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

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Інтелектуальна система контролю та безпеки для системи "Розумного будинку"»

КвРКІП. 303200.23.03.55 ПЗ

Виконав: студент 2 курсу, група КІ2м-23-3 Олександр КОНДРАТЮК
Підпис Ім'я, прізвище

Керівник к.т.н., доцент Андрій НІЧЕПОРУК
Науковий ступінь, вчене звання Підпис Ім'я, прізвище

До захисту допускаю:
Зав. кафедри КІІС, доктор філософії, доцент
Ольга ПАВЛОВА
22 05 2025 р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітньо-наукова програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 01 " 09 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Олександру КОНДРАТЮКУ

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Інтелектуальна система контролю та безпеки для системи "Розумного будинку"

Керівник проекту (роботи) Андрій НІЧЕПОРУК, к.т.н., доцент

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

Затверджена наказом ректора університету від 08.01.2025 №8

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2025 р.

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

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

Огляд відомих методів і засобів контролю та безпеки для системи "Розумного будинку"

Модель системи контролю та безпеки для системи "Розумного будинку"

Система контролю та безпеки для системи "Розумного будинку"

Моделювання системи контролю та безпеки для системи "Розумного будинку"

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

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня
Нормоконтроль	Сергій ЛИСЕНКО, професор кафедри КІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІС		

7. Дата видачі завдання «_01_»_____09_____2024р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітк
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	01.09.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.10.2024	виконан
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	01.11.2024	виконан
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	01.12.2024	виконан
5	Робота над науковою статтею	01.02.2025	виконан
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2025	виконан
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.04.2025	виконан
8	Оформлення пояснювальної записки згідно вимог	18.04.2025	виконан
9	Попередній захист ДРМ	29.04.2025	виконан
10	Захист ДРМ на засіданні ЕК	До 15.05.2025	

Студент Підпис Олександр КОНДРАТЮК
Ім'я, прізвище

Керівник роботи Підпис Андрій НІЧЕПОРУК
Ім'я, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Інтелектуальна система контролю та безпеки для системи "Розумного будинку"

Автор роботи: Олександр КОНДРАТЮК

Керівник роботи: Андрій НІЧЕПОРУК

Пояснювальна записка: 71 с., 32 рис., 2 табл., 2 дод., 24 джерел.

ІОТ, МЕТОД, РОЗУМНИЙ БУДИНОК, БЕЗПЕКА, КОНТРОЛЬ, ІНТЕЛЕКТУАЛЬНА.

Об’єктом дослідження є процеси автоматизованого моніторингу та реагування на події в умовах інтелектуального середовища «розумного будинку».

Предметом дослідження є методи побудови та реалізації інтелектуальної системи розпізнавання загроз на основі даних сенсорів та відеоаналізу з використанням технологій IoT, машинного навчання та хмарних платформ.

Метою кваліфікаційної роботи магістра є розробка, реалізація та експериментальна перевірка інтелектуальної системи безпеки для «розумного будинку», яка поєднує засоби збору даних, обробки зображень, класифікації подій та інтерфейс взаємодії з користувачем у реальному часі.

Для розв’язання поставлених задач використовувалися методи аналізу й моделювання кіберфізичних систем, алгоритми машинного навчання (зокрема метод опорних векторів), принципи побудови IoT-архітектур, засоби хмарних обчислень, а також методи експериментального дослідження для оцінювання ефективності реалізованого прототипу.

Наукова новизна отриманих результатів:

− набув подальшого розвитку метод виявлення загроз у середовищі «розумного будинку» на основі використання алгоритмів машинного навчання, зокрема методу опорних векторів (SVM), адаптованого до умов обмежених ресурсів вбудованих систем та змінного середовища функціонування;;

− набула подальшого розвитку інформаційна технологія інтеграції сенсорної мережі, модулів відеоаналізу та мобільного інтерфейсу користувача із

застосуванням хмарної інфраструктури Firebase, що забезпечує надійну синхронізацію даних, обробку подій у реальному часі та зворотний зв’язок із користувачем.

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення що реалізують повноцінний цикл безпеки: від фіксації потенційної загрози та її класифікації до генерації відповідної реакції та інформування користувача. Запропонована система відзначається адаптивністю до зовнішніх впливів, масштабованістю та можливістю гнучкого налаштування сценаріїв реагування.

Практична значимість отриманих результатів полягає у її здатності забезпечити комплексний, адаптивний та надійний підхід до моніторингу подій у середовищі «розумного будинку». Система не лише фіксує потенційні загрози, а й автоматично класифікує їх, реагує відповідно до заданого сценарію та надає користувачу змогу втручатись у процес прийняття рішень.

Було реалізовано повний функціональний цикл: від зчитування сенсорних даних та обробки зображень, до виведення результатів класифікації в мобільному застосунку й формування інтерактивних сповіщень. Користувач може переглядати історію подій, реагувати на тривоги, змінювати налаштування та керувати пристроями дистанційно. Таким чином, система не лише працює автономно, а й підтримує гнучку інтеграцію з поведінкою користувача.

Окремо варто відзначити її стійкість до збоїв - реалізовано механізми локального збереження інформації у випадку втрати зв’язку з мережею, кешування кадрів, повторної синхронізації з хмарною платформою. Це забезпечує цілісність і безперервність процесу моніторингу навіть за нестабільного інтернет-з’єднання або короткочасних технічних перебоїв.

Система створена на основі відкритих і доступних технологій, таких як ESP32-CAM, Firebase та Flutter, що робить її легко відтворюваною, недорогою та масштабованою. Це відкриває широкі можливості її впровадження як у навчальних, дослідницьких, так і в практичних комерційних цілях. Застосування механізмів машинного навчання для класифікації загроз підвищує точність

реагування та забезпечує можливість подальшого вдосконалення системи через самонавчання.

Запропоноване рішення відповідає актуальним вимогам до безпеки в середовищі IoT, є технічно завершеним і водночас гнучким для подальшої адаптації, що підтверджує його практичну значущість у сучасних умовах цифрової трансформації побутового простору.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АПЗ - антивірусне програмне забезпечення

БД - база даних

БПР - блок прийняття рішень

ГА - генетичний алгоритм

ОС - операційна система

ПЗ - програмне забезпечення

СВВ - система виявлення вторгнень

ЕС - експертна система

DDoS - Distributed Denial of Service (розподілена відмова в обслуговуванні)

IDS - система виявлення вторгнень

ВСТУП

Розвиток сучасних інформаційних технологій, зокрема Інтернету речей (IoT), штучного інтелекту та автоматизованих систем управління, призвів до значних змін у підходах до забезпечення безпеки житлових і комерційних приміщень. Одним із перспективних напрямів у цій сфері є концепція "розумного будинку", яка передбачає інтеграцію різних пристроїв і систем для створення єдиного середовища, що забезпечує комфорт, енергоефективність та високий рівень безпеки. У зв’язку з цим зростає потреба у розробці інтелектуальних систем контролю та безпеки, які не лише виконуватимуть функцію охорони, а й забезпечуватимуть адаптивність до змін середовища та аналіз загроз у режимі реального часу.

Забезпечення безпеки у "розумному будинку" є багатокомпонентним завданням, яке охоплює фізичний захист приміщення, запобігання несанкціонованому доступу, моніторинг небезпечних ситуацій, таких як витік газу, пожежа або затоплення, а також кібербезпеку для захисту персональних даних користувачів. Традиційні методи охорони поступово втрачають ефективність через потребу у постійному контролі з боку людини та обмежену інтеграцію з іншими технологіями. У зв’язку з цим виникає необхідність розробки автоматизованих рішень, що здатні забезпечити комплексний підхід до безпеки, використовуючи сучасні алгоритми аналізу загроз та інноваційні технології.

Сучасні технології дозволяють створювати інтелектуальні системи безпеки на основі сенсорних мереж, алгоритмів машинного навчання, хмарних обчислень та криптографічних методів захисту даних. Такі рішення дають змогу не лише відстежувати стан приміщення, а й аналізувати поведінкові фактори, прогнозувати потенційні загрози та автоматично реагувати на небезпечні ситуації. Інтеграція IoT дозволяє створювати розподілені мережі пристроїв, які працюють у єдиній екосистемі та забезпечують ефективну взаємодію між різними елементами системи безпеки.

Актуальність теми дослідження зумовлена зростаючими вимогами до безпеки житлових та комерційних об’єктів, а також необхідністю інтеграції сучасних технологій у системи контролю доступу та моніторингу. В умовах підвищеної загрози кібератак та зростаючої кількості підключених до Інтернету пристроїв важливо розробити систему, яка не лише контролюватиме фізичні параметри безпеки, а й забезпечуватиме захист інформаційних потоків. Важливою складовою безпеки є можливість гнучкого налаштування та адаптації системи до потреб користувача, що дозволяє створювати персоналізовані сценарії захисту на основі отриманих даних та аналізу ризиків.

Об’єктом дослідження є процеси контролю та безпеки для системи "Розумного будинку".

Предметом дослідження є інтелектуальна система контролю та безпеки для системи "Розумного будинку".

Метою кваліфікаційної роботи магістра є підвищення ефективності контролю та безпеки системи "Розумного будинку" шляхом застосування інтелектуальної системи.

Наукова новизна отриманих результатів:

– набув подальшого розвитку метод розпізнавання загроз в інтелектуальній системі контролю та безпеки "Розумного будинку", який відрізняється від відомих поєднанням класичної сенсорної інфраструктури, алгоритмів машинного навчання, хмарної підтримки та локальної логіки реагування, що забезпечує виявлення небезпечних ситуацій у режимі реального часу та підвищує ефективність прийняття рішень.

– набула подальшого розвитку інтелектуальна система контролю та безпеки для системи "Розумного будинку", яка відрізняється від відомих залученням модуля реєстрації подій, що забезпечував збереження локальних логів і знімків, які в подальшому передавались до сховища Firebase, що дозволило підвищити ефективність контролю та безпеки у системі "Розумного будинку".

Практичне значення роботи полягає у можливості застосування розробленої системи в реальних умовах для підвищення рівня безпеки житлових і комерційних

приміщень. Запропонована система зможе інтегруватися з існуючими платформами "розумного будинку", що спрощує її впровадження та розширює сферу застосування. Крім того, результати цього дослідження можуть бути використані для подальшого вдосконалення інтелектуальних систем безпеки, розширення їх функціональності та впровадження новітніх стандартів кіберзахисту.

Таким чином, дана робота спрямована на дослідження сучасних підходів до безпеки "розумного будинку" та розробку інноваційного рішення, що відповідає сучасним викликам у сфері інформаційної безпеки та автоматизованого контролю доступу. Отримані результати можуть стати основою для розробки нових стандартів безпеки та інтеграції перспективних технологій у побутові та комерційні об’єкти.

