. Salhi et al. *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 11–13 January 2019. 2019. URL: https://doi.org/10.1109/icce.2019.8661990.

58. Development and Implementation of a Smart Water Metering and Monitoring System for Homes with Intermittent Water Supply / J. L. Torres-Gutierrez et al. *Technologies*. 2026. Vol. 14, no. 2. P. 135. URL: https://doi.org/10.3390/technologies14020135.

59. Noninvasive Acoustic Recognition of Water Flow Sources for Human Activity Monitoring in Smart Homes / S. Comai et al. *Sensors*. 2025. Vol. 25, no. 19. P. 6221. URL: https://doi.org/10.3390/s25196221.

60. Neto A., Gomes L., Vale Z. Human-in-the-Loop Interaction: Application of Machine Learning and Intelligent Virtual Assistant in a Smart Home to Reduce Electric Water Heater Consumption. *Lecture Notes in Networks and Systems*. Cham, 2026. P. 313–325. URL: https://doi.org/10.1007/978-3-032-01234-0_26.

61. IoT-Smart Water Monitoring Module for Home Connection for Pattern Identification Based on ESP32-Grafana / G. H. C. Cabrera et al. *2025 IEEE Colombian Caribbean Conference (C3)*, Santa Marta, Colombia, 17–20 September 2025. 2025. P. 1–6. URL: https://doi.org/10.1109/c366505.2025.11340073.

62. Water Wastage Detection in Smart Homes Through IoT and Machine Learning / C. Brunelli et al. *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 6–9 January 2024. 2024. URL: https://doi.org/10.1109/ccnc51664.2024.10454886.

63. The design and implementation of a smart home for water conservation with onsite rainwater harvesting / R. P. Manser et al. *Environment, Development and Sustainability*. 2026. URL: https://doi.org/10.1007/s10668-025-07285-y.

64. Real-Time Smart Water Management System (SWMS) for Smart Home / A. Verma et al. *Lecture Notes in Civil Engineering*. Singapore, 2023. P. 129–137. URL: https://doi.org/10.1007/978-981-99-2905-4_10.

65. Mathunjwa B. M., Hsu Y. L. Feasibility study for lifestyle monitoring of older adults living independently at home using smart water meter data. *Gerontechnology*. 2024. Vol. 23, s. P. 1. URL: https://doi.org/10.4017/gt.2024.23.s.1035.opp.

66. Securing fog-assisted IoT smart homes: a federated learning-based intrusion detection approach / R. Bensaid et al. *Cluster Computing*. 2024. Vol. 28, no. 1. URL: https://doi.org/10.1007/s10586-024-04711-0.

67. IoT-Based Intelligent Gas Leakage Detection and Fire Protection System / G. Z. Islam et al. *International Journal of Interactive Mobile Technologies (iJIM)*. 2022. Vol. 16, no. 21. P. 49–70. URL: https://doi.org/10.3991/ijim.v16i21.30311.

68. Yousiff S. A., Muhajjar R. A., Al-Zubaidie M. H. Designing A Blockchain Approach to Secure Firefighting Stations Based Internet of Things. *Informatica*. 2023. Vol. 47, no. 10. URL: https://doi.org/10.31449/inf.v47i10.5395.

69. A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience / U. Islam et al. *Scientific Reports*. 2025. Vol. 15, no. 1. URL: https://doi.org/10.1038/s41598-025-09696-3.

70. Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks / J. Goh et al. *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, Singapore, 12–14 January 2017. 2017. URL: https://doi.org/10.1109/hase.2017.36.

71. Ibrahim M., Elhafiz R. Security Analysis of Cyber-Physical Systems Using Reinforcement Learning. *Sensors*. 2023. Vol. 23, no. 3. P. 1634. URL: https://doi.org/10.3390/s23031634.

72. Wu L., Chen L., Hao X. Multi-Sensor Data Fusion Algorithm for Indoor Fire Early Warning Based on BP Neural Network. *Information*. 2021. Vol. 12, no. 2. P. 59. URL: https://doi.org/10.3390/info12020059.

73. Kaitovic I., Lukovic S., Malek M. Proactive Failure Management in Smart Grids for Improved Resilience: A Methodology for Failure Prediction and Mitigation. *2015 IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, 6–10 December 2015. 2015. URL: https://doi.org/10.1109/glocomw.2015.7414155.

74. Artificial Intelligence-Based Secured Power Grid Protocol for Smart City / A. Sulaiman et al. *Sensors*. 2023. Vol. 23, no. 19. P. 8016. URL: https://doi.org/10.3390/s23198016.

75. Al Ghamdi A., Khairullah E., Al mojamed M. LoRaWAN Performance Analysis for a Water Monitoring and Leakage Detection System in a Housing Complex. *Sensors*. 2022. Vol. 22, no. 19. P. 7188. URL: https://doi.org/10.3390/s22197188.

76. A Cyber-Physical System for Wildfire Detection and Firefighting / P. Battistoni et al. *Future Internet*. 2023. Vol. 15, no. 7. P. 237. URL: https://doi.org/10.3390/fi15070237.

77. IOT-Based Gas Leakage Detection and Gas Empty Alert System / P. Priya et al. *International Journal of Scientific Research in Engineering and Management*. 2024. Vol. 08, no. 06. P. 1–9. URL: https://doi.org/10.55041/ijsrem35873.

78. Setiawan F. B., Magfirawaty. Securing Data Communication Through MQTT Protocol with AES-256 Encryption Algorithm CBC Mode on ESP32-Based Smart Homes. *2021 International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE)*, Banda Aceh, Indonesia, 20–21 October 2021. 2021. URL: https://doi.org/10.1109/cosite52651.2021.9649577.

79. Ciuffreda I., Casaccia S., Revel G. M. A Multi-Sensor Fusion Approach Based on PIR and Ultrasonic Sensors Installed on a Robot to Localise People in Indoor Environments. *Sensors*. 2023. Vol. 23, no. 15. P. 6963. URL: https://doi.org/10.3390/s23156963.

80. IoT and AI for Real-time Water Monitoring and Leak Detection / L. Guezouli et al. *Journal of Renewable Energies*. 2024. Vol. 27, no. 2. URL: https://doi.org/10.54966/jreen.v27i2.1210.

81. Reliability and Detectability of Emergency Management Systems in Smart Cities under Common Cause Failures / T. C. Jesus et al. *Sensors*. 2024. Vol. 24, no. 9. P. 2955. URL: https://doi.org/10.3390/s24092955.

82. Babiuch M., Postulka J. Smart Home Monitoring System Using ESP32 Microcontrollers. *Internet of Things*. 2020. URL: https://doi.org/10.5772/intechopen.94589.

83. Mohsin A. S. M., Muyeed M. A. IoT based smart emergency response system (SERS) for monitoring vehicle, home and health status. *Discover Internet of Things*. 2024. Vol. 4, no. 1. URL: https://doi.org/10.1007/s43926-024-00073-6.

84. Malebary S. J. Early Fire Detection Using Long Short-Term Memory-Based Instance Segmentation and Internet of Things for Disaster Management. *Sensors*. 2023. Vol. 23, no. 22. P. 9043. URL: https://doi.org/10.3390/s23229043.

85. Yang T., Ham S., Park S. Safety Monitoring System for Seniors in Large-Scale Outdoor Smart City Environment. *Applied Sciences*. 2025. Vol. 15, no. 24. P. 13057. URL: https://doi.org/10.3390/app152413057.

86. Nandy T., Coutu R., Ababei C. Carbon Monoxide Sensing Technologies for Next-Generation Cyber-Physical Systems. *Sensors*. 2018. Vol. 18, no. 10. P. 3443. URL: https://doi.org/10.3390/s18103443.

ДОДАТОК А
(обов’язковий)

КОПІЇ СТАТТІ У ФАХОВОМУ НАУКОВОМУ ВИДАННІ

1) Войчур Ю.О., Медзатий Д.М., Жандра А.Я. Підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». *Вісник Хмельницького національного університету. Серія «Технічні науки»*. 2026. №1. С. _____.

УДК 004.9

Ю. О. ВОЙЧУР[1], Д. М. МЕДЗАТИЙ[2], А. Я. ЖАНДРА[3]
Хмельницький національний університет
ORCID ID: 0000-0003-3085-7315[1], /0009-0004-3247-6406[2]
e-mail: voichury@khmnhu.edu.ua[1], medza@ukr.net[2], a.zhandra@gmail.com[3]

ПІДСИСТЕМА ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АВАРІЙНИМ СИТУАЦІЯМ В КІБЕРФІЗИЧНІЙ СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

У представленій статті обґрунтовано концепцію та технічну реалізацію підсистеми виявлення та запобігання аварійним ситуаціям кіберфізичної системи «Розумний будинок». Актуальність дослідження зумовлена стрімкою цифровізацією побуту та ускладненням інженерних мереж. Кіберфізична система розглядається не просто як набір гаджетів, а як складний інтегрований простір, де цифрові сервіси та фізичні пристрої взаємодіють у безперервному циклі для забезпечення безпеки життєдіяльності. У роботі проведено детальний огляд існуючих рішень, що дозволило виявити їхні ключові недоліки – високу вартість та вузьку спеціалізацію на окремих загрозах. Для подолання цих бар'єрів запропоновано універсальну комплексну підсистему, яка базується на доступному та потужному контролері ESP32, що забезпечує високу швидкість обробки даних завдяки двоядерному процесору та вбудованим АЦП. Апаратний стек підсистеми включає лінійку напівпровідникових датчиків MQ-7, MQ-4 та MQ-2 для детектування чадного газу, метану й диму, а також цифровий термометр DS18B20 та зондовий датчик витоку води YI-S. Особливу увагу приділено архітектурі системи, яка побудована на трирівневій структурі – локальному рівні збору первинної інформації, середньому рівні первинної обробки на базі ESP32 та верхньому аналітичному рівні, де реалізовано модулі ситуаційного аналізу та прийняття рішень. Комунікація між рівнями здійснюється через протокол MQTT поверх Wi-Fi, що гарантує мінімальні затримки передачі даних та надійність доставки критичних повідомлень завдяки використанню рівня якості обслуговування QoS 1. Наукова новизна підходу полягає у використанні принципу ситуаційної інтелектуалізації, де система сприймає дані як цілісні сценарії, що дозволяє виконувати перехресну верифікацію подій, наприклад, підтверджувати факт пожежі одночасним зростанням температури та рівня задимлення, суттєво знижуючи ймовірність хибних тривог. Запропоноване рішення демонструє оптимальний баланс між вартістю компонентів та технічною складністю, трансформуючи житловий простір у саморефлексивне безпечне середовище.

Ключові слова: кіберфізична система «Розумний будинок», Інтернет речей (IoT) , контролер ESP32, датчик MQ-7, датчик MQ-4, датчик MQ-2, датчик DS18B20, датчик YI-S, протокол MQTT, ситуаційний аналіз, автоматичне реагування.

Yu. O. VOICHUR, D. M. MEDZATYI, A. Ya. ZHANDRA
Khmelnytskyi National University

SUBSYSTEM FOR DETECTING AND PREVENTING EMERGENCY SITUATIONS IN THE CYBER-PHYSICAL SYSTEM "SMART HOME"

This article substantiates the concept and technical implementation of a subsystem for detecting and preventing emergency situations in the cyber-physical system "Smart Home." The relevance of the study is due to the rapid digitalization of everyday life and the increasing complexity of engineering networks. The cyber-physical system is considered not just as a set of gadgets, but as a complex integrated space where digital services and physical devices interact in a continuous cycle to ensure safety. The paper provides a detailed review of existing solutions, revealing their key shortcomings: high cost and narrow specialization in specific threats. To overcome these barriers, a universal integrated subsystem is proposed, based on the affordable and powerful ESP32 controller, which provides high data processing speed thanks to a dual-core processor and built-in ADCs. The subsystem's hardware stack includes a line of MQ-7, MQ-4, and MQ-2 semiconductor sensors for detecting carbon monoxide, methane, and smoke, as well as a DS18B20 digital thermometer and a YI-S water leak probe sensor. Particular attention has been paid to the system architecture, which is based on a three-level structure: the local level for collecting primary information, the middle level for primary processing based on ESP32, and the upper analytical level, where situational analysis and decision-making modules are implemented. Communication between levels is carried out via the MQTT protocol over Wi-Fi, which guarantees minimal data transmission delays and reliable delivery of critical messages thanks to the use of QoS 1 quality of service level. The scientific novelty of the approach lies in the use of the principle of situational intellectualization, where the system perceives data as holistic scenarios, allowing for cross-verification of events, for example, confirming the fact of a fire by a simultaneous increase in temperature and smoke level, significantly reducing the likelihood of false alarms. The proposed solution demonstrates an optimal balance between component cost and technical complexity, transforming the living space into a self-reflective safe environment.

Keywords: cyber-physical system "Smart Home", Internet of Things (IoT), ESP32 controller, MQ-7 sensor, MQ-4 sensor, MQ-2 sensor, DS18B20 sensor, YI-S sensor, MQTT protocol, situational analysis, automatic response.

Вступ

Сучасне розуміння кіберфізичних систем (КФС) значно еволюціонувало, перетворившись із вузькотехнічного терміна на фундаментальну міждисциплінарну категорію [1, 2]. Сьогодні така система розглядається як складний інтегрований простір, де обчислювальні алгоритми, цифрові сервіси та фізичні пристрої взаємодіють у безперервному циклі. КФС фактично стирає межу між віртуальним та матеріальним світами, об'єднуючи датчики, мікроконтролери та хмарні технології в єдину функціональну мережу [3]. Це яскраве втілення концепції Інтернету речей, яке знаходить застосування в усіх сферах – від промисловості та медицини до створення інтелектуального житлового простору [4].

У контексті «Розумного будинку» кіберфізична система виступає не просто як набір дистанційно керованих гаджетів, а як цілісна екосистема, спрямована на підвищення комфорту, безпеки та енергоефективності. Вона об'єднує управління усіма керованими функціями та комунікаціями будинку в єдиний інтелектуальний контур [5, 6]. Головною перевагою такої структури є здатність автоматизувати рутинні побутові процеси, позбавляючи мешканців необхідності постійного ручного контролю [7]. Система самостійно збирає дані, аналізує їх та приймає рішення згідно із заданими параметрами, забезпечуючи наочність управління та суттєву економію ресурсів.

Важливою рисою КФС «Розумний будинок» є її адаптивність та здатність функціонувати в умовах високої невизначеності. На відміну від класичних систем автоматизації, вона виступає активним суб'єктом прийняття рішень, що базується на глибокому аналізі контексту та сенсорної інформації [8]. Система не лише реагує на подразники, а й розпізнає складні ситуації, вибудовуючи логіку дій без прямого втручання людини. Це стає можливим завдяки здатності до самонавчання – накопичуючи дані про звички користувачів та зовнішні впливи, «Розумний будинок» постійно вдосконалює власні алгоритми реагування, стаючи більш стійким до збоїв.

Архітектурно така система базується на багаторівневій структурі, що охоплює шлях від фізичного рівня (сенсори, актуатори, контролери) до когнітивного висновку на основі функціонування кібернетичного (алгоритми прийняття рішень, база знань) та комунікаційного (мережі передачі даних) рівнів [9]. Сенсорний рівень відповідає за первинне сприйняття середовища (дим, газ, температура, виток води тощо), тоді як обчислювальний рівень забезпечує фільтрацію та передачу цих даних. Аналітичне ядро, використовуючи алгоритми прийняття рішень, класифікує стани та формує стратегію дій. Завершує цей цикл виконавчий рівень, де актуатори та реле перетворюють цифрові команди у фізичні дії, а когнітивно-комунікаційний модуль забезпечує зв'язок із користувачем через хмарні інтерфейси [10].

Сучасна парадигма КФС відмовляється від запрограмованої лінійної логіки на користь ситуаційної інтелектуалізації [11]. Це означає, що система сприймає дані не як окремі цифри, а як цілісні сценарії реальності [12]. Завдяки впровадженню технологій граничних обчислень (edge computing), обробка інформації відбувається безпосередньо в точках її збору, що мінімізує затримки та гарантує автономність будинку навіть за відсутності інтернету [13]. Модуль ситуаційного аналізу дозволяє виявляти аномалії в життєритмі оселі, відрізняючи стандартні побутові процеси від потенційних загроз або аварійних випадків.

Особливою складністю проектування таких систем у житловому секторі є вплив людського фактора, який позбавлений жорсткого детермінізму. Тому КФС «Розумний будинок» має відповідати вимогам систем реального часу, де швидкість реакції на критичні події вимірюється частками секунди [14]. Вона повинна бути онтологічно відкритою, дозволяючи легко інтегрувати нові пристрої та сценарії без перебудови всієї архітектури. Зрештою, така система трансформується з технічного засобу в інтелектуального агента, що поєднує інженерну точність із когнітивною гнучкістю для забезпечення безпеки життєдіяльності.

Актуальність розробки підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» зумовлена стрімкою цифровізацією побутового простору та ускладненням інженерних мереж, що потребує автоматизованого контролю в режимі реального часу. Сучасне помешкання насичене великою кількістю енергоємних приладів, розгалуженими системами водопостачання та газозабезпечення, де найменша несправність або вихід параметрів за межі норми можуть призвести до

катастрофічних наслідків, таких як пожежі, затоплення чи вибухи. У сучасному помешканні критично важливо забезпечити не просто моніторинг, а здатність системи миттєво ідентифікувати аномалії в роботі електромереж, водопостачання чи газового обладнання ще на стадії зародження проблеми, що дозволяє уникнути катастрофічних наслідків, таких як пожежі або затоплення.

Традиційні методи та засоби захисту, що базуються на автономних датчиках без централізованого інтелектуального управління, часто виявляються недостатніми, оскільки вони лише констатують факт аварії, не маючи можливості вчасно її попередити або мінімізувати збитки через превентивні дії. Впровадження кіберфізичних підходів дозволяє об'єднати фізичні процеси з обчислювальними алгоритмами, забезпечуючи не тільки моніторинг, а й глибокий аналіз даних для прогнозування потенційних загроз ще до їх фактичного виникнення, перетворюючи пасивне спостереження на активне запобігання через автоматичне перекриття клапанів чи знеструмлення небезпечних ділянок. Особливої ваги це набуває в умовах нестабільної роботи енергосистем та зростання ризиків техногенного характеру, де швидкість реакції системи вимірюється мілісекундами, що критично для збереження життя мешканців та цілісності майна.

Крім того, актуальність підсистеми підкріплюється економічним аспектом, адже вартість ліквідації наслідків аварій значно перевищує витрати на розробку та впровадження інтелектуальних засобів захисту, які здатні самостійно перекрити подачу води чи газу в разі витоку. Розвиток технологій Інтернету речей та штучного інтелекту відкриває нові можливості для створення адаптивних систем, що здатні до самонавчання на основі поведінкових патернів користувачів, що робить таку підсистему фундаментом безпеки сучасного інтелектуального житла шляхом розпізнавання найменших відхилень від норми, які людина може не помітити.

Соціальна значущість підсистеми полягає у створенні безпечного та комфортного середовища для вразливих груп населення, таких як люди похилого віку або особи з обмеженими можливостями, для яких автоматизоване запобігання аваріям є життєво необхідною функцією, перетворюючи «Розумний будинок» з просто комфортного середовища на надійний інтелектуальний щит, здатний до самостійної діагностики та оперативного реагування в екстремальних умовах.

Таким чином, створення ефективної підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» є пріоритетним завданням, що відповідає сучасним тенденціям розвитку безпечних будинків та інтелектуальних систем життєзабезпечення.

Огляд відомих рішень щодо виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»

Проведемо огляд відомих методів та рішень щодо виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок».

Якщо надзвичайна ситуація трапляється вдома у літньої людини, яка проживає сама, початок надання невідкладної допомоги може бути відкладено, що призводить до ще гірших наслідків для цієї групи населення. Розумні системи екстреного виклику вдома (HECS) можуть виявляти падіння та автоматично запускати екстрений сигнал тривоги, потенційно скорочуючи час до надання невідкладної допомоги та покращуючи результати. Окрім стандартної системи HECS з базовою станцією та портативним радіопередавачем, розумна система HECS включає датчики, які можуть виявляти падіння та автоматично вмикати сигнал тривоги [15, 16].

У статті [17] описано системи, спеціально розроблені для підвищення безпеки та незалежності людей з інвалідністю та людей похилого віку, які проживають вдома. Для таких людей негайна допомога в надзвичайній ситуації має вирішальне значення. Коротко обговорюється технічний стан систем екстреного виклику, спеціально розроблених для використання людьми похилого віку, зокрема добре відома радіокнопка екстреного виклику, за допомогою якої можна вручну активувати сигнал тривоги. Однак ця система не забезпечує належної безпеки у всіх надзвичайних ситуаціях. Тому пропонуються альтернативні або додаткові системи, призначені для автоматичного ввімкнення сигналу тривоги на основі запису та оцінки так званих життєво важливих параметрів. Крім того, в середовищі «Розумного будинку» з мережевими пристроями можна використовувати додаткові параметри – так звані параметри середовища. Виявлено, що ідентифікація надзвичайної ситуації стає більш надійною зі збільшенням кількості використовуваних параметрів.