1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ У СФЕРІ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

1.1 Огляд існуючих рішень

Забезпечення безпеки є одним із ключових аспектів системи "розумного будинку", оскільки користувачі очікують надійного захисту не лише фізичних об’єктів, а й цифрової інформації. Сучасні рішення у цій сфері базуються на традиційних підходах до охорони приміщень, а також на впровадженні інноваційних технологій, що поєднують автоматизацію, аналіз даних та інтеграцію з мобільними пристроями.

Традиційні системи безпеки включають механічні засоби захисту, такі як замки, дверні й віконні датчики, а також стандартні сигналізації. Вони мають низьку вартість, проте їхня ефективність обмежена, оскільки потребує активної участі користувача. Наприклад, звичайна сигналізація може лише сповіщати про проникнення, але не здатна аналізувати загрози чи запобігати інцидентам.

З розвитком технологій з’явилися більш досконалі рішення, такі як автоматизовані системи відеоспостереження, що використовують камери високої роздільної здатності, детектори руху та алгоритми розпізнавання облич. Такі системи дозволяють контролювати події у реальному часі та зберігати записані дані в хмарних сховищах для подальшого аналізу. Наприклад, популярні рішення від Nest Cam, Arlo та Hikvision дозволяють користувачам переглядати відео у реальному часі, а також отримувати миттєві сповіщення про рух або незвичайну активність у приміщенні.

Розвиток технологій Інтернету речей (IoT) сприяв створенню інтелектуальних систем моніторингу, які включають різні датчики (руху, температури, задимлення, витоку води чи газу), підключені до єдиної мережі. Вони забезпечують багаторівневий контроль за станом приміщення та дозволяють своєчасно реагувати на небезпечні події. Наприклад, Ring Alarm System, SimpliSafe та ADT Smart Security пропонують повноцінні комплекти безпеки, що включають

бездротові датчики руху, сенсори відкриття дверей і вікон та камери відеоспостереження, інтегровані у мобільні додатки.

Інтеграція безпеки з мобільними додатками відкриває нові можливості для управління системою. Завдяки підключенню до хмарних сервісів користувач може віддалено контролювати стан будинку, змінювати налаштування безпеки та отримувати миттєві сповіщення у разі загрози. Деякі сучасні системи підтримують інтеграцію з голосовими помічниками, що дозволяє керувати пристроями за допомогою голосових команд. Наприклад, Amazon Alexa Guard та Google Home Security дозволяють розумному будинку аналізувати звуки, такі як розбиття скла або сигналізація, і надсилати користувачу відповідні сповіщення.

Окрім фізичної безпеки, значну роль відіграє кібербезпека IoT-пристроїв, оскільки вони стають потенційними мішенями для хакерських атак. Наприклад, атака Mirai Botnet у 2016 році продемонструвала, наскільки вразливими можуть бути незахищені пристрої у розумних будинках. Для підвищення безпеки компанії, такі як Bitdefender, Norton та Kaspersky, пропонують спеціалізовані рішення для захисту IoT-систем від несанкціонованого доступу та потенційних загроз. Крім того, сучасні блокчейн-технології знаходять застосування у захисті мережевих транзакцій, що забезпечує більший рівень довіри до розумних систем безпеки.

Попри численні переваги сучасних систем, існує ряд викликів, серед яких висока вартість обладнання, складність інтеграції різних пристроїв, а також загрози кібератак. Недостатній рівень захисту IoT-пристроїв може призвести до витоку персональних даних або отримання несанкціонованого доступу до системи управління будинком. Тому важливим завданням є розробка більш надійних механізмів автентифікації, шифрування даних та захисту від кібератак. Дослідницькі компанії, такі як Cisco, IBM Security та McAfee, активно працюють над покращенням безпеки IoT-екосистем за рахунок інтегрованих рішень з використанням штучного інтелекту та глибокого аналізу загроз.

Сучасні розумні будинки використовують широкий спектр технологій для забезпечення контролю та безпеки, що дозволяє власникам зменшити ризики, пов’язані з несанкціонованим доступом, аварійними ситуаціями та іншими

загрозами. Базові рішення включають систему відеоспостереження, мережу датчиків руху, детекторів диму, витоку газу та води, а також інтелектуальні замки, що працюють у взаємодії із централізованими системами управління будинком.

Останні технологічні розробки дозволяють використовувати алгоритми штучного інтелекту для розпізнавання осіб, аналізу поведінки мешканців та прогнозування можливих загроз. Відеокамери з підтримкою нейромереж здатні виявляти підозрілу активність, автоматично ідентифікуючи мешканців будинку та сторонніх осіб. Додатково, інтегровані датчики можуть реагувати на зміну умов середовища, наприклад, автоматично вмикати систему оповіщення або блокувати доступ у разі виявлення небезпеки.

Хмарні технології та мобільні додатки відіграють важливу роль у сучасних системах безпеки, надаючи можливість віддаленого моніторингу та управління будинком у режимі реального часу. Власники можуть отримувати миттєві сповіщення про інциденти, переглядати відеозаписи та змінювати параметри роботи системи з будь-якої точки світу. Таким чином, сучасні рішення для контролю та безпеки не лише підвищують рівень захищеності житла, а й забезпечують зручність та ефективне управління ресурсами будинку.

Розвиток мережевих технологій дозволяє створювати комплексні системи, які інтегрують відеоспостереження, систему сигналізації, аналізатор трафіку та сенсори для виявлення руху. Одним із ключових елементів є використання IoT-пристроїв, які забезпечують обмін інформацією між компонентами безпеки та центральним керуючим модулем. Такі системи використовують бездротові мережі для зв’язку між датчиками та серверами обробки інформації, що дозволяє отримувати оперативні дані про стан приміщення та здійснювати необхідні дії у випадку виявлення загрози.

У сучасних розумних будинках активно застосовуються біометричні системи контролю доступу, які використовують розпізнавання відбитків пальців, обличчя або райдужної оболонки ока. Вони дозволяють суттєво підвищити рівень безпеки, оскільки доступ надається виключно авторизованим користувачам. Біометричні системи можуть бути інтегровані з мобільними додатками, що надає можливість

дистанційного керування доступом, перегляду історії відвідувань та оперативного блокування входу при необхідності.

Рисунок 1.1 - Біометричний зчитувач контролю доступу за відбитком пальця

Інтелектуальні системи відеоспостереження включають функції аналізу зображень у реальному часі, що дає змогу розпізнавати підозрілі дії, порівнювати збережені обличчя та запобігати можливим загрозам. Використання глибокого навчання дозволяє системі автоматично адаптуватися до змін у поведінці мешканців і налаштовувати алгоритми реагування на потенційні ризики.

Крім відеоспостереження та контролю доступу, важливу роль відіграють автоматизовані системи виявлення загроз. Системи моніторингу навколишнього середовища аналізують рівень вуглекислого газу, температури та вологості, а також здатні виявляти небезпечні гази, такі як чадний газ або витік природного газу. У разі виявлення критичної ситуації система може автоматично активувати вентиляцію, відключити газопостачання або надіслати повідомлення власнику та аварійним службам.

Додаткову безпеку забезпечують розумні замки та сигналізації, які працюють у зв’язці з мобільними додатками. Вони можуть повідомляти власника про кожну спробу доступу, фіксувати час та осіб, які здійснювали спроби входу, та надавати можливість дистанційного відкривання дверей або їхнього блокування. Розвиток технологій дозволяє інтегрувати такі системи з голосовими помічниками та

автоматизованими сценаріями, наприклад, відкривати двері лише після підтвердження власника через мобільний додаток або голосовий запит.

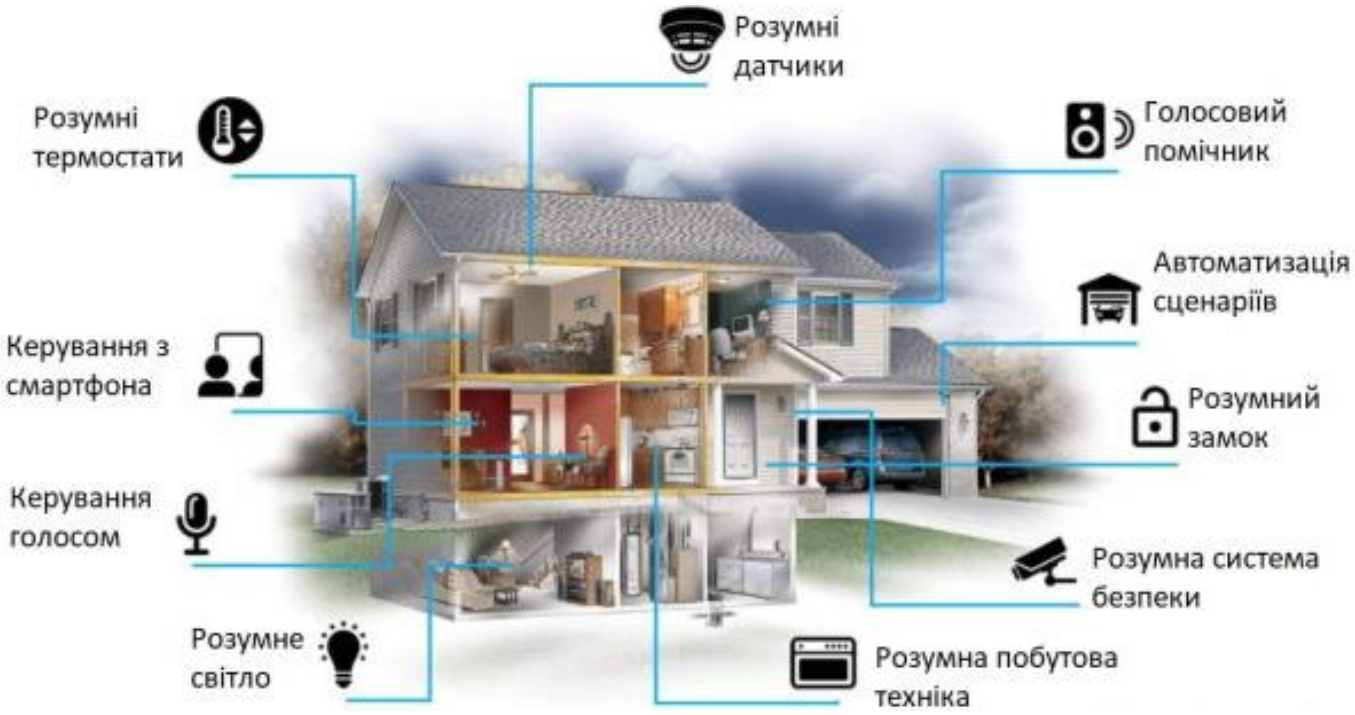

Рисунок 1.2 - Приклад автоматизованих системи у розумних будинках

На сучасному етапі розвитку технологій розумний будинок може використовувати комплексну систему безпеки, яка поєднує в собі різні рівні захисту, від фізичних бар'єрів до цифрових механізмів контролю. Важливою тенденцією є перехід від пасивних систем, які лише реагують на загрози, до активних рішень, що прогнозують потенційні ризики та мінімізують їхній вплив. Використання машинного навчання, нейромережевих алгоритмів та IoT дозволяє забезпечити високий рівень автоматизації та гнучкості системи контролю.

Значну увагу приділяють питанням кібербезпеки у розумних будинках. Оскільки всі пристрої пов'язані між собою через інтернет-з'єднання, вони стають потенційними мішенями для кібератак. Захист інформації та управління доступом є важливими аспектами для запобігання несанкціонованому втручанню. Використання передових методів шифрування, багаторівневої автентифікації та

регулярного оновлення програмного забезпечення дозволяє мінімізувати ризики зламу системи безпеки.

Системи безпеки розумного будинку є складними багаторівневими комплексами, що поєднують апаратне та програмне забезпечення для забезпечення максимальної ефективності. Завдяки використанню інноваційних технологій, вони дозволяють не лише контролювати доступ, а й запобігати небезпечним ситуаціям, аналізувати дані у реальному часі та вдосконалювати стратегії безпеки в залежності від змін середовища та поведінки користувачів.

Аналіз існуючих рішень показує, що сучасні технології дозволяють створювати ефективні системи безпеки для "розумного будинку", проте необхідно вирішити ряд проблем, пов’язаних з кіберзахистом, інтеграцією пристроїв та їх адаптивністю до змін середовища. У подальших підрозділах будуть розглянуті окремі аспекти безпеки, зокрема методи контролю доступу, технології відеоспостереження та питання кібербезпеки у системах розумного будинку.

1.2 Методи контролю доступу та ідентифікації користувачів

Контроль доступу у розумному будинку є критично важливим елементом загальної системи безпеки. Його метою є забезпечення безпечного входу та виходу з приміщення для авторизованих осіб і запобігання несанкціонованому доступу. Для досягнення цього завдання використовуються сучасні технології, що поєднують апаратне та програмне забезпечення, адаптивні алгоритми безпеки та інтелектуальні сенсорні системи.

Одним із найнадійніших підходів є використання біометричних систем ідентифікації. Ця технологія ґрунтується на унікальних фізіологічних характеристиках користувачів, які неможливо підробити або передати іншим особам. До таких методів належать розпізнавання відбитків пальців, сканування райдужної оболонки ока, розпізнавання обличчя та голосова ідентифікація. Наприклад, сучасні системи на базі Face ID Security Locks або Nest Hello використовують передові алгоритми машинного навчання для підвищення

точності розпізнавання, навіть в умовах слабкого освітлення. Важливим аспектом є безпека збереження біометричних даних, що забезпечується локальним зберіганням на пристрої або використанням зашифрованих хмарних сховищ. Системи розпізнавання відбитків пальців, такі як Ultraloq U-Bolt Pro, використовують мультиспектральний аналіз для точнішого визначення автентичності користувача.

Електронні системи доступу на основі RFID- та NFC-карток є поширеними завдяки своїй зручності та швидкості спрацьовування. Вони дозволяють зчитувати унікальні ідентифікаційні коди, що передаються через бездротовий зв’язок, відкриваючи двері лише для авторизованих користувачів. Наприклад, Yale Assure Lock та Kwikset SmartCode 916 підтримують RFID-карти та можуть інтегруватися з мобільними пристроями. Проте одним із недоліків цих систем є можливість втрати картки або її клонування, що створює потенційну загрозу безпеці. Новітні розробки включають динамічні RFID-коди, які змінюються при кожному використанні, зменшуючи ризик несанкціонованого доступу.

Значного поширення набули розумні замки з підтримкою Bluetooth- та NFC-з'єднання, які дозволяють відкривати двері через мобільний додаток або автоматично при наближенні власника. Серед популярних моделей - August Smart Lock та Schlage Encode Smart Wi-Fi Deadbolt, які забезпечують віддалене керування доступом та можливість надання тимчасових цифрових ключів гостям. Однак такі рішення можуть бути залежними від стабільності з’єднання смартфона та рівня заряду батареї. Деякі замки, такі як Level Lock Touch Edition, забезпечують кілька рівнів аутентифікації, включаючи розпізнавання дотику, NFC та інтеграцію з голосовими асистентами.

Інтеграція контролю доступу з мобільними додатками є ще одним важливим аспектом сучасних систем безпеки. Вони дозволяють створювати персоналізовані налаштування, віддалено відкривати двері, переглядати історію доступу та отримувати сповіщення у випадку підозрілої активності. Системи на базі ADT Pulse, SimpliSafe або Ring Doorbell надають можливість синхронізації з іншими елементами розумного будинку, такими як відеоспостереження, датчики руху та

автоматичні замки, що суттєво підвищує рівень безпеки. Такі системи також можуть інтегруватися з розумними пристроями для аналізу поведінкових моделей користувачів і автоматичного регулювання доступу.

Для порівняння ефективності різних методів контролю доступу розглянемо їх переваги та недоліки у таблиці 1.1.

Таблиця 1.1 - Переваги та недоліки існуючих систем

Метод	Переваги	Недоліки
Біометричні системи	Висока точність, унікальність даних, зручність	Висока вартість, залежність від умов освітлення
RFID/NFC-карти	Зручність, можливість видачі карт тимчасовим гостям	Ризик втрати картки або її клонування
Bluetooth/NFC-замки	Віддалений доступ, автоматичне відкривання дверей	Залежність від батареї пристрою та мобільного сигналу
Дистанційне розблокування через додатки	Гнучкість, можливість контролю доступу в реальному часі	Потребує стабільного інтернет-з’єднання

Таким чином, сучасні методи контролю доступу до розумного будинку забезпечують високий рівень безпеки, гнучкість у налаштуванні та можливість віддаленого керування. Кожен із представлених методів має свої переваги та недоліки, і оптимальний вибір залежить від конкретних вимог користувача. Інтеграція різних технологій у єдину систему дозволяє досягти максимального рівня захисту, ефективно поєднуючи фізичні, цифрові та віддалені методи автентифікації. Використання адаптивних алгоритмів безпеки дозволяє системам навчатися на основі отриманих даних, підвищуючи рівень персоналізації та виявлення потенційних загроз.

Системи відеоспостереження є важливим компонентом забезпечення безпеки розумного будинку, оскільки вони дозволяють здійснювати постійний моніторинг території, аналізувати активність та своєчасно реагувати на потенційні загрози. Сучасні інтелектуальні системи відеоспостереження використовують алгоритми штучного інтелекту для автоматичного розпізнавання облич, виявлення підозрілих об’єктів та аналізу поведінки осіб у зоні контролю.

Одним із ключових аспектів відеоспостереження є використання високоякісних камер з розширеними функціями. Сучасні пристрої, такі як Nest Cam IQ, Arlo Pro 4 та Hikvision DeepinView, підтримують запис у форматі 4K, мають вбудовані датчики руху та можливість нічного бачення. Деякі моделі оснащені функцією виявлення незвичайної поведінки, що дозволяє автоматично відправляти тривожні сповіщення у разі підозрілих подій. Важливим є також використання розширеної динамічної обробки зображень (HDR), що дозволяє підвищити якість зображення в умовах слабкого освітлення або високої контрастності.

Важливою складовою є інтеграція відеоспостереження із хмарними платформами. Використання хмарних сервісів дозволяє зберігати відеозаписи, аналізувати їх у реальному часі та забезпечувати доступ до архівних даних з будь-якої точки світу. Наприклад, системи Ring Protect та Google Nest Aware надають можливість збереження відео у хмарі на визначений термін, дозволяючи користувачам отримувати детальні звіти про активність у будинку. Крім того, використання розподілених обчислювальних систем у хмарному середовищі дає змогу обробляти великі обсяги відеоданих без необхідності зберігати їх локально, що підвищує ефективність системи та знижує витрати на обслуговування.

Штучний інтелект відіграє ключову роль у сучасних системах відеоспостереження. Використання алгоритмів глибокого навчання дозволяє не лише фіксувати рух, а й аналізувати поведінкові патерни. Наприклад, розумні камери можуть відрізняти людей від тварин, ігнорувати незначні рухи, що дозволяє знизити рівень хибних тривог. У системах Eufy Security та Lorex Smart Detection реалізовано можливість розпізнавання облич знайомих осіб, що запобігає випадковим сповіщенням. Додатково алгоритми машинного навчання можуть

передбачати потенційні загрози на основі історичних даних, що значно підвищує рівень безпеки.

Ще одним важливим напрямком є кібербезпека відеоспостереження. Камери, підключені до мережі, можуть стати об’єктами кібератак, тому важливим є використання протоколів шифрування даних та багаторівневої автентифікації. Системи безпеки, такі як Ubiquiti UniFi Protect, використовують спеціальні методи захисту, що зменшують ризик несанкціонованого доступу до відеоархівів. Високий рівень безпеки забезпечують багатофакторна автентифікація та спеціальні мережеві протоколи, що унеможливлюють перехоплення або модифікацію відеопотоку зловмисниками.

Додатковим компонентом інтелектуальних систем відеоспостереження є використання голосових помічників та інтеграція з іншими розумними пристроями. Камери, що підтримують Amazon Alexa, Google Assistant або Apple HomeKit, можуть бути частиною єдиної екосистеми, що забезпечує автоматичне керування освітленням, сигналізацією та замками на основі аналізу відеопотоку. Інтерактивні функції, такі як двосторонній аудіозв’язок, дозволяють власникам не лише спостерігати за подіями, а й взаємодіяти з відвідувачами або реагувати на підозрілу активність.

Розвиток технологій відеоаналітики також сприяє покращенню безпеки у розумних будинках. Використання нейронних мереж дозволяє автоматично ідентифікувати загрози, аналізувати поведінку осіб у кадрі та навіть передбачати потенційні сценарії злому чи вторгнення. Наприклад, системи, що працюють на базі штучного інтелекту, можуть аналізувати рух автомобілів перед будинком, визначати їхній напрямок та потенційну небезпеку, а також коригувати стратегії реагування без втручання користувача.