Для літніх людей, які живуть самі, технічні рішення для виявлення надзвичайних ситуацій є важливими для швидкого отримання допомоги, коли це необхідно. Автори [18] представляють новий метод виявлення надзвичайних ситуацій у приватних домогосподарствах, який виявляє надзвичайно тривалі періоди бездіяльності та може обробляти помилкову або невизначену інформацію про активність. Вводиться показник неактивності, який забезпечує ймовірнісне зважування періодів бездіяльності на основі надійності вимірювань датчиків. Аналізуючи історичні показники неактивності, можна виявити аномалії, які потенційно представляють собою надзвичайну ситуацію.

Захист житлових районів все ще здійснюється за допомогою охоронців, які контролюють стан кожного будинку. Однак охоронці можуть охороняти лише зовнішню частину будинку, не знаючи про умови всередині. Тим часом система «Розумного будинку» є однією з технологій, яка продовжує розвиватися для моніторингу умов у будинку. У роботі [19] створено систему, яка може фактично контролювати стан кожного будинку, шляхом інтеграції технології та використання трьох основних датчиків – датчиків вогню, газу та руху. Ця система має переваги з точки зору встановлення гнучкого обладнання, яке можна налаштувати відповідно до потреб. Крім того, охоронці також можуть дізнаватися про умови в кожному будинку, а також отримувати актуальні сповіщення через розроблений застосунок. Система в будинку здатна надсилати інформацію про умови в ньому під час активації, включаючи небезпечні умови для активації сигналізації. З тестування обладнання видно, що чутливість вузла датчика вогню сильно залежить від кольору вогню, величини пожежі та відстані виявлення. Крім того, вузли датчиків газу можуть забезпечити швидку реакцію, якщо їх встановити поблизу джерела витоку.

У статті [20] описується проектування та впровадження пристрою Інтернету речей на базі ESP32-S3, який інтегрує моніторинг безпеки газу в режимі реального часу з голосовим помічником на базі штучного інтелекту, що забезпечує покращений зворотний зв'язок з користувачем та розмовний контекст. Основною метою системи є поєднання голосової взаємодії в режимі "вільні руки" з великою мовною моделлю (LLM) та реальним виявленням газу MQ-2 для моніторингу безпеки навколишнього середовища. Прототип продемонстрував надійну продуктивність в обробці голосових запитів з контекстною пам'яттю та моніторингом навколишнього середовища. Ця робота ілюструє економічно ефективний та адаптивний підхід до розробки багатофункціональних рішень шляхом поєднання ESP 32 із сучасними хмарними сервісами штучного інтелекту та комплексними механізмами зворотного зв'язку з користувачами. Одночасно система проводить моніторинг навколишнього середовища за допомогою газового датчика MQ-2. При виявленні рівня газу, що перевищує заздалегідь визначений поріг, система запускає локальне голосове сповіщення через свій динамік, активує зумер та надсилає сповіщення через Telegram та мобільну панель керування Blynk, забезпечуючи своєчасне локальне та віддалене сповіщення.

В останні роки прогрес у технологіях «Розумного будинку» підкреслив необхідність розробки систем раннього виявлення пожежі та диму для підвищення безпеки та захисту. Традиційні методи виявлення пожежі, що базуються на теплових або димових датчиках, мають обмеження щодо часу реагування та адаптивності до навколишнього середовища. Для вирішення цих проблем у статті [21] представлено модель багатомасштабного інформаційного трансформатора–DETR (MITI-DETR), яка включає багатомасштабну ідентифікацію ознак на основі трансформатора, спеціально розроблені для виявлення пожежі в розумних будинках. Ця робота пропонує надійне рішення для раннього виявлення пожежі в розумних будинках, поєднуючи високу точність з можливістю розгортання в режимі реального часу.

Проєкт, описаний у [22], мав на меті впровадити застосування інтелектуальної пожежної сигналізації Arduino в реальних життєвих ситуаціях. Проєкт розпочався з дослідження та проєктування архітектури системи перед створенням прототипу. Далі відбувалась розробка прототипу з використанням відповідних датчиків. Далі відбувалось програмування системи, де команди записуються у вигляді коду та виконуються для запуску прототипу. Було проведено чотири експерименти для перевірки ефективності прототипу пристрою, призначеного для моніторингу температури, вологості та концентрації газу в навколишньому середовищі. Система використовує різні датчики для виявлення пожеж та реагування на них у режимі реального часу, швидко їх локалізуючи та сповіщаючи служби екстреної допомоги. Запропонований метод є економічно ефективним та пропонує ефективне рішення для запобігання пожежам у «Розумних будинках».

Дослідження [23] зосереджено на розробці мобільного застосунку для системи «Розумного будинку» на базі Інтернету речей, здатного керувати побутовою технікою та подавати сигнал тривоги у разі пожежі та витоку газу. Дослідники використовували безкоштовний інструмент для створення веб-застосунків під назвою MIT App Inventor для створення застосунку та його функцій. Також для підключення застосунку до системи «Розумного будинку» використовувалась хмарна база даних Firebase. Кінцевим продуктом дослідження став мобільний застосунок для Android-пристроїв, здатний вмикати або вимикати побутову техніку та діяти як сигнал тривоги у разі пожежі або витоку газу в будинку.

У статті [24] пропонується система «Розумного будинку» на основі нечіткої логіки, яка виявляє ймовірність пожежі та активує екстрені сповіщення та дії. Система інтегрує принципи нечіткої логіки з інтелектуальними методами сенсорного зондування та прийняття рішень, які зменшують небезпеку пожежі в режимі реального часу. Ефективність та надійність системи демонструються за допомогою експериментів та оцінки. Результати досліджень підкреслюють потенціал використання підходів на основі нечіткої логіки для підвищення безпеки житлових приміщень та зменшення кількості інцидентів, пов'язаних з пожежами.

У дослідженні [25] автори пропонують нову структуру федеративного навчання (FL) для вирішення проблеми швидкого виявлення диму під час пожежі на межі середовищ «Розумного будинку». Запропонована структура використовує три різні алгоритми FL для глобальної агрегації прогнозів машинного навчання на основі даних з різних датчиків Інтернету речей. Ця структура дозволяє здійснювати раннє прогнозування, використовуючи обчислювальні можливості на межі, тим самим покращуючи швидкість реагування та ефективність систем пожежної безпеки.

Автори [26] розробили ефективне рішення для виявлення пожежі в «Розумних будинках» за допомогою методів обробки зображень та машинного навчання. FireD витягує ознаки з фотографій та захоплених відеокадрів за допомогою згорткової нейронної мережі (CNN) та надсилає їх до нейронної мережі, яка реалізує алгоритм кластеризації, відомий як Yolov5, щоб забезпечити можливість класифікації зображень як з пожежею та без пожежі. Після виявлення пожежі модель надсилає зображення до хмари Heroku, яка служить контейнерною хмарною платформою як послуга (PaaS) для доступу, розгортання та управління зображеннями. Про виявлення пожежі сповіщення надсилається до Telegram через Telegram-бот.

У роботі [27] представлено системну модель проєктування та впровадження системи пожежної сигналізації, інтегрованої з Інтернетом речей (IoT) для раннього виявлення пожежі та реагування. Основною метою цієї роботи є покращення заходів пожежної безпеки шляхом використання технології IoT для виявлення пожеж на ранніх стадіях, що дозволяє оперативно діяти, мінімізуючи пошкодження майна та рятуючи життя. Запропонована система включає кілька датчиків, стратегічно розміщених у середовищі розумного будинку, для постійного контролю температури, рівня диму та CO. Реалізована модель включає ряд датчиків разом з візуальним індикатором на OLED та гучним зумером для попередження мешканців про потенційну пожежну небезпеку. Крім того, система запускає автоматичну систему водяного спринклера для гасіння пожежі на попередніх стадіях. Інтеграція технології IoT дозволяє здійснювати моніторинг у режимі реального часу та дистанційний доступ до системи пожежної сигналізації. Зібрані дані з датчиків можуть бути передані на централізовану станцію моніторингу або доступні через мобільний застосунок, що полегшує дистанційний моніторинг, аналіз та контроль пожежної небезпеки. Результати дослідження демонструють потенціал системи пожежної сигналізації на базі IoT у покращенні заходів пожежної безпеки.

Аналіз сучасних методів та рішень у сфері виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» свідчить про перехід від простих автономних датчиків до комплексних інтелектуальних систем, які поєднують моніторинг фізичних параметрів із просунутою аналітикою. Особлива увага в дослідженнях приділяється створенню систем екстреного виклику, що є критично важливим для безпеки літніх людей та осіб з інвалідністю. Розробки охоплюють широкий спектр технологій – від ймовірнісного зважування сенсорних даних до інтеграції голосових помічників на базі великих мовних моделей (LLM) та мультисенсорних вузлів для контролю витоків газу й вогню. Сучасні архітектури все частіше використовують мобільні застосунки та хмарні сервіси, такі як Telegram або Blynk, для миттєвого

віддаленого сповіщення користувачів та охоронних структур про виникнення загрози. Важливим вектором розвитку є впровадження методів штучного інтелекту, зокрема нечіткої логіки, федеративного навчання та згорткових нейронних мереж (CNN) для візуального розпізнавання пожеж у реальному часі. Використання моделей типу MITI-DETR або алгоритмів Yolov5 дозволяє значно підвищити точність детектування диму та вогню, мінімізуючи хибні спрацьовування та скорочуючи час реакції порівняно з традиційними тепловими детекторами. Крім того, спостерігається тенденція до створення закритих циклів реагування, де система не лише сповіщає про небезпеку, а й самостійно активує виконавчі механізми, такі як автоматичні спринклерні системи гасіння. Таким чином, сучасні кіберфізичні рішення трансформуються у когнітивні екосистеми, що здатні до багаторівневого аналізу середовища, забезпечуючи високу стійкість житла до техногенних та побутових аварій.

Аналіз існуючих рішень дозволяє виділити кілька критичних недоліків, які обмежують їхнє масове впровадження та ефективність у реальних умовах. Головним бар'єром залишається висока вартість інтелектуальних систем, особливо тих, що використовують складні нейромережеві моделі, дороге серверне обладнання або спеціалізовані когнітивні датчики, що робить повну автоматизацію безпеки недоступною для пересічного споживача. Крім того, більшість представлених на ринку та в наукових працях рішень мають вузькоспеціалізований характер, зосереджуючись на вирішенні лише однієї конкретної проблеми – наприклад, виключно на пожежній сигналізації. Такий фрагментарний підхід змушує власників житла встановлювати кілька незалежних підсистем від різних виробників, які часто несумісні між собою, створюють надмірне навантаження на мережу та потребують окремого обслуговування.

Саме тому постає гостра науково-технічна потреба у розробці єдиної комплексної підсистеми, яка б функціонувала як цілісний організм у межах кіберфізичного простору. Актуальним є створення універсального рішення, здатного одночасно здійснювати прецизійний моніторинг множини критичних параметрів – концентрації природного та чадного газів, появи диму, несанкціонованих витоків води, а також фіксації аномальних температурних коливань. Така багатофункціональність дозволить не лише знизити загальну вартість володіння системою, а й забезпечить синергетичний ефект, коли дані з одного датчика (наприклад, температури) допомагають підтвердити показники іншого (наприклад, диму), суттєво підвищуючи достовірність виявлення аварійних ситуацій. Проєктування такої комплексної підсистеми і є метою даного дослідження.

Вибір апаратних складових підсистеми

Для побудови комплексної підсистеми важливо обрати датчики, які поєднують точність, довговічність та прийнятну ціну.

Датчики чадного газу (CO) працюють на різних принципах – напівпровідникові (дешевші, але споживають більше енергії) та електрохімічні (високоточні, ідеальні для автономних систем). У Таблиці 1 представлені результати порівняльного аналізу датчиків чадного газу.

Таблиця 1

Порівняльний аналіз датчиків чадного газу

Модель датчика	Тип	Діапазон вимірювання (ppm)	Переваги	Недоліки	Орієнтовна вартість
MQ-7	Напівпровідниковий	10 – 1000	Дуже низька ціна, простота підключення до Arduino/ESP32	Потребує циклічного нагріву, високе енергоспоживання, чутливий до вологості	Низька

MQ-9	Напівпровідниковий	10 – 1000	Комбінований – реагує на CO та горючі гази (CH4, LPG)	Менша точність саме по чадному газу порівняно з MQ-7	Низька
MG-811	Електрохімічний / Хімічний	350 – 10000	Висока чутливість, стабільність роботи	Висока ціна, складніша схема підключення	Середня
ME2-CO	Електрохімічний	0 – 1000	Висока точність, лінійна залежність сигналу, низьке енергоспоживання	Обмежений термін служби електроліту (2-5 років)	Середня
FIGARO TGS5042	Електрохімічний	0 – 10000	Промисловий стандарт, висока селективність, довгий термін служби (до 10 років)	Висока вартість, потребує якісної обв'язки	Висока

Для розробки бюджетної, але надійної системи «Розумного будинку» для широкого вжитку, оптимальним вибором є MQ-7 (для прототипів та систем з живленням від мережі). Оскільки метою є побудова комплексної системи, то більше підходять датчики серії MQ, які мають схожу логіку підключення, що спростить проєктування плати для моніторингу газу, диму та витоків одночасно.

Для моніторингу природного газу (метану CH4) найчастіше використовують напівпровідникові датчики, які змінюють свій опір при контакті з молекулами газу. Оскільки метан легший за повітря, при проєктуванні системи слід враховувати, що ці датчики мають розміщуватися у верхній частині приміщення. У Таблиці 2 наведені результати порівняльного аналізу датчиків природного газу, які найкраще підходять для інтеграції в кіберфізичну систему «Розумний будинок».

Таблиця 2

Порівняльний аналіз датчиків природного газу

Модель датчика	**Тип**	**Діапазон детектування (ppm)**	**Особливості**	**Енергоспоживання**	**Вартість**
MQ-4	Напівпровідниковий (SnO_2)	200 – 10000	Висока чутливість саме до метану (CH4), низька чутливість до диму	Високе	Низька
MQ-5	Напівпровідниковий	200 – 10000	Більш універсальний – реагує на метан та пропан-бутан (LPG)	Високе	Низька

MQ-9	Напівпровідниковий	100 – 10000	Гібридний – виявляє метан та чадний газ, проте з меншою точністю порівняно з MQ-7	Середнє	Низька
TGS2611	Напівпровідниковий	500 – 10000	Висока селективність до метану, компактний розмір	Середнє	Висока
MiCS-5524	MEMS (напівпровідниковий)	1000 – 10000	Сучасна технологія, дуже компактний, придатний для портативних пристроїв	Низьке	Середня

MQ-4 є «золотим стандартом» для бюджетних комплексних систем безпеки. Його головна перевага – вузька спеціалізація на метані, що зменшує кількість хибних спрацьовувань, коли на кухні готується їжа або використовуються миючі засоби. MQ-5 доцільно обирати лише в тому випадку, якщо в будинку використовується і природний газ (магістральний), і балонний (пропан), оскільки він ефективно «бачить» обидва види палива. TGS2611 рекомендується для систем преміум-класу, де пріоритетом є довговічність та стабільність показань без частих калібрувань. Отже, для нашої підсистеми оберемо в якості датчику прирожного газу саме датчик MQ-4.

Для комплексної системи безпеки вибір датчика диму є критичним, оскільки саме вони відповідають за раннє виявлення пожежі. У сучасних кіберфізичних системах використовуються переважно два типи – іонізаційні (швидко реагують на відкрите полум'я) та оптичні/фотоелектричні (краще розпізнають тління та густий дим). У Таблиці 3 представлені результати порівняльного аналізу датчиків диму, які можна інтегрувати в систему «Розумний будинок».

Таблиця 3

Порівняльний аналіз датчиків диму

Модель датчика	**Тип**	**Чутливість**	**Переваги**	**Недоліки**	**Вартість**
MQ-2	Напівпровідниковий	Дим, LPG, пропан, водень	Універсальність, дуже низька ціна, простота обробки сигналу	Високе енергоспоживання	Низька
GP2Y1010AU0F	Оптичний (інфрачервоний)	Дрібні частки пилу та диму	Дуже низьке енергоспоживання, компактність, висока швидкість реакції	Потребує захисту від зовнішнього світла, чутливий до звичайного пилу	Середня

MAX30105	Оптичний (Particle Sensor)	Дим, дихання, частки	Надзвичайна точність (використовує ІЧ, червоний та зелений світлодіоди)	Складний протокол зв'язку (I2C), вища ціна	Висока
MQ-303A	Напівпровідниковий (MEMS)	Дим, пари спирту	Мініатюрний розмір, низьке енергоспоживання порівняно з серією MQ	Менша площа контакту з повітрям, потребує калібрування	Середня
DSM501A	Оптичний	Дим, пил (PM2.5)	Здатний розрізняти розмір часток	Габаритний корпус, потребує вертикального встановлення	Середня

MQ-2 – це оптимальний вибір для комплексного бюджетного рішення, оскільки він дозволяє одним модулем «закрити» питання і диму, і витоку горючих газів. Це значно здешевлює конструкцію, що відповідає вимозі щодо подолання дороговизни існуючих систем. Якщо ж пріоритетом є точність та уникнення хибних спрацювань, варто інтегрувати оптичний датчик типу GP2Y1010AU0F або DSM501A. Вони аналізують фізичну наявність часток у повітрі, а не хімічний склад, що робить їх надійнішими. Отже, для нашої підсистеми оберемо в якості датчику диму саме датчик MQ-2.

Для комплексної системи безпеки датчик витоку води є одним із найпростіших, але водночас критично важливих елементів. На відміну від газових сенсорів, вони зазвичай споживають мінімум енергії, оскільки працюють за принципом замикання контактів через провідне середовище (воду). У Таблиці 4 представлені результати порівняльного аналізу датчиків витоку води, які допоможуть запобігти затопленню.

Таблиця 4

Порівняльний аналіз датчиків витоку води

Модель датчика	**Тип**	**Принцип роботи**	**Переваги**	**Недоліки**	**Вартість**
HW-038 (Rain/Water Level)	Контактний (резистивним)	Вимірювання опору	Надзвичайно низька ціна, сумісність з усіма мікроконтролерами	Швидка корозія контактів (електроліз), потребує частої заміни	Дуже низька
YI-S (Зондовий)	Контактний (щуповий)	Два металеві щупи, що замикаються водою	Стійкість до корозії, легкість очищення, довговічність	Потребує безпосереднього контакту з калюжею певної глибини	Низька
Non-contact (Безконтактний)	Ємнісний	Виявлення води через стінку труби або резервуара	Не контактує з водою (немає корозії), висока надійність	Складніше налаштувати для виявлення розливу на підлозі	Середня

Optical Liquid Level	Оптичний	Відбиття/заломлення світла всередині призми	Висока точність, миттєва реакція, працює роками	Складніший у монтажі на пласкі поверхні (підлогу)	Середня
XKC-Y25-T12V	Індуктивний / Ємнісний	Детектування рідини без прямого контакту	Безпека (немає оголених дротів), ідеально для агресивних середовищ	Чутливий до товщини поверхні, через яку «дивиться»	Висока

Найдешевшим є датчик HW-038, проте для реальної експлуатації в «Розумному будинку» він не підходить через швидке руйнування контактів під дією струму та вологи. Тому оптимальним вибором для комплексної підсистеми є зондові датчики (YI-S) з нержавіючими щупами або контактними пластинами, покритими золотом/нікелем. Вони дешеві, надійні та легко інтегруються в загальний аналітичний модуль. Щоб уникнути помилкових тривог через високу вологість, у програмне забезпечення комплексної системи варто додати алгоритм перевірки – сигнал вважається аварійним лише тоді, коли рівень сигналу з датчика тримається стабільно високим протягом 1-2 секунд.

Для комплексної системи безпеки датчик температури відіграє подвійну роль – він не лише забезпечує клімат-контроль, а й слугує критичним верифікатором пожежі. Якщо датчик диму фіксує задимлення, а температурний сенсор одночасно показує стрімке зростання температури більше 60°C, система може з майже 100% впевненістю ідентифікувати реальну пожежу, уникаючи помилкових тривог. В Таблиці 5 представлені результати порівняльного аналізу датчиків температури, придатних для детектування аномальних температур.

Таблиця 5

Порівняльний аналіз датчиків температури

Модель датчика	**Тип**	**Діапазон температур**	**Точність**	**Переваги для системи безпеки**	**Вартість**
DHT11 / DHT22	Цифровий (містить ємнісний сенсор вологості)	-40°C ... +80°C	±0.5 - 2°C	Вимірює і вологість, низька ціна	Низька
DS18B20	Цифровий (1-Wire)	-55°C ... +125°C	±0.5°C	Герметичний корпус (можна занурювати у воду), висока перешкодостійкість	Середня
LM35	Аналоговий	-55°C ... +150°C	±0.25°C	Пряма лінійна залежність 10 мВ/1°C, надзвичайно швидка реакція	Низька
BMP280 / BME280	Цифровий (I2C)	-40°C ... +85°C	±1°C	Додатково вимірює тиск, що дозволяє фіксувати зворотну тягу в димоходах	Середня

MLX90614	ІЧ-пірометр (безконтактний)	-70°C ... +380°C	±0.5°C	Дистанційне виявлення джерел тепла (може «побачити» вогонь здалеку)	Висока

Для виявлення (верифікації) пожежі найкращим вибором є DS18B20. Завдяки цифровому інтерфейсу 1-Wire, можна підключити десятки таких датчиків до одного піна мікроконтролера, розмістивши їх у кожній кімнаті. Його здатність працювати до +125°C дозволяє системі продовжувати передавати дані навіть у розпал аварії.