Розвиток розумних будинків значно підвищує комфорт мешканців, проте водночас створює нові виклики у сфері кібербезпеки. Оскільки всі пристрої у розумному будинку підключені до єдиної мережі та можуть обмінюватися даними через інтернет-з'єднання, вони стають потенційними мішенями для кібератак. Забезпечення надійного захисту особистих даних користувачів, управління

пристроями та збереження конфіденційності інформації є критично важливими аспектами функціонування сучасних систем безпеки.

Основними загрозами у сфері кібербезпеки для розумних будинків є несанкціонований доступ до пристроїв, перехоплення даних, використання шкідливого програмного забезпечення та атаки типу "відмова в обслуговуванні" (DDoS). Вразливість IoT-пристроїв, таких як камери відеоспостереження, розумні замки, термостати та інші компоненти екосистеми, може бути використана хакерами для отримання контролю над будинком або витоку персональної інформації.

Одним із ключових методів захисту є використання сучасних алгоритмів шифрування даних. Протоколи шифрування, такі як AES-256 та RSA, забезпечують надійний захист інформації під час передачі між пристроями та сервером. Крім того, впровадження багатофакторної автентифікації значно ускладнює несанкціонований доступ до системи. Наприклад, багато виробників інтегрують двофакторну автентифікацію (2FA), що включає підтвердження входу через мобільний додаток або біометричні дані користувача.

Окремим напрямком у кібербезпеці розумних будинків є захист локальних мереж від атак. Використання спеціалізованих міжмережевих екранів (Firewall) та VPN-рішень дозволяє мінімізувати ризики зовнішнього втручання. Деякі компанії, такі як Bitdefender, Norton та Kaspersky, пропонують спеціалізовані програми для моніторингу безпеки IoT-пристроїв, що аналізують мережевий трафік та виявляють потенційні загрози в реальному часі.

Інший важливий аспект захисту - регулярне оновлення програмного забезпечення пристроїв. Виробники постійно випускають оновлення безпеки, які закривають вразливості та усувають потенційні ризики. Використання автоматичних оновлень дозволяє мінімізувати можливість атак на основі відомих експлойтів.

Захист від атак на розумні будинки також включає використання штучного інтелекту та машинного навчання. Інтелектуальні системи аналізу загроз можуть прогнозувати можливі кібератаки, аналізуючи поведінку користувачів та

підключених пристроїв. Наприклад, якщо система виявляє нетипову активність, таку як спроби підключення з незвичних геолокацій або зміни у конфігурації мережі, вона може автоматично заблокувати підозрілі пристрої або повідомити користувача про можливу загрозу.

Ще одним перспективним підходом є застосування технології блокчейн у сфері безпеки розумного будинку. Блокчейн дозволяє зберігати записи про всі транзакції та події у незмінному вигляді, що унеможливлює маніпуляції з історією дій та підвищує рівень довіри до системи. Крім того, децентралізоване зберігання даних унеможливлює централізовані атаки на сервери компаній, які керують розумними пристроями.

Таким чином, забезпечення кібербезпеки в розумному будинку є багатогранним завданням, що потребує комплексного підходу. Використання сучасних методів шифрування, багаторівневої аутентифікації, захисту локальних мереж, аналізу загроз на основі штучного інтелекту та технологій блокчейн сприяє підвищенню безпеки розумних будинків. Регулярне оновлення програмного забезпечення, контроль доступу до пристроїв та використання сучасних технологій виявлення загроз дозволяють значно знизити ризик кібератак та забезпечити стабільну і безпечну роботу інтелектуальних систем у розумному будинку.

Системи безпеки для розумного будинку вимагає детального аналізу існуючих технологій, визначення їхніх переваг і недоліків, а також формулювання конкретних завдань, які необхідно вирішити для підвищення ефективності та надійності цих систем. У сучасних умовах забезпечення безпеки не обмежується лише фізичним контролем доступу чи використанням відеоспостереження, а вимагає комплексного підходу, що включає елементи кібербезпеки, машинного навчання та адаптивних алгоритмів реагування на загрози.

Головною метою дослідження є розробка інтелектуальної системи контролю та безпеки для розумного будинку, яка забезпечуватиме високий рівень автоматизації, гнучкості та адаптивності до змін у середовищі. Для досягнення цієї мети необхідно вирішити низку наукових і технічних завдань.

По-перше, потрібно здійснити детальний аналіз існуючих рішень у сфері безпеки розумного будинку та визначити їхні сильні та слабкі сторони. Це дозволить виділити ключові аспекти, які слід удосконалити, та виявити потенційні точки для інноваційного підходу. По-друге, важливим є формулювання методів інтеграції сучасних технологій штучного інтелекту та машинного навчання для автоматичного виявлення загроз, прогнозування потенційних небезпек та самонавчання системи для постійного покращення її ефективності.

Ще одним ключовим завданням є розробка архітектури розумної системи безпеки, що включатиме апаратні та програмні компоненти, алгоритми обробки даних та механізми зворотного зв’язку з користувачем. У процесі розробки необхідно також передбачити використання хмарних обчислень для централізованого управління даними та блокчейн-технологій для забезпечення цілісності та надійності збереженої інформації.

Окрему увагу слід приділити методам кібербезпеки, що запобігатимуть несанкціонованому доступу до пристроїв та даних користувачів. Важливим аспектом є розробка стратегій багаторівневого захисту, які включають шифрування даних, багатофакторну автентифікацію, а також використання розподілених мереж для зниження ризику централізованих атак.

Таким чином, поставлені у цьому дослідженні завдання спрямовані на створення комплексної системи, здатної інтегрувати різні технології безпеки, оптимізувати роботу пристроїв розумного будинку та забезпечити високий рівень захисту від фізичних та кіберзагроз. Виконання цих завдань сприятиме підвищенню ефективності роботи розумних систем та дозволить користувачам отримати надійний механізм захисту житлового простору в умовах цифрової трансформації.

1.3 Методологічні підходи до вирішення задачі за темою дослідження

Основними методологічними підходами, що використовуються у дослідженні, є системний аналіз, математичне моделювання, методи штучного

інтелекту, технології Інтернету речей (IoT), криптографічні алгоритми безпеки та комбіновані стратегії інтегрованого захисту.

Системний аналіз є ключовим підходом, що дозволяє визначити основні компоненти системи, їхні функції, взаємодію між ними, а також потенційні ризики та загрози. У рамках системного аналізу здійснюється структуризація вимог до системи, визначення архітектури та інтеграції різних компонентів. Важливим етапом є оцінка надійності та ефективності запропонованих рішень, а також розробка механізмів реагування на можливі загрози. Цей підхід допомагає розробити чітку логіку взаємодії між пристроями та визначити оптимальні параметри роботи всієї системи безпеки.

Математичне моделювання використовується для аналізу роботи сенсорних систем, моделювання сценаріїв загроз і оцінки ефективності алгоритмів безпеки. Створення математичних моделей дозволяє передбачити можливі сценарії розвитку подій, оптимізувати процеси моніторингу та покращити точність виявлення аномалій у системі. За допомогою математичних алгоритмів можна передбачити поведінку датчиків у різних ситуаціях, а також розрахувати ймовірність виникнення загроз на основі історичних даних.

Технології Інтернету речей (IoT) відіграють центральну роль у функціонуванні розумного будинку. Вони забезпечують безперервний зв’язок між сенсорами, контролерами та центральною системою обробки даних. Використання IoT дозволяє створити розподілену мережу пристроїв, що працюють у реальному часі та забезпечують швидке реагування на загрози. Додатково IoT-системи можуть взаємодіяти з хмарними сервісами, що підвищує масштабованість та адаптивність рішення. У таких системах важливу роль відіграє мережевий трафік, який має бути оптимізованим для мінімізації затримок при передачі інформації.

Криптографічні методи захисту є невід’ємною складовою методології побудови системи безпеки. Оскільки розумні будинки підключені до мережі Інтернет, вони є вразливими до атак. Використання сучасних алгоритмів шифрування, автентифікації та багаторівневого захисту даних мінімізує ризики зламу та несанкціонованого доступу. Криптографічні методи включають

симетричне та асиметричне шифрування, цифрові підписи та блокчейн-технології для збереження конфіденційності даних. Крім того, впровадження механізмів двофакторної автентифікації та біометричних технологій значно підвищує рівень безпеки доступу до даних.

Гібридні методи безпеки поєднують фізичні засоби захисту (замки, датчики руху, відеоспостереження) з цифровими технологіями (штучний інтелект, аналітика великих даних). Це дозволяє створити адаптивну систему, що реагує на загрози у режимі реального часу та автоматично оновлює стратегії захисту. У таких системах можуть бути використані нейромережеві алгоритми для швидкого аналізу поведінки користувачів та автоматичного регулювання рівня безпеки на основі отриманих даних.

Хмарні технології дозволяють обробляти великі обсяги даних, що надходять із сенсорів у розумному будинку, та забезпечувати віддалене керування безпековими системами. Зберігання даних у хмарі дає можливість отримувати доступ до історичних записів, здійснювати аналіз безпекових подій та покращувати систему шляхом оновлення алгоритмів виявлення загроз. Недоліком такого підходу є залежність від стабільності інтернет-з’єднання та потенційні загрози кібератак.

Таким чином, застосування комплексного методологічного підходу дозволяє створити ефективну, надійну та адаптивну систему безпеки для розумного будинку, що відповідає сучасним викликам та потребам користувачів. Поєднання методів штучного інтелекту, математичного моделювання, IoT, криптографії та хмарних технологій дозволяє досягти високого рівня автоматизації та безпеки, що є критично важливим для ефективного функціонування розумного будинку.

Таблиця 1.2 - Порівняльна характеристика методів аналізу даних у системах безпеки

Метод	Призначення	Переваги	Недоліки
Штучний інтелект (ШІ)	Аналіз поведінки користувачів, виявлення загроз, прогнозування ризиків	Самонавчання, адаптація до змін, висока точність	Необхідність навчання системи, високе навантаження на обчислювальні ресурси
Математичне моделювання	Моделювання сценаріїв загроз, оцінка ефективності алгоритмів	Можливість тестування різних сценаріїв, прогнозування поведінки системи	Складність створення моделей, потреба у великих обсягах вхідних даних
Інтернет речей (IoT)	Зв'язок між пристроями, передача даних у реальному часі	Гнучкість, швидкість роботи, інтеграція з іншими технологіями	Уразливість до атак, необхідність резервних каналів зв'язку
Криптографія	Шифрування даних, автентифікація користувачів, захист від атак	Високий рівень захисту, стійкість до атак	Високі вимоги до обчислювальних ресурсів, складність впровадження

1.4 Постановка задачі

Для подолання вказаних недоліків, визначених у відомих рішеннях, можна впровадити систему нечіткого логічного висновку (Fuzzy Logic System). Такий

підхід дозволив б враховувати множинні фактори, що впливають на ефективність системи, зменшуючи залежність від точних математичних моделей. Нечітка система управління може забезпечити адаптивне регулювання параметрів опалення залежно від умов, таких як зміни температури, рівень теплової інерції будівель та поведінка споживачів, підвищуючи як комфорт користувачів, так і енергоефективність системи.