Для інтеграції обраного набору датчиків (MQ-7, MQ-4, MQ-2, YI-S та DS18B20) контролер повинен мати достатню кількість аналогових входів (для серії MQ) та цифрових інтерфейсів, а також підтримувати бездротовий зв'язок для миттєвого сповіщення користувача. У Таблиці 6 представлені результати порівняльного аналізу популярних платформ для створення кіберфізичних систем.

Таблиця 6

Порівняльний аналіз контролерів

Характеристика	**Arduino Uno (R3/R4)**	**ESP8266 (NodeMCU)**	**ESP32 (DevKit V1)**	**STM32 (Black Pill)**	**Raspberry Pi Zero 2 W**
Процесор	ATMega328P (8-біт)	ESP8266 (32-біт)	Dual-core (32-біт)	Cortex-M4	ARM Cortex-A53
Аналогові входи (ADC)	6 (10-біт)	1 (10-біт)	15+ (12-біт)	10 (12-біт)	Немає (потрібен АЦП)
Бездротовий зв'язок	Немає	Wi-Fi	Wi-Fi + Bluetooth	Немає	Wi-Fi + Bluetooth
Енергоспоживання	Низьке	Середнє	Середнє (є Deep Sleep)	Низьке	Високе
Обсяг пам'яті (Flash)	32 KB	4 MB	4 MB - 16 MB	512 KB	Залежить від SD-карти
Вартість	Низька	Дуже низька	Низька/Середня	Середня	Висока (дефіцит)

Для нашої комплексної підсистеми найкращим вибором є ESP32, оскільки він має велику кількість АЦП для датчиків MQ-7, MQ-4, MQ-2, що видають аналоговий сигнал. На відміну від ESP8266 (де вхід лише один) або Arduino (де їх 6, але низька розрядність), ESP32 дозволяє підключити всі газові датчики одночасно з високою точністю зчитування. ESP32 має вбудований Wi-Fi та Bluetooth, що є критично важливим для «Розумного будинку», оскільки не потрібно купувати додаткові модулі, щоб надсилати сповіщення про витоки газу чи пожежу на смартфон через мобільний застосунок або протокол MQTT. ESP32 має двоядерний процесор, який дозволяє розділити завдання – одне ядро займається постійним опитуванням датчиків у реальному часі, а інше – обробкою Wi-Fi з'єднання та шифруванням даних. ESP32 відмінно працює з протоколом 1-Wire (датчик DS18B20), тобто датчик температури можна підключити до будь-якого вільного цифрового піна. При високій потужності ESP32 залишається доступним за ціною, що відповідає концепції подолання дороговизни систем безпеки.

Для комплексної підсистеми кіберфізичної системи «Розумний будинок», яка базується на контролері ESP32 та групі датчиків безпеки, вибір стандарту передачі даних є критичним. Система має бути надійною,

працювати в реальному часі та легко інтегруватися з мобільними пристроями. У Таблиці 7 представлені результати порівняльного аналізу основних стандартів передачі даних.

Таблиця 7

Порівняльний аналіз стандартів передачі даних

Стандарт	Радіус дії	Енергоспоживання	Пропускна здатність	Переваги	Недоліки
Wi-Fi (IEEE 802.11)	Середній (30-50 м)	Високе	Дуже висока	Пряме підключення до роутера та інтернету, не потрібен хаб	Залежність від стабільності роутера, енергозалежність
Zigbee / Z-Wave	Середній (10-100 м)	Дуже низьке	Низька	Стійка mesh-мережа, ідеально для датчиків на батарейках	Потребує спеціальний шлюз (Gateway), вища ціна модулів
Bluetooth LE (BLE)	Малий (10-20 м)	Низьке	Середня	Економний, прямий зв'язок зі смартфоном	Обмежений радіус дії, складно керувати віддалено без шлюзу
LoRaWAN	Великий (до 5-15 км)	Дуже низьке	Дуже низька	Величезна дальність, робота в підвалах/бетонних спорудах	Повільна передача даних, складна інфраструктура

Для розроблюваної підсистеми оптимальним рішенням є використання протоколу MQTT (Message Queuing Telemetry Transport), що працює поверх Wi-Fi. Оскільки обраний контролер ESP32 вже має вбудований Wi-Fi модуль, це дозволяє реалізувати систему без додаткових витрат на шлюзи (як у випадку з Zigbee). Це повністю відповідає вимозі щодо бюджетності рішення. Wi-Fi забезпечує достатню швидкість для передачі великої кількості даних від багатьох датчиків одночасно. Протокол MQTT – це «золотий стандарт» для IoT-систем завдяки своїм особливостям: легкість (протокол мінімізує обсяг переданих даних, що важливо для швидкої реакції системи), надійність (MQTT має рівні якості обслуговування (QoS – Quality of Service); наприклад, для датчика газу можна встановити рівень «QoS 1», який гарантує, що повідомлення про аварію точно дійде до користувача), модель «Видавець-Підписник» (датчики публікують дані в певні «топіки» (наприклад, home/safety/gas), а смартфон або сервер негайно отримує їх), затримка передачі даних складає мілісекунди, що критично для запобігання пожежам чи вибухам.

На основі проведеного аналізу можна зробити висновок, що сформований перелік апаратних засобів є оптимальним для створення комплексної, бюджетної та високоефективної підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок». Обрана конфігурація дозволяє подолати головні недоліки існуючих рішень - їхню високу вартість та вузьку спеціалізацію. Використання лінійки датчиків MQ-7, MQ-4 та MQ-2 у поєднанні з DS18B20 та YI-S дозволяє системі одночасно контролювати п'ять критичних загроз – чадний газ, природний газ, задимлення, аномально висока температура та витоки води. Це

перетворює підсистему з простого детектора на повноцінний когнітивний вузол безпеки. Комбінація датчика диму MQ-2 та прецизійного термометра DS18B20 реалізує принцип перехресної перевірки. Це мінімізує кількість хибних спрацювань, що є ключовим показником надійності для кіберфізичних систем. Вибір ESP32 як обчислювального центру є найбільш виправданим. Завдяки вбудованому 12-бітному АЦП для точного зчитування аналогових сигналів газу та інтегрованому Wi-Fi модулю, контролер забезпечує високу швидкість обробки даних та миттєву передачу тривожних сигналів без потреби в дорогому додатковому обладнанні. Використання стандарту Wi-Fi у поєднанні з протоколом MQTT гарантує низьку затримку (low latency) та високу надійність доставки повідомлень (QoS). Це критично для систем реального часу, де кожна секунда зволікання при аварії може мати серйозні наслідки.Застосування напівпровідникових та резистивних сенсорів у поєднанні з доступним контролером ESP32 робить підсистему в кілька разів дешевшою за промислові аналоги, зберігаючи при цьому необхідний рівень точності для побутового використання.

Отже, запропонований апаратний стек створює надійний фундамент для підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок», яка здатна адаптуватися до мінливих умов середовища, забезпечувати автономний захист житла та надавати користувачу повний контроль над безпекою через сучасні цифрові канали зв'язку.

Підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»

Отже, основні елементи підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»:

1) датчик чадного газу MQ-7;
2) датчик природного газу MQ-4;
3) датчик диму MQ-2;
4) датчик витоку води YI-S;
5) датчик аномально високих температур DS18B20;
6) контролер ESP32;
7) стандарт передачі даних – протокол MQTT, що працює поверх Wi-Fi.

Архітектура підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» складається з локального рівня – контролер ESP32 збирає дані з датчиків MQ-7, MQ-4, MQ-2, DS18B20 та YI-S, протоколу передачі – MQTT-клієнт на ESP32, хмарного/локального брокера – Mosquitto або безкоштовні хмарні сервіси (Adafruit IO, HiveMQ), кінцевий пристрій – смартфон із мобільним застосунком.

На нижньому рівні відбувається безпосереднє зчитування параметрів навколишнього середовища обраними датчиками. Ці фізичні компоненти збирають первинну інформацію, яка є основою для подальшого аналізу.

Зібрані дані передаються на середній рівень, центральним елементом якого є контролер ESP32. Контролер виконує роль мосту та первинного процесора – він отримує дані від датчиків. Після первинної обробки та перевірки, контролер використовує Wi-Fi-зв'язок та протокол MQTT для ефективної передачі даних на верхній рівень, що забезпечує мінімальний мережевий трафік та надійну інтеграцію у мережу будинку. Для всіх критично важливих повідомлень, що стосуються імплементації рішень, було встановлено рівень якості обслуговування QoS 1 (At least once).

На верхньому рівні розміщуються методи прийняття рішень та керування, які є аналітичним ядром та модулем ситуаційного аналізу підсистеми. Тут відбувається фінальний аналіз отриманих комплексних даних – застосовуються методи для розпізнавання поточних ситуацій та для визначення оптимальних дій відповідно до заздалегідь заданих правил, що містяться в розділі правил бази знань. Завершальним етапом роботи підсистеми є виконання необхідних дій в автоматичному режимі, спрямованих на попередження та запобігання аварійним ситуаціям. Це включає сповіщення користувача, перекривання подачі води/газу, сповіщення екстрених рятувальних служб тощо.

Спроєктуємо архітектуру підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» – рис. 1.

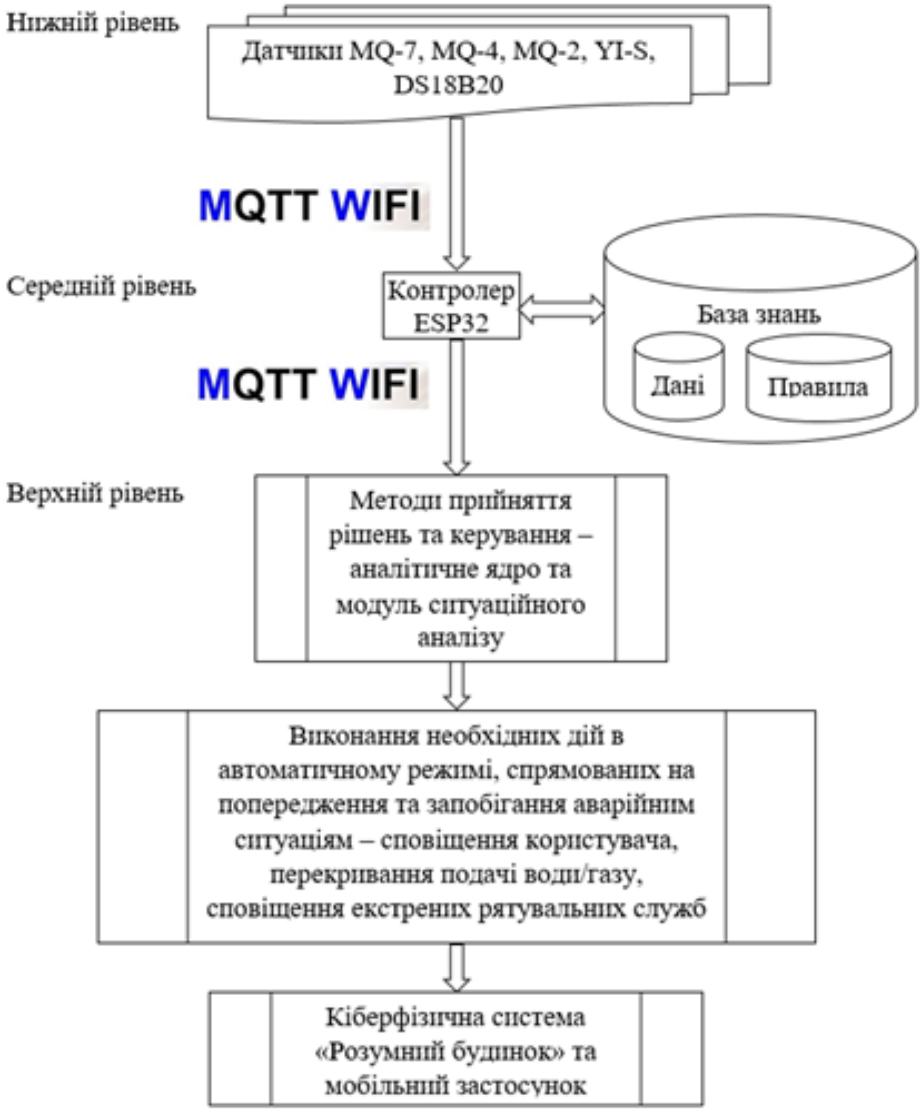


Рис. 1. Архітектура підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок»

Розроблена підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» забезпечує високий рівень безпеки завдяки комплексній інтеграції різнопланових сенсорів та алгоритмів обробки даних у реальному часі. Головними перевагами такої архітектури є її багатофункціональність, що дозволяє одночасно контролювати витоки газів, води та виникнення пожеж, а також економічна доступність за рахунок використання контролера ESP32 та недорогих напівпровідникових датчиків. Використання протоколу MQTT з рівнем якості QoS 1 гарантує надійність доставки критичних повідомлень, а багаторівнева структура прийняття рішень мінімізує вплив людського фактора та забезпечує оперативне автоматичне реагування на загрози. Разом з тим, система має певні обмеження, пов'язані із залежністю від стабільності Wi-Fi-з'єднання та необхідністю регулярного калібрування напівпровідникових сенсорів серії MQ, які схильні до деградації з часом і чутливі до змін вологості повітря. Проте, завдяки впровадженню методів ситуаційного аналізу та перехресної верифікації даних, підсистема трансформує житловий простір у когнітивне середовище, здатне ефективно запобігати техногенним аваріям та забезпечувати надійний захист майна і життя мешканців.

Висновки

Розроблена підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» є ефективним та економічно доступним рішенням, яке долає обмеження

вузькоспеціалізованих і дорогих аналогів. Завдяки інтеграції лінійки датчиків MQ-7, MQ-4, MQ-2, DS18B20 та YI-S під керуванням контролера ESP32, система забезпечує прецизійний моніторинг одночасно п'яти критичних загроз – витоків природного та чадного газів, появи диму, несанкціонованих витоків води та аномальних температурних коливань. Використання багаторівневої архітектури та протоколу MQTT поверх Wi-Fi з рівнем якості QoS 1 гарантує надійну передачу даних у реальному часі та оперативне автоматичне реагування на небезпеку, включаючи сповіщення користувача та перекриття відповідних комунікацій. Попри певні обмеження, пов'язані із залежністю від стабільності мережевого з'єднання та необхідністю калібрування сенсорів, впровадження методів ситуаційного аналізу та перехресної верифікації даних дозволяє трансформувати житловий простір у безпечне когнітивне середовище, що є життєво важливим для захисту мешканців, зокрема вразливих груп населення.

Література

1. Resilient Distributed Optimization for Multi-Agent Cyberphysical Systems / M. Yemini et al. *IEEE Transactions on Automatic Control*. 2025. P. 1–16. URL: https://doi.org/10.1109/tac.2025.3532791.
2. Explainable AI for Cyber-Physical Systems: Issues and Challenges / A. Hoenig et al. *IEEE Access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3395444.
3. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook / S. J. Oks et al. *Information Systems Frontiers*. 2022. URL: https://doi.org/10.1007/s10796-022-10252-x.
4. Fuada S., Hendriyana H. UPISmartHome V.2.0 – A Consumer Product of Smart Home System with an ESP8266 as the Basis. *Journal of Communications*. 2022. P. 541–552. URL: https://doi.org/10.12720/jcm.17.7.541-552.
5. Sung W.-T., Hsiao S.-J. Creating Smart House via IoT and Intelligent Computation. *Intelligent Automation & Soft Computing*. 2023. Vol. 35, no. 1. P. 415–430. URL: https://doi.org/10.32604/iasc.2023.027618.
6. Smart Home Personal Assistants: Fueled by Natural Language Processor and Blockchain Technology / S. A. Ansar et al. *2022 Second International Conference on Interdisciplinary Cyber Physical Systems (ICPS)*, Chennai, India, 9–10 May 2022. 2022. URL: https://doi.org/10.1109/icps55917.2022.00029.
7. Yaici W., Entchev E., Longo M. Internet of Things (IoT)-Based System for Smart Home Heating and Cooling Control. 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), Prague, Czech Republic, 28 June – 1 July 2022. 2022. URL: https://doi.org/10.1109/eeeic/icpseurope54979.2022.9854634.
8. Harnessing Real-Time Data for Intelligent Decision-Making in Cyber-Physical Systems / T. Premavathi et al. *Advances in Computer and Electrical Engineering*. 2024. P. 257–286. URL: https://doi.org/10.4018/979-8-3693-5728-6.ch010.
9. Azeri N., Hioual O., Hioual O. Towards an Approach for Modeling and Architecting of Self-Adaptive Cyber-Physical Systems. *2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, Oum El Bouaghi, Algeria, 12–13 October 2022. 2022. URL: https://doi.org/10.1109/pais56586.2022.9946921.
10. Cognitive architecture for cognitive cyber-physical systems / J. Al Haj Ali et al. *IFAC-PapersOnLine*. 2024. Vol. 58, no. 19. P. 1180–1185. URL: https://doi.org/10.1016/j.ifacol.2024.09.099.
11. Kluge T. A role-based architecture for self-adaptive cyber-physical systems. *SEAMS '20: IEEE/ACM 15th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, Seoul Republic of Korea. New York, NY, USA, 2020. URL: https://doi.org/10.1145/3387939.3391601.
12. Nota G., Petraglia G. Heritage buildings management: the role of situational awareness and cyber-physical systems. *Journal of Ambient Intelligence and Humanized Computing*. 2024. URL: https://doi.org/10.1007/s12652-023-04750-2.
13. Edge-Computing-Driven Internet of Things: A Survey / L. Kong et al. *ACM Computing Surveys*. 2022. URL: https://doi.org/10.1145/3555308.

14. Design Procedure for Real-Time Cyber–Physical Systems Tolerant to Cyberattacks / C. M. Paredes et al. *Symmetry*. 2024. Vol. 16, no. 6. P. 684. URL: https://doi.org/10.3390/sym16060684.

15. Assessing the effectiveness and cost-effectiveness of a smart home emergency call system: study protocol for a randomised controlled trial in Germany / H. Rehse et al. *BMJ Open*. 2025. Vol. 15, no. 4. P. e092893. URL: https://doi.org/10.1136/bmjopen-2024-092893.

16. Smart Assistance of Elderly Individuals in Emergency Situations at Home / A. R. Reddy et al. *Internet of Things*. Cham, 2021. P. 95–115. URL: https://doi.org/10.1007/978-3-030-63937-2_6.

17. Personennotrufsysteme auf Basis menschlicher vital- und systemtechnischer Parameter in einer Smart-Home-Umgebung / Emergency-call Systems Based on Human Vital and System-technical Parameters in a Smart-home Environment / M. Hampicke et al. *Biomedizinische Technik/Biomedical Engineering*. 2002. Vol. 47, no. 11. P. 278–284. URL: https://doi.org/10.1515/bmte.2002.47.11.278.

18. Wilhelm S., Wahl F. Emergency Detection in Smart Homes Using Inactivity Score for Handling Uncertain Sensor Data. *Sensors*. 2024. Vol. 24, no. 20. P. 6583. URL: https://doi.org/10.3390/s24206583.

19. Pramunanto E., Muhtadin M., Febrian W. Integrated Smart Safety Home System based on Wireless Sensor Network and Internet of Things as Emergency Preventive Efforts in Settlement Areas. *2019 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, Surabaya, Indonesia, 19–20 November 2019. 2019. URL: https://doi.org/10.1109/cenim48368.2019.8973328.

20. Şevik R., Demirci R., Yılmaz Y. IoT-Powered Voice Interaction and Proactive Gas Leak Detection System for Smart Homes with Embedded Gas Sensing and Instant AI Alerts. *2025 Innovations in Intelligent Systems and Applications Conference (ASYU)*, Bursa, Turkiye, 10–12 September 2025. 2025. P. 1–8. URL: https://doi.org/10.1109/asyu67174.2025.11208502.

21. A Multi-Scale Approach to Early Fire Detection in Smart Homes / A. Abdusalomov et al. *Electronics*. 2024. Vol. 13, no. 22. P. 4354. URL: https://doi.org/10.3390/electronics13224354.

22. Development of Arduino based smart home fire alarm system with emergency SOS notification / K. R. Rajinran et al. *PROCEEDINGS OF 5TH INTERNATIONAL CONFERENCE ON SUSTAINABLE INNOVATION IN ENGINEERING AND TECHNOLOGY 2023*, Kuala Lumpur, Malaysia. 2024. P. 020103. URL: https://doi.org/10.1063/5.0229532.

23. Paglinawan C. C., Bagunu R. A. D., Castillo S. T. Mobile Application for IoT-Based Smart Home System for Appliance Control and Fire Alert. *2024 16th International Conference on Computer and Automation Engineering (ICCAE)*, Melbourne, Australia, 14–16 March 2024. 2024. URL: https://doi.org/10.1109/iccae59995.2024.10569777.