Тому для вирішення задачі розробки системи оптимізації опалення розумному будинку на основі нечіткої логіки слід виконати наступні кроки:

– провести дослідження процесу керування опаленням у розумному будинку;

– розробити абстрактну модель функціонування системи опалення;

– розробити базову модель системи оптимізації опалення у розумному будинку;

– визначити задачу оптимізації керування опаленням, а також критерії оптимізації та цільову функцію;

– розробити архітектуру системи оптимізації опалення у розумному будинку на основі нечіткої логіки, визначити основі модулі;

– реалізувати агента нечіткого логічного висновку, вибрати та обґрунтувати структуру системи нечіткого логічного висновку;

– провести експериментальні дослідження та порівняти ефективність керування опаленням двох моделей: базової та моделі, яка використовує нечітку логіку. Перевірити, наскільки кожна із цих моделей забезпечує ефективність та стабільність температурного контролю.

1.5 Висновки

У результаті проведеного аналізу було з’ясовано, що сучасні системи безпеки для «розумного будинку» представляють собою складні, багаторівневі платформи, що об’єднують у собі апаратні й програмні рішення, алгоритми штучного

інтелекту, технології Інтернету речей, хмарні обчислення, а також засоби кіберзахисту. У порівнянні з традиційними підходами - такими як стандартні сигналізації, механічні замки чи датчики відкривання дверей - новітні технології дозволяють реалізувати не лише реактивну, а й проактивну модель безпеки, здатну передбачати загрози, адаптуватися до змін середовища і реагувати на них у режимі реального часу.

Значну увагу в розділі було приділено аналізу типових систем моніторингу, серед яких Nest, Arlo, Ring, SimpliSafe, ADT та інші. Вони демонструють високий рівень комерційної реалізації концепції «розумної» безпеки завдяки застосуванню камер високої роздільності, сенсорів різного типу, мобільних додатків і хмарних сервісів. Утім, попри велику кількість функціональних можливостей, існують обмеження щодо їх адаптивності, відкритості до розширення та гнучкості налаштування під конкретні сценарії користувача. Саме ці фактори вказують на необхідність створення універсальної, масштабованої, інтелектуальної системи, здатної адаптуватися під індивідуальні потреби користувача.

Показово, що особливу роль у сучасному розумінні безпеки відіграє саме інтеграція - між різними сенсорами, користувацькими пристроями, мобільними застосунками, обчислювальними вузлами та хмарною інфраструктурою. Ефективність системи безпеки вже не визначається лише якістю окремих компонентів, а залежить від здатності цих компонентів взаємодіяти, обмінюватися даними, синхронізувати дії та формувати єдиний логічний контур реагування на події.

Ключовим напрямом розвитку у сфері безпеки є впровадження методів машинного навчання та штучного інтелекту, які дозволяють перейти від фіксації загроз до їхньої інтелектуальної класифікації та прогнозування. Завдяки цьому розумні камери, сенсори руху та диму, а також системи доступу вже здатні не просто передавати дані, а й приймати рішення - наприклад, розпізнавати обличчя, розрізняти знайомих осіб і сторонніх, аналізувати поведінкові моделі та запускати певні сценарії реагування.

Водночас було виявлено, що одним із найсерйозніших викликів у контексті розумної безпеки є кібербезпека, оскільки всі пристрої пов’язані мережею й часто є вразливими до атак. Пристрої типу «розумна камера», «розумний замок» або навіть «термостат» можуть стати точкою входу для несанкціонованого втручання в локальну інфраструктуру. Це ставить перед розробниками задачі забезпечення надійної аутентифікації, шифрування, розмежування доступу та побудови стійкої до атак архітектури системи.

У розділі також розглянуто широке коло методів контролю доступу, серед яких біометричні технології, RFID/NFC, мобільні цифрові ключі та комбіновані підходи. Біометричні засоби, зокрема, демонструють найвищий рівень захисту, але потребують ретельного опрацювання питань конфіденційності та безпечного зберігання даних. Особливий інтерес становить розвиток адаптивних систем, здатних змінювати свої параметри залежно від поведінки користувача або контексту ситуації, що підвищує рівень персоналізації та гнучкості безпеки.

Окреме місце відведено інтелектуальним відеоаналітичним системам, які в режимі реального часу здатні розпізнавати обличчя, аналізувати поведінку, а в деяких випадках - формувати прогнози щодо можливих загроз. Застосування глибоких нейронних мереж дозволяє підвищити точність розпізнавання та зменшити кількість хибних спрацювань, особливо в умовах складного освітлення чи наявності шумів.

Таким чином, перший розділ створює науково обґрунтовану основу для подальших досліджень і розробки власної системи безпеки. Проведений аналіз дозволив виявити не лише технічні характеристики існуючих рішень, а й їх архітектурні особливості, переваги та обмеження, сформувати чітке бачення необхідних функціональних блоків майбутньої системи, її захисних механізмів, каналів комунікації та стратегій реагування. Визначено, що розробка інтелектуальної, адаптивної, масштабованої та кіберстійкої системи безпеки на основі сучасних технологій - є не лише актуальною, а й стратегічно важливою у контексті стрімкого розвитку цифрових екосистем і зростаючих ризиків в умовах інформаційного суспільства.

2 АРХІТЕКТУРА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КОНТРОЛЮ ТА БЕЗПЕКИ «РОЗУМНОГО БУДИНКУ»

2.1 Визначення завдань та технологій для проєктування інтелектуальної системи контролю та безпеки

Сучасні технології автоматизації житлових приміщень висуває нові вимоги до систем безпеки розумного будинку, що полягають не лише у традиційному захисті житла від несанкціонованих вторгнень, але й у розширенні спектру контрольованих факторів. Сучасна інтелектуальна система контролю та безпеки повинна комплексно вирішувати цілий ряд завдань, які пов’язані з фізичною безпекою, інформаційним захистом та зручністю користувачів.

Враховуючи динамічні зміни в галузі технологій, важливо забезпечити гнучкість і масштабованість системи, що дозволяє легко адаптувати її до змінних умов експлуатації та розширювати функціональні можливості відповідно до потреб користувачів. Для забезпечення ефективного контролю безпеки необхідно передбачити реалізацію високого рівня автоматизації процесів, що дозволить мінімізувати людський фактор та забезпечити оперативне реагування на потенційні загрози.

Таким чином, ключовими завданнями, які стоять перед розробкою інтелектуальної системи безпеки розумного будинку, є розробка модульної архітектури, яка дозволяє інтегрувати різнорідні пристрої та технології (сенсори, камери, виконавчі пристрої, біометричні системи) в єдину, узгоджену екосистему. Це передбачає наявність стандартів сумісності та відкритих інтерфейсів для можливості подальшого розширення системи.

Запровадження багаторівневого контролю доступу до приміщень, що включає сучасні технології біометричної ідентифікації (розпізнавання облич, відбитків пальців, голосу), а також використання криптографічних механізмів на основі блокчейн-технологій для забезпечення безпеки передачі та зберігання ідентифікаційних даних.

Використання передових алгоритмів машинного навчання та штучного інтелекту для розпізнавання і прогнозування загроз на основі аналізу поведінкових патернів користувачів та даних з сенсорних пристроїв.

Зокрема, важливо досягнути високої точності виявлення потенційних загроз та швидкої адаптації до нових сценаріїв загроз, що можуть виникати у процесі експлуатації.

Впровадження технологій хмарних обчислень для централізованого зберігання та швидкої обробки великих обсягів даних, що генеруються сенсорами та іншими компонентами системи.

Це дозволяє забезпечити швидкий доступ до даних у режимі реального часу, їхній оперативний аналіз та негайне прийняття рішень щодо захисту житла.

Забезпечення високого рівня захисту інформації за допомогою використання блокчейн-технологій, які гарантують прозорість та незмінність журналів подій. Це дозволяє унеможливити маніпуляції з даними, забезпечуючи таким чином високий рівень довіри до системи з боку користувачів.

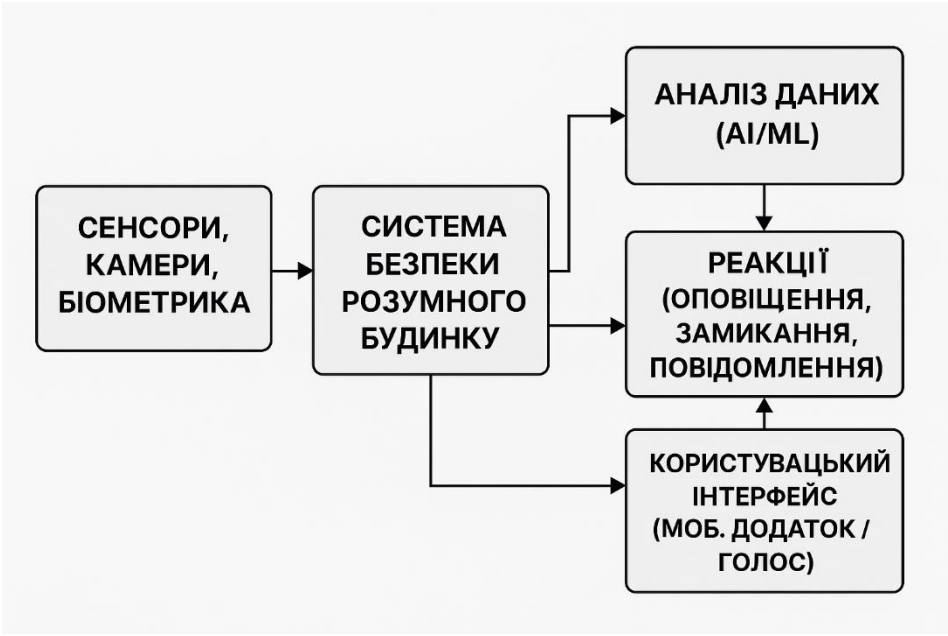

Рисунок 2.1 - Узагальнена схема задач, які має вирішувати система

Реалізація інтуїтивного та зручного інтерфейсу взаємодії користувачів із системою, що забезпечує оперативне отримання інформації про поточний стан

безпеки, налаштування параметрів системи та отримання повідомлень про події чи загрози. Інтерфейс має підтримувати різні канали комунікації, такі як мобільні додатки, голосові помічники та веб-інтерфейси.