24. Chrysafiadi K., Tsichrintzi E.-A., Sakkopoulos E. A smart home fuzzy logic-based cooking fire prevention system addressing human errors due to distraction or minor medical memory lapses. *Procedia Computer Science*. 2024. Vol. 246. P. 3390–3399. URL: https://doi.org/10.1016/j.procs.2024.09.218.

25. A Trustable Federated Learning Framework for Rapid Fire Smoke Detection at the Edge in Smart Home Environments / A. N. Patel et al. *IEEE Internet of Things Journal*. 2024. P. 1. URL: https://doi.org/10.1109/jiot.2024.3439228.

26. Fired:An Image-Based Fire Detector for Smart Homes using Machine Learning Algorithms / G. M. Srinath et al. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, Chikkaballapur, India, 18–19 April 2024. 2024. P. 1–4. URL: https://doi.org/10.1109/ickecs61492.2024.10616511.

27. Debnath S., Gautam J., Rai S. K. IoT Based Smart Home and Office Fire Notification Alert System. *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Gwalior, India, 14–16 March 2024. 2024. URL: https://doi.org/10.1109/iatmsi60426.2024.10503336.

References

1. Resilient Distributed Optimization for Multi-Agent Cyberphysical Systems / M. Yemini et al. IEEE Transactions on Automatic Control. 2025. P. 1–16.

2. Explainable AI for Cyber-Physical Systems: Issues and Challenges / A. Hoenig et al. IEEE Access. 2024. P. 1.

3. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook / S. J. Oks et al. Information Systems Frontiers. 2022.

4. Fuada S., Hendriyana H. UPISmartHome V.2.0 – A Consumer Product of Smart Home System with an ESP8266 as the Basis. Journal of Communications. 2022. P. 541–552.

5. Sung W.-T., Hsiao S.-J. Creating Smart House via IoT and Intelligent Computation. Intelligent Automation & Soft Computing. 2023. Vol. 35, no. 1. P. 415–430.

6. Smart Home Personal Assistants: Fueled by Natural Language Processor and Blockchain Technology / S. A. Ansar et al. 2022 Second International Conference on Interdisciplinary Cyber Physical Systems (ICPS), Chennai, India, 9–10 May 2022. 2022.

7. Yaici W., Entchev E., Longo M. Internet of Things (IoT)-Based System for Smart Home Heating and Cooling Control. 2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), Prague, Czech Republic, 28 June – 1 July 2022. 2022.

8. Harnessing Real-Time Data for Intelligent Decision-Making in Cyber-Physical Systems / T. Premavathi et al. Advances in Computer and Electrical Engineering. 2024. P. 257–286.

9. Azeri N., Hioual O., Hioual O. Towards an Approach for Modeling and Architecting of Self-Adaptive Cyber-Physical Systems. 2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS), Oum El Bouaghi, Algeria, 12–13 October 2022. 2022.

10. Cognitive architecture for cognitive cyber-physical systems / J. Al Haj Ali et al. IFAC-PapersOnLine. 2024. Vol. 58, no. 19. P. 1180–1185.

11. Kluge T. A role-based architecture for self-adaptive cyber-physical systems. SEAMS '20: IEEE/ACM 15th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, Seoul Republic of Korea. New York, NY, USA, 2020.

12. Nota G., Petraglia G. Heritage buildings management: the role of situational awareness and cyber-physical systems. Journal of Ambient Intelligence and Humanized Computing. 2024.

13. Edge-Computing-Driven Internet of Things: A Survey / L. Kong et al. ACM Computing Surveys. 2022.

14. Design Procedure for Real-Time Cyber–Physical Systems Tolerant to Cyberattacks / C. M. Paredes et al. Symmetry. 2024. Vol. 16, no. 6. P. 684.

15. Assessing the effectiveness and cost-effectiveness of a smart home emergency call system: study protocol for a randomised controlled trial in Germany / H. Rehse et al. BMJ Open. 2025. Vol. 15, no. 4. P. e092893.

16. Smart Assistance of Elderly Individuals in Emergency Situations at Home / A. R. Reddy et al. Internet of Things. Cham, 2021. P. 95–115.

17. Personennotrufsysteme auf Basis menschlicher vital- und systemtechnischer Parameter in einer Smart-Home-Umgebung / Emergency-call Systems Based on Human Vital and System-technical Parameters in a Smart-home Environment / M. Hampicke et al. Biomedizinische Technik/Biomedical Engineering. 2002. Vol. 47, no. 11. P. 278–284.

18. Wilhelm S., Wahl F. Emergency Detection in Smart Homes Using Inactivity Score for Handling Uncertain Sensor Data. Sensors. 2024. Vol. 24, no. 20. P. 6583.

19. Pramunanto E., Muhtadin M., Febrian W. Integrated Smart Safety Home System based on Wireless Sensor Network and Internet of Things as Emergency Preventive Efforts in Settlement Areas. 2019 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM), Surabaya, Indonesia, 19–20 November 2019. 2019.

20. Şevik R., Demirci R., Yılmaz Y. IoT-Powered Voice Interaction and Proactive Gas Leak Detection System for Smart Homes with Embedded Gas Sensing and Instant AI Alerts. 2025 Innovations in Intelligent Systems and Applications Conference (ASYU), Bursa, Turkiye, 10–12 September 2025. 2025. P. 1–8.

21. A Multi-Scale Approach to Early Fire Detection in Smart Homes / A. Abdusalomov et al. Electronics. 2024. Vol. 13, no. 22. P. 4354.

22. Development of Arduino based smart home fire alarm system with emergency SOS notification / K. R. Rajimon et al. PROCEEDINGS OF 5TH INTERNATIONAL CONFERENCE ON SUSTAINABLE INNOVATION IN ENGINEERING AND TECHNOLOGY 2023, Kuala Lumpur, Malaysia. 2024. P. 020103.

23. Paglinawan C. C., Bagunu R. A. D., Castillo S. T. Mobile Application for IoT-Based Smart Home System for Appliance Control and Fire Alert. 2024 16th International Conference on Computer and Automation Engineering (ICCAE), Melbourne, Australia, 14–16 March 2024. 2024.

24. Chrysafiadi K., Tsichrintzi E.-A., Sakkopoulos E. A smart home fuzzy logic-based cooking fire prevention system addressing human errors due to distraction or minor medical memory lapses. Procedia Computer Science. 2024. Vol. 246. P. 3390–3399. U

25. A Trustable Federated Learning Framework for Rapid Fire Smoke Detection at the Edge in Smart Home Environments / A. N. Patel et al. IEEE Internet of Things Journal. 2024. P. 1.

26. Fired:An Image-Based Fire Detector for Smart Homes using Machine Learning Algorithms / G. M. Srinath et al. 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chikkaballapur, India, 18–19 April 2024. 2024. P. 1–4.

27. Debnath S., Gautam J., Rai S. K. IoT Based Smart Home and Office Fire Notification Alert System. 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 14–16 March 2024. 2024.

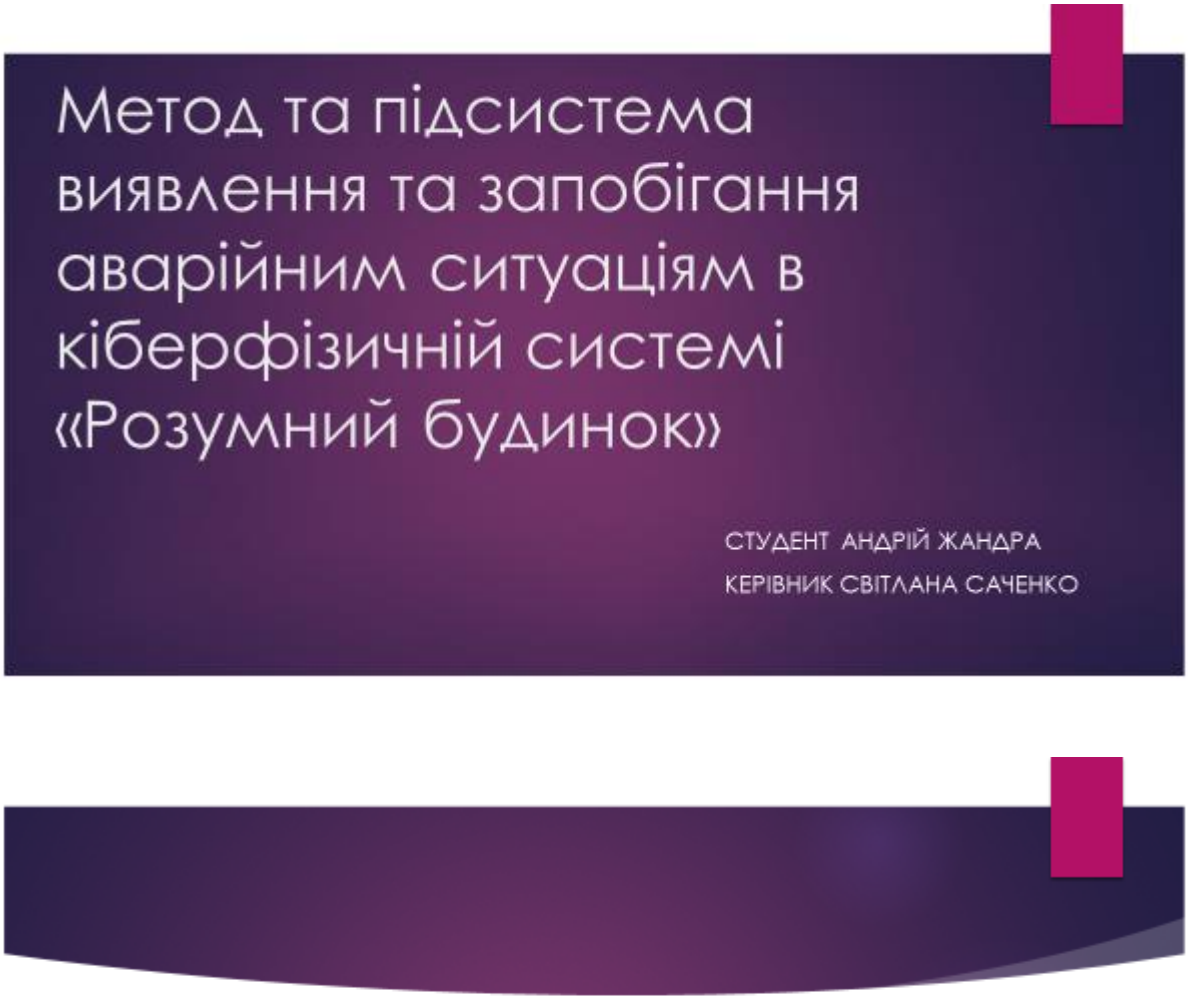
Рецензія / Peer review:

Надрукована / Printed:

Рецензент: д.т.н., проф., професор кафедри КІС ХНУ О. С. Савенко

ДОДАТОК Б
(обов'язковий)

ПРЕЗЕНТАЦІЯ ДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ



- **Мета кваліфікаційної роботи** – автоматизація процесу виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», зокрема, автоматизація процесу виявлення витоків чадного газу, природного газу, води, виявлення диму, аномально високих температур.
- **Об'єкт дослідження** – процес виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»
- **Предмет дослідження** – метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

- **Наукова новизна отриманих результатів:** розроблено метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», що відрізняється від існуючих аналогів прецизійним моніторингом одночасно п'яти критичних загроз – витоків природного та чадного газів, появи диму, несанкціонованих витоків води та аномальних температурних коливань та забезпечує виконання необхідних дій в автоматичному режимі, спрямованих на попередження та запобігання аварійним ситуаціям (сповіщення користувача, перекривання подачі води/газу, сповіщення екстрених рятувальних служб тощо).
- **Практична значущість отриманих результатів** полягає у реалізації підсистеми виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок», яка забезпечує високий рівень безпеки завдяки комплексній інтеграції різнопланових сенсорів та алгоритмів обробки даних у реальному часі.

Публікація

За темою кваліфікаційної роботи опублікована одна стаття у фаховому науковому журналі України категорії Б:

Войчур Ю.О., Медзатий Д.М., Жандра А.Я. Підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». Вісник Хмельницького національного університету. Серія «Технічні науки». 2026. №1. С. _____.

Постановка задачі

Для розроблення методу та підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» слід розв'язати такі задачі:

- аналіз відомих методів та рішень для виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;
- вибір компонентів для підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;
- розроблення методу та алгритму функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;
- розроблення архітектури підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»;
- проведення експериментів із використанням розробленої підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

Вибір датчиків для нижнього рівня підсистеми

Датчик CO чадного газу MQ-7 5B

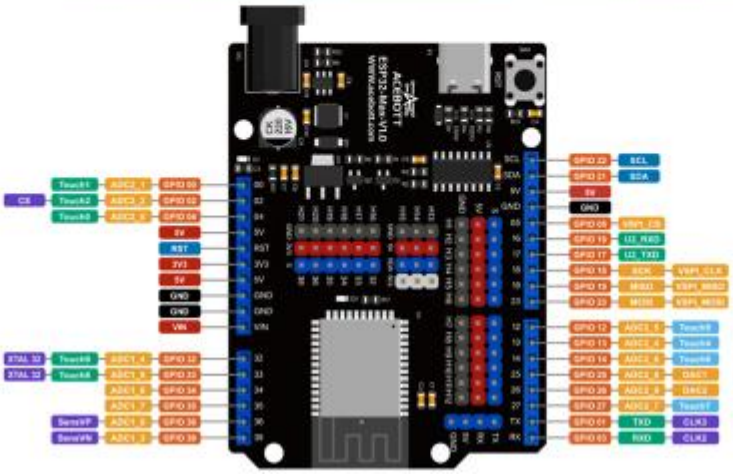
Датчик природного газу MQ-4

Датчик диму MQ-2

Датчик витоку води WL400 Water Level Sensor

Датчик детектування аномальної температури DS18B20

Вибір компонентів для середнього рівня підсистеми



Сценарії роботи підсистеми та реагування підсистеми

Множина основних сценаріїв роботи підсистеми:

$$SDPE = \{ sdpe_1, .., sdpe_8 \} = \{ ngld, rcmp, cmlrt, nglrt, srt, wld, ao, lc \}$$

де ngld – виявлення витоку природного газу (датчик MQ-4 фіксує концентрацію метану (CH4) вище заданого безпечного порогу (> 1000 ppm)), rcmp – загроза отруєння чадним газом (датчик MQ-7 детектує підвищення рівня чадного газу, що часто трапляється при несправності пічного опалення або камінів), …

Множина відповідних сценаріїв реагування підсистеми:

$$CRS = \{ crs_1, .., crs_{15} \} = \{ iscap, lava, somgv, aowv, isha, iscaf, ses, deab, aafs, iscafl, acsvw, nufh, apco, sadmm, mlfpa \}$$

де iscap – негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Небезпека отруєння», lava – активація локальної звукової та світлової сигналізації, …

Метод виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»:

1) етап первинного сенсорного моніторингу – безпосереднє зчитування параметрів навколишнього середовища за допомогою обраних датчиків - циклічно з частотою кілька разів на секунду, що забезпечує миттєву ідентифікацію аномалій ще на стадії їх зародження;

2) етап збору та попередньої обробки даних – зібрані дані передаються на середній рівень, де центральним елементом виступає контролер ESP32;

3) етап комунікаційної передачі – після первинної обробки контролер використовує мережеві протоколи (Wi-Fi та MQTT) для ефективної передачі даних на верхній аналітичний рівень;

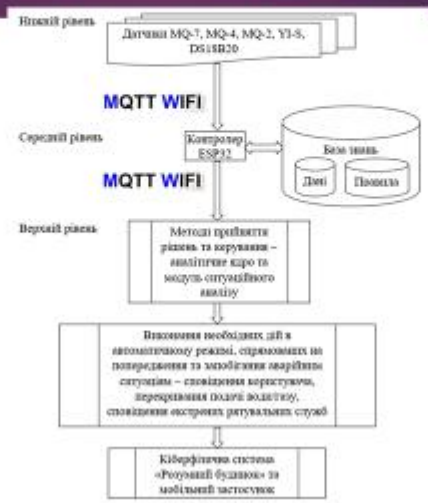
4) етап ситуаційного аналізу та прийняття рішень – фінальний аналіз отриманих комплексних даних та застосовуються методи для розпізнавання поточних ситуацій;

5) етап автоматичного реагування та запобігання – виконання необхідних дій в автоматичному режимі, спрямованих на нейтралізацію загрози:

- якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію sdpe1 = ngld, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: crs1 = iscap, crs2 = lava, crs3 = somgv, crs4 = aowv, crs5 = isha;
- …
- якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію sdpe8 = lc, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: crs14 = sadmm, crs15 = mlfpa;

5) етап адаптації та зворотного зв'язку – завдяки здатності до самонавчання, система накопичує дані про зовнішні впливи та звички користувачів.

Архітектура підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»



Приклад функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

В певний момент часу підсистема виявлення та запобігання аварійним ситуаціям у кіберфізичній системі «Розумний будинок» виявила одночасну появу диму та збільшення температури – датчик MQ-2 зафіксував задимлення та датчик DS18B20 одночасно зареєстрував стрімке зростання температури понад 60°C.

Згідно з розробленим правилом, якщо підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виявила спрацювання сценарію sdpe5 = srt, то підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» виконує такі сценарії реагування: crs6 = iscaf, crs7 = ses, crs8 = deab, crs9 = aafs, crs2 = lava, тобто відбувається негайне надсилання критичного сповіщення на смартфон користувача через MQTT з позначкою «Пожежа», відбувається надсилання сигналу екстреним службам (через хмарні сервіси або Telegram-бот), відбувається знеструмлення відповідної зони будинку для запобігання коротким замиканням, відбувається активація автоматичної системи пожежогасіння (спринклерів) у зоні займання, а також відбувається активація локальної звукової та світлової сигналізації.

ВИСНОВКИ

Дана кваліфікаційна робота забезпечила автоматизацію процесу виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», зокрема, автоматизацію процесу виявлення витоків чадного газу, природного газу, води, виявлення диму, аномально високих температур.

У розділі 1 кваліфікаційної роботи проведений аналіз відомих методів та рішень для виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

У розділі 2 здійснений вибір компонентів для підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

У розділі 3 кваліфікаційної роботи розроблені метод та алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

У розділі 4 спроєктовано підсистему виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

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

Назва кваліфікаційної роботи Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»
Автор Жандра Андрій Ярославович
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: Саченко Світлана Іванівна, к.е.н., доцент

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	

Підтвердження:

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

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 7,08% і адресується до 34 першоджерела; та системою Anti-Plagiarism складає 17%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

20.04.2026

Завідувач кафедри _____ Підпис — Ольга ПАВЛОВА (Ім'я, ПРІЗВИЩЕ)

Гарант освітньої програми _____ Підпис — Олег САВЕНКО (Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи _____ Підпис — Світлана САЧЕНКО (Ім'я, ПРІЗВИЩЕ)

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Андрій ЖАНДРА
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

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

20 квітня 2026 року

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 ЖАНДРА

Співавтор:

Назва: Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок»

Експерт: Світлана САЧЕНКО

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:7.08%

Коефіцієнт подібності 2:2.31%

Мікропробіли: 3

Заміна букв: 1

Інтервали: 0

Білі знаки: 1

Дата створення звіту: 2026-04-20 11:36:58.0

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:

2026-04-20 Доцент Андрій Нічепорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Жандра Андрій Ярославович

Тема: Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі "Розумний будинок"

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість сторінок записки _____

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є автоматизація процесу виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок», зокрема, автоматизація процесу виявлення витоків чадного газу, природного газу, води, виявлення диму, аномально високих температур.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У розділі 1 кваліфікаційної роботи проведений аналіз відомих методів та рішень для виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». У розділі 2 здійснений вибір компонентів для підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». У розділі 3 кваліфікаційної роботи розроблені метод та алгоритм функціонування підсистеми виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок». У розділі 4 спроєктовано підсистему виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок».

4. Позитивні сторони роботи: розроблення методу та архітектури підсистеми кіберфізичної системи

5. Негативні сторони роботи: мало уваги приділено формалізації підсистеми

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно з діючими стандартами оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на середньому науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: добре/B (85).

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Федорчук Павло Петрович

зав. кафедрою ІПЗ, ХНУ

"21" квітня 2026 р. _____(підпис)

Mon Apr 20 11:58:40 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 17.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 14%**

	Документ		Сумарний збіг по Базі Даних	
ID: 270548 Назва: МКР Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі «Розумний будинок» Додано в БД: 2026-04-20 Автора: Андрій ЖАНДРА Керівники: Світлана САЧЕНКО Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	155292	961	28105 (18%)	203 (21%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми
269860	Назва: Звіт з НДП Метод та підсистема виявлення та запобігання аварійним ситуаціям в кіберфізичній системі “Розумний будинок” Додано в БД: 2026-03-18 Автора: Жандри А.Я. Керівники: Саченко С.І. Консультанти: Опоненти:	26762 (17.0%)	187 (19.0%)