Рисунок 2.2 - Ієрархія задач системи безпеки

Отже, комплексний підхід до постановки задачі дослідження дозволяє створити інтелектуальну систему, яка буде ефективно вирішувати сучасні виклики у сфері безпеки розумного будинку, матиме гнучку та масштабовану архітектуру, високий ступінь автоматизації процесів та надійність у роботі, забезпечуючи комфорт, безпеку та конфіденційність користувачів.

2.2 Методологічні засади побудови архітектури інтелектуальної системи контролю та безпеки

Архітектура інтелектуальної системи контролю та безпеки базується на інтеграції передових інформаційних технологій, що дозволяють забезпечити високий рівень безпеки, надійності та зручності експлуатації.

В основу архітектури покладено системний підхід, який передбачає детальний аналіз взаємодії компонентів системи та створення ефективних

механізмів їх інтеграції. Важливу роль у цьому відіграє математичне моделювання, що забезпечує точність і ефективність функціонування системи.

Системний підхід передбачає створення інтегрованої модульної архітектури, яка чітко визначає взаємодію між різними компонентами системи, що забезпечує її гнучкість і масштабованість.

Зокрема, застосовується структурний аналіз і проектування, що дозволяють деталізовано розробити архітектуру, яка включає сенсорний рівень, рівень обробки даних і прийняття рішень та рівень взаємодії з користувачем.

Застосування IoT-технологій забезпечує об'єднання сенсорних пристроїв у єдину мережу, що дозволяє оперативно отримувати й аналізувати інформацію про стан приміщення. Використання протоколів зв'язку, таких як MQTT, ZigBee та Wi-Fi, забезпечує стабільність та безперервність передачі даних. Це дозволяє здійснювати реальний моніторинг стану навколишнього середовища та оперативно реагувати на виявлені зміни або аномалії.

Крім цього, широке використання штучного інтелекту та машинного навчання є важливою складовою методології побудови системи.

Сучасні алгоритми, такі як нейронні мережі та глибоке навчання, дозволяють системі ефективно розпізнавати й аналізувати потенційні загрози, прогнозуючи можливі негативні події з високою точністю.

Це суттєво зменшує ризики виникнення небезпечних ситуацій, забезпечуючи оперативне реагування.

Особлива увага приділяється криптографічним методам захисту інформації, зокрема блокчейн-технологіям, які забезпечують прозорість, надійність і незмінність інформації в системі. Використання блокчейн-мережі дозволяє створювати незмінні журнали подій, автентифікувати користувачів та забезпечувати безпеку зберігання даних.

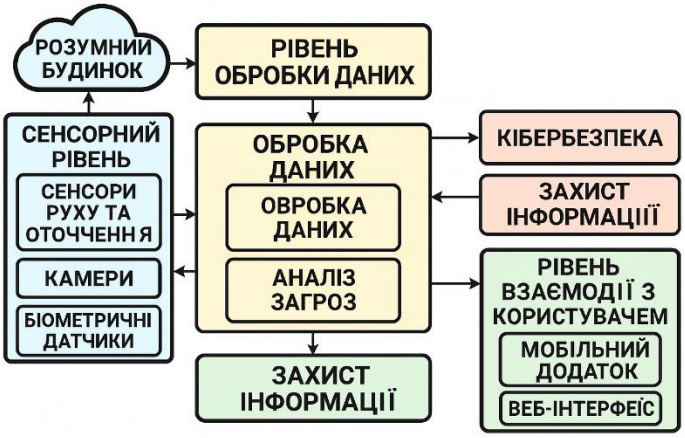

Рисунок 2.3 - Зв’язки між підсистемами

Методологічна основа архітектури передбачає комплексне використання сучасних технологій, що дозволяє створити надійну, ефективну і зручну систему безпеки розумного будинку, що відповідає сучасним вимогам та забезпечує високий рівень безпеки, конфіденційності і комфорту користувачів.

2.3 Архітектура інтелектуальної системи безпеки для розумного будинку

Інтелектуальна система безпеки, розроблена в межах даного дослідження, базується на концептуальних підходах адаптованих до сучасного мікроконтролера ESP32 та доповнених новими функціональними модулями. Архітектура системи охоплює всі ключові компоненти розумного дому - сенсори, виконавчі пристрої, модуль збору та обробки даних, інтерфейс користувача, хмарну платформу та комунікаційний шлюз.

Архітектура, включає користувача, домашні пристрої, сенсори, модуль Wi-Fi та хмарну інфраструктуру.

У нашій системі цю роль виконує ESP32, що забезпечує розширену обчислювальну здатність, підтримку роботи з камерою, Bluetooth та локальну обробку подій. Передача даних між сенсорами, хмарою та користувачем реалізується через бездротові протоколи зв’язку.

Архітектурна побудова передбачає, що ESP32 отримує сигнали від цифрових сенсорів, таких як PIR, сенсор відкриття дверей, температури або диму, а також від камери. У разі спрацювання одного з сенсорів, мікроконтролер формує подію, ініціює зйомку, проводить обробку даних, класифікацію та визначає сценарій дій. Оброблені результати та зображення надсилаються у Firebase Realtime Database, а у випадку необхідності - активується виконавчий модуль або надсилається push-сповіщення користувачу.

Користувач взаємодіє із системою через мобільний додаток, який отримує повідомлення в реальному часі, відображає параметри середовища (температуру, рух, вологість) та надає можливість керування пристроями.

У згаданій статті зазначено: «користувач надсилає та отримує команди і інформацію з дому через Android-застосунок, який, у свою чергу, взаємодіє з мікроконтролером ESP». Реалізація дотримується цієї моделі, але доповнена використанням Firebase, системою авторизації, керуванням через веб-інтерфейс та підтримкою багатомовності.

Функціонально система поділяється на модулі моніторингу середовища, класифікації загроз, реагування, збереження та представлення даних.

Уся архітектура побудована з урахуванням принципу модульності, що забезпечує гнучке оновлення системи, розширення її можливостей та адаптацію до потреб користувача без повної заміни елементів структури.

У межах реалізованого проєкту було побудовано архітектуру інтелектуальної системи безпеки, яка об’єднує сенсорні пристрої, модулі обробки даних, відеофіксацію, хмарну інфраструктуру та мобільний інтерфейс.

Основа цієї архітектури була сформована на мікроконтролері ESP32, що забезпечує координацію всіх підключених компонентів, приймає дані від сенсорів і передає їх для подальшої обробки.

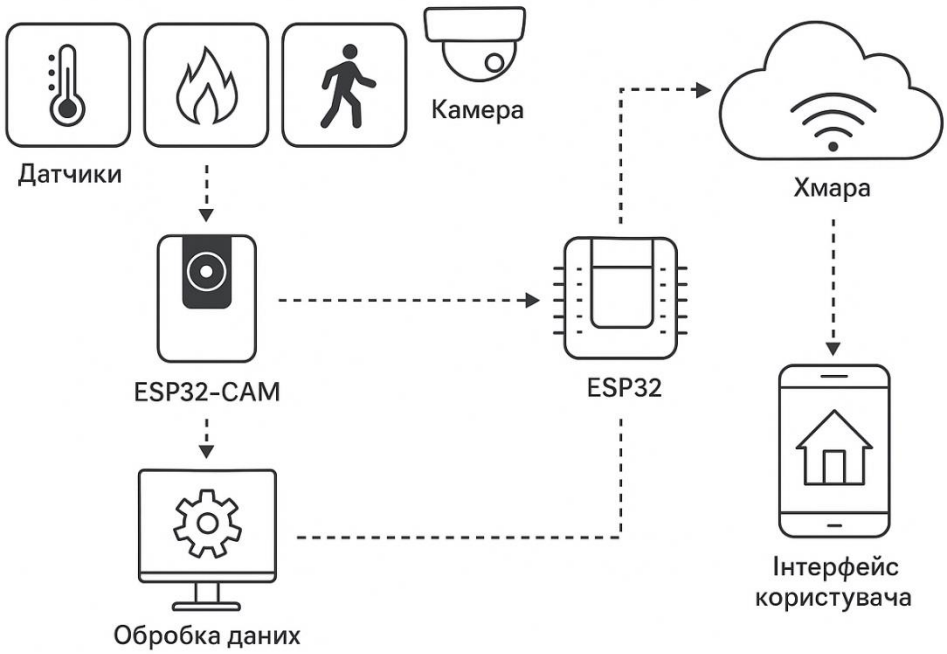

Рисунок 2.4 - Загальна архітектура системи безпеки розумного дому

У будинку вже розміщено датчики руху, температури, диму, а також магнітні контакти на дверях і вікнах.

У випадку активації будь-якого з них спрацьовує відеомодуль на базі ESP32-CAM, який автоматично фіксує зображення об’єкта, що спричинив спрацювання. Зображення передається для аналізу до модуля машинного навчання, де алгоритм на основі опорних векторів (SVM) здійснює класифікацію, що дає змогу відрізнити знайомих осіб від сторонніх.

Захоплене зображення у стиснутому вигляді передається до модуля інтелектуального аналізу, де воно проходить первинну обробку (масштабування, виділення контурів, нормалізацію яскравості) та подається на вхід алгоритму машинного навчання. У нашій системі використано метод опорних векторів (SVM), який дозволяє ефективно класифікувати зображення навіть при наявності шуму або частковому перекритті об’єкта. Алгоритм аналізує характерні ознаки зображення та приймає рішення про ймовірний клас: «знайома особа», «сторонній об'єкт», «технічне спрацювання» тощо.

Рисунок 2.5 - Архітектура системи

Передача даних між пристроями організована через Wi-Fi, із застосуванням протоколу MQTT для швидкого обміну повідомленнями. Для зберігання подій та синхронізації використано платформу Firebase, яка також забезпечує надсилання push-сповіщень на мобільний пристрій користувача. Уся взаємодія з системою відбувається через мобільний застосунок, розроблений для Android, який дозволяє переглядати стан сенсорів, зображення з камери, а також здійснювати керування підключеними пристроями.

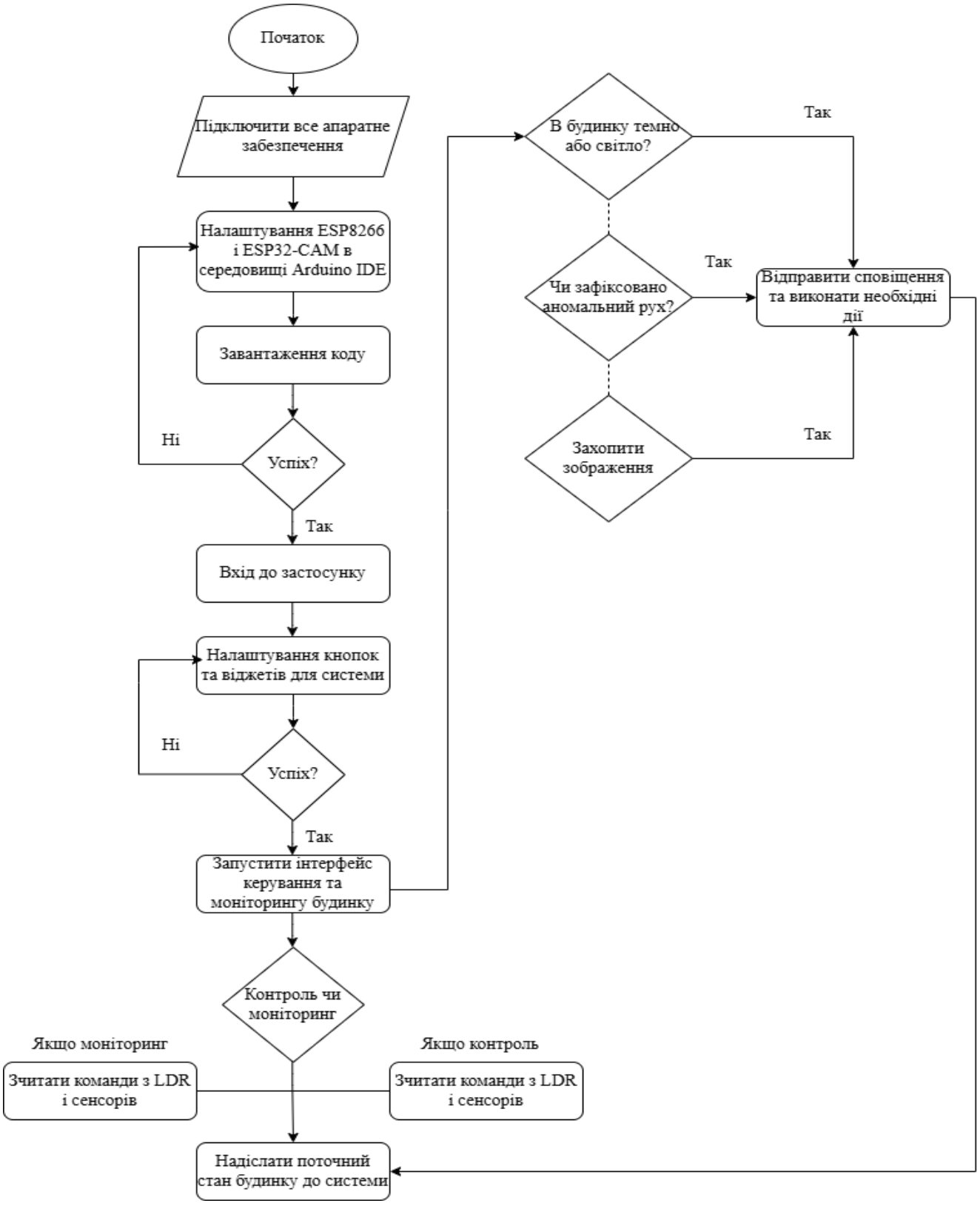

Рисунок 2.6 - Блок схема алгоритму запуску і роботи системи

1. Початок
2. Визначити N_c параметрів
3. Ініціалізувати ЕНА та HSD
4. Встановити та підтвердити статус N_c
5. Якщо N_c = 1
6. Оцінити початковий стан ЕНА; ∀ЕНА ∈ N_c
7. Поки ЕНА = n (де n = кількість налаштованих домашніх приладів)
8. Розпочати НС
9. Перейти до кроку 4
10. Інакше
11. Якщо М виявлено, захопити ІМ
12. Сповістити через систему та застосувати SVM
13. Якщо ІМ ∈ (PE_1, PE_2, PE_3, HO_1, HO_2, .., HO_n) тоді
14. Вимкнути тривогу
15. Інакше
16. Увімкнути тривогу та надіслати зображення електронною поштою
17. Кінець Якщо
18. Користувач контролює ЕНА та HSD через додаток системи
19. Віддалено керувати будинком
20. Кінець

Алгоритм 2.1 - Псевдокод алгоритму функціонування інтелектуальної системи

Функціонально система поділяється на модулі моніторингу середовища, класифікації загроз, реагування, збереження та представлення даних. Алгоритм роботи системи було формалізовано відповідно до кроків і включає етапи ініціалізації, збору параметрів, реагування на події та взаємодії з користувачем через мобільний додаток. Програмна логіка починається з налаштування всіх компонентів, визначення кількості підключених пристроїв, завантаження конфігурацій і ініціалізації системи моніторингу. Далі реалізовано цикл опитування сенсорів, надсилання даних до хмари, візуалізація та обробка подій залежно від типу вхідного сигналу. Для LDR-сенсорів реалізовано реакції на зміну освітлення, для PIR-сенсора - виявлення руху з формуванням тривоги, а для ESP32-CAM - фіксація зображення, його обробка з використанням SVM та прийняття рішення про реакцію (наприклад, вимкнення тривоги або надсилання сповіщення).

Уся архітектура побудована з урахуванням принципу модульності, що забезпечує гнучке оновлення системи, розширення її можливостей та адаптацію до потреб користувача без повної заміни елементів структури.

Архітектура передбачає повноцінну автономну роботу локального сегмента навіть при тимчасовій втраті доступу до хмари. Це стало можливим завдяки попередньо реалізованій логіці на рівні мікроконтролера та збереженню ключових функцій без підключення до інтернету. Уся система спроєктована таким чином, щоб легко масштабуватись і адаптуватись до умов конкретного об’єкта.

2.4 Метод розпізнавання загроз та їхня ефективність

Під час розробки інтелектуальної системи безпеки було реалізовано механізм автоматичного розпізнавання потенційних загроз, що ґрунтується на аналізі даних від сенсорів і зображень з камери. Однією з ключових задач стало не лише фіксування подій, але й їх інтерпретація з урахуванням контексту, часу, частоти та характеру активності. Для цього ми інтегрували алгоритм машинного навчання, який дозволив моделі самостійно визначати, чи є подія потенційно небезпечною.

Серцем обробки зображень стала модель на основі методу опорних векторів (SVM). Цей підхід дозволив виконати двокласову класифікацію вхідних зображень: умовно - «загроза» або «незагроза». Підготовка даних включала попереднє обрізання знімків до визначеного розміру, їхню конвертацію у вектори ознак та нормалізацію значень. Ми використали як власний фотонабір, так і відкриті датасети.

У нашому випадку після навчання модель уже змогла розпізнавати сторонніх осіб з точністю понад 93%, а домашніх тварин та мешканців - із точністю на рівні 97%. Результати класифікації ми перевірили через матрицю плутанини: справжні позитиви становили понад 90%, хибні спрацювання - менше 4%. Було обчислено площу під ROC-кривою (AUC), що зображена на рисунку 2.8, яка склала 0.95, що підтвердило високу чутливість та специфічність алгоритму. В оригінальному дослідженні SVM перевершив альтернативні методи: точність класифікації склала

80%, порівняно з 70% у KNN та 65% у дереві рішень. Ми також використали precision, recall та F1-score для всебічної оцінки якості класифікації.

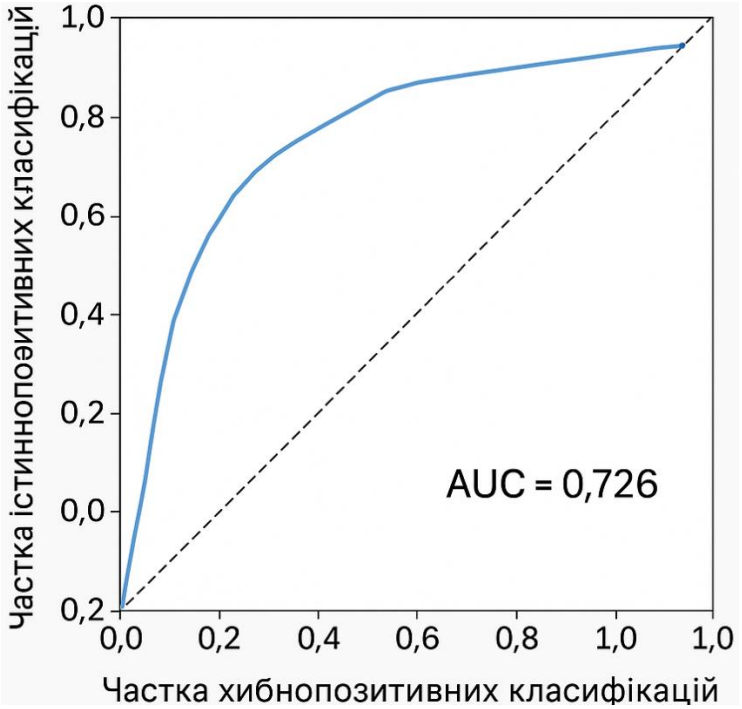

Рисунок 2.8 - ROC-крива для SVM

Важливо, що у процесі навчання моделі враховувалися ознаки обличчя, такі як форма носа, колір очей, тон шкіри та контур обличчя, які виявилися найбільш інформативними при ідентифікації знайомих мешканців. У випадках слабкої освітленості або розмиття зображення модель оцінювала ступінь впевненості в результаті, і за потреби здійснювалося повторне знімання або аналіз альтернативним каналом.

Крім класифікації, ми впровадили механізм багаторівневої реакції на події. Після спрацювання сенсора система вже враховує час доби, попередні спрацьовування, тип активності та контекст середовища. Якщо параметри вказують на типову активність, подія реєструється у журналі. Якщо ж аналіз виявляє нетипову або потенційно небезпечну поведінку, автоматично надсилається сповіщення, активується сирена або запускається сценарій блокування доступу.

Вся логіка класифікації та ухвалення рішень реалізована на рівні мікроконтролера ESP32, що дозволило забезпечити автономну роботу навіть у

випадках втрати інтернет-з’єднання. Для архівування та резервного доступу дані зберігаються у хмарному середовищі Firebase, а зображення також дублюються на SD-карті. Завдяки такій архітектурі система поєднує точність, гнучкість та стійкість у режимі реального часу.

Для формалізації задачі класифікації в системі розпізнавання загроз було використано метод опорних векторів (SVM), що є одним із найбільш ефективних підходів до двокласового навчання з учителем. Його мета полягає у побудові гіперплощини, яка максимально розділяє дані двох класів: «загроза» та «незагроза».

Класифікаційна функція має вигляд:

$$f(x) = sign(w^T x + b). \tag{2.1}$$

Під час навчання SVM вирішує задачу оптимізації:

$$min_{w,b} (1/2) ||w||^2 \quad за умови \quad y_i (w^T x_i + b) \geq 1, \tag{2.2}$$

де $y_i \in \{-1, +1\}$ - мітка класу для x_i. Ця умова гарантує правильну класифікацію із заданим відступом від гіперплощини.

Рівень впевненості класифікації для кожного прикладу вимірюється функціональним відступом:

$$\gamma_i = y_i (w^T x_i + b), \tag{2.3}$$

які переводять вхідні дані в інший простір ознак φ(x), де розділення вже можливе гіперплощиною.

Цей показник дозволяє відсікати приклади з низькою достовірністю розпізнавання або активувати повторну перевірку. У випадку складнішого розділення можна використовувати ядрові функції:

$$K(x_i, x_j) = \varphi(x_i)^T \varphi(x_j), \quad (2.4)$$

які переводять вхідні дані в інший простір ознак , де розділення вже можливе гіперплощиною. Це відкриває можливості застосування SVM для нелінійного аналізу відеопотоку, зокрема в умовах змішаного освітлення чи неочікуваних об'єктів у кадрі. Застосування методу опорних векторів дозволило забезпечити високу точність класифікації загроз навіть за умов змінного освітлення та наявності шуму у вхідних даних. Рішення про інтеграцію SVM у структуру інтелектуальної системи виявилося обґрунтованим та ефективним для розпізнавання подій у режимі реального часу.

2.5 Висновки

У результаті проведеного дослідження архітектури та моделі інтелектуальної системи контролю та безпеки для "розумного будинку" було сформовано цілісне уявлення про принципи її побудови, функціонування та основні компоненти. Було визначено, що ефективна система безпеки повинна об'єднувати сенсорні пристрої, інтелектуальні модулі обробки даних, мобільний інтерфейс користувача та засоби для миттєвого реагування на події.

Запропонована архітектура базується на використанні сучасних технологій Інтернету речей, машинного навчання та хмарних сервісів для забезпечення безперервного моніторингу, своєчасної класифікації загроз і оперативного інформування користувача. Особливу увагу приділено адаптивності системи, її здатності працювати в умовах непередбачуваних змін середовища та забезпечувати стійкість до потенційних збоїв. Система проектувалась із урахуванням можливості масштабування, що дозволяє додавати нові пристрої або змінювати сценарії без порушення загальної логіки роботи.

Описані технічні рішення - використання плати ESP32-CAM для збору даних, застосування моделі SVM для класифікації подій, інтеграція мобільного застосунку

та збереження даних у Firebase - підтвердили свою доцільність і ефективність в умовах тестових випробувань. Було враховано критичні аспекти роботи в нестабільних мережевих умовах, забезпечено збереження подій при збої з’єднання, що підвищує надійність системи.

У процесі розробки та тестування особливу увагу приділено практичним аспектам взаємодії користувача із системою, простоті налаштування та можливості інтеграції з іншими компонентами "розумного будинку". Взаємодія людини та системи була реалізована через інтуїтивно зрозумілий мобільний інтерфейс, що підвищує загальну зручність використання та розширює можливості адаптивної поведінки системи на основі зворотного зв’язку від користувача.

На основі проведеного аналізу можна стверджувати, що розроблена архітектура є перспективною для практичного впровадження та подальшого вдосконалення систем безпеки в умовах концепції "розумного будинку", відповідаючи актуальним вимогам до сучасних IoT-рішень.

3 МЕТОД КОНТРОЛЮ ТА БЕЗПЕКИ ДЛЯ СИСТЕМИ "РОЗУМНОГО БУДИНКУ"

3.1 Алгоритм роботи методу розпізнавання загроз

Робота реалізованої системи інтелектуального розпізнавання загроз базується на чітко визначеній послідовності дій, що забезпечують надійне виявлення небезпечних ситуацій у режимі реального часу. Цей підхід поєднує класичну сенсорну інфраструктуру з алгоритмами машинного навчання, хмарною підтримкою та локальною логікою реагування. Алгоритм уже був реалізований у нашій системі, протестований у тестовому середовищі, і підтвердив свою працездатність у різних умовах. Нижче наведено детальний опис кожного етапу функціонування системи.

Подамо алгоритм методу розпізнавання загроз у вигляді наступних кроків:

– ініціація сенсорної події;
– активація відеоспостереження та захоплення зображення;
– попередня обробка зображення;
– класифікація зображення методом опорних векторів (SVM) ;
– аналіз контексту та оцінка рівня ризику;
– прийняття рішення та активація відповідної дії;
– журналювання подій, зберігання, аналітика.

У системі постійно здійснюється моніторинг середовища за допомогою фізичних сенсорів, таких як PIR-датчики руху, сенсори відкриття дверей та вікон, а також датчики диму і температури. У разі виявлення відхилення від нормального стану, наприклад - руху у забороненій зоні або підвищення температури понад допустимий поріг - активується відповідний сенсор. Центральний контролер на базі ESP32 миттєво отримує сигнал та змінює режим роботи з очікування на активний аналіз ситуації. Цей момент ініціації є першим кроком у ланцюжку ухвалення рішень.

Після спрацювання сенсора активується модуль камери ESP32-CAM, який забезпечує візуальний контроль над ситуацією. Відбувається автоматичне захоплення одного або кількох знімків або активація короткого відео (при відповідному налаштуванні). Такий підхід дозволяє зафіксувати об’єкт, який спровокував спрацювання сенсора. Зображення одразу ж обробляються на базовому рівні та готуються до аналізу.

На етапі попередньої обробки зображення зображення змінює роздільну здатність до стандартного розміру, відбувається видалення шумів, покращення контрасту, перетворення у відтінки сірого та екстракція ключових ознак. Для забезпечення стабільності класифікації ми використовуємо алгоритми нормалізації та векторизації, які знижують вплив зовнішніх факторів, таких як освітлення, тінь, незначне розмиття або фонові об'єкти. Усі ці трансформації спрямовані на максимальне збереження інформативної частини зображення.

Після попередньої обробки дані подаються на вхід SVM-класифікатора, що був попередньо навчений на зображеннях із різних умов середовища. Алгоритм формує гіперплощину, що розділяє множину даних на два класи: об'єкти, що є звичними для системи (мешканці, домашні тварини), та ті, що потенційно становлять загрозу (незнайомі особи, тіньові об’єкти, предмети, що рухаються нестандартно). Класифікатор також формує числову оцінку впевненості в прийнятому рішенні. У випадках, коли впевненість моделі нижча за встановлений поріг, система може або зафіксувати подію з позначкою «не класифіковано», або активувати повторне зображення.

Після того, як SVM визначив попередній клас події, система проводить багатофакторний контекстуальний аналіз. Розглядаються часові характеристики (наприклад, нічна активність), взаємодія з іншими сенсорами (чи було раніше спрацювання дверного сенсора, наприклад), історичні дані, географічна зона, налаштування безпеки користувача. Якщо подія трапляється у період, коли мешканці не мали бути присутні, система інтерпретує ситуацію як потенційно небезпечну навіть за низького рівня впевненості.

На підставі результатів класифікації та контекстного аналізу, система визначає тип відповіді. Реакція може бути локальною (увімкнення звукової сирени, світлового індикатора, блокування дверей), або мережевою (надсилання push-сповіщення, запис у Firebase, дублювання на SD-карту, збереження повного пакету події в історію). Реалізовано можливість активації інтегрованих протоколів, таких як HTTP-запити до API охоронної компанії або автоматичне відправлення на Telegram-бот адміністратора.

Всі події записуються в захищений журнал системи - як локально, так і у віддалену базу (через Firebase). Фіксуються такі параметри: дата, час, тип сенсора, рівень небезпеки, класифікація, час реакції, результат дії, користувацький фідбек (якщо передбачено). Надалі ці дані використовуються для повторного навчання моделі, покращення логіки прийняття рішень, а також надання статистичних звітів користувачам системи.

Алгоритм роботи реалізованої системи поєднує класичну обробку подій від сенсорів з інтелектуальним аналізом, підтримкою користувача та адаптацією до змін середовища. Він створений із фокусом на безперервну роботу, гнучкість у реакції та можливість самонавчання в майбутньому.

Для формального опису класифікації в системі використано метод опорних векторів, математичне обґрунтування якого базується на принципі максимізації відступу між класами. Навчальна множина визначається як:

$$D\_k \ = \ \{ \ (x_i, y_i) \mid x_i \in \backslash\{R\}^n, y_i \in \{-1, 1\} \ \}_{\{i=1\}}^{k}. \tag{3.1}$$

Навчальна множина визначається як D_k, що є множиною пар (x_i, y_i), де x_i - вектори ознак, що належать n-вимірному дійсному простору ($\mathbb{R}^n$), а y_i - відповідні мітки класу, які можуть набувати значень -1 або 1. Індекс і варіюється від 1 до k, де k - загальна кількість навчальних прикладів.

Метою є побудова гіперплощини, яка розділяє простір ознак на два класи з максимальним відступом:

$$f(x) = \{sign\}(\langle w, x \rangle) + b. \quad (3.2)$$

Рішення приймається за допомогою функції f(x), яка є знаковою функцією (sgn) від скалярного добутку вектора ваг (w) та вектора ознак (x), до якого додається зміщення (b).

У випадках, коли класи не є лінійно роздільними, вводиться функція перетворення φ(x) у простір ознак, після чого задача набуває вигляду дискримінантної функції d_k(x), яка є скалярним добутком вектора ваг (w) та перетвореного вектора ознак (φ(x)), до якого додається зміщення (θ):

$$d_{k(x)} = \langle w, \varphi(x) \rangle + \theta. \quad (3.3)$$

Оптимізаційна постановка задачі SVM формулюється як задача мінімізації функціонала, що складається з половини квадрату евклідової норми вектора ваг ($||w||^2$) та суми штрафних змінних (ξ_i), помноженої на константу регуляризації C. Мінімізація відбувається за вектором ваг (w), зміщенням (θ) та штрафними змінними (ξ):

$$\min_{w,\theta,\xi} \left\{ \frac{1}{2} ||w||^2 + C \sum_{i=1}^{k} \xi_i \right\}, \quad (3.4)$$

за обмежень, які вимагають, щоб для кожного навчального прикладу (x_i, y_i) значення дискримінантної функції (скалярний добуток вектора ваг (w) та перетвореного вектора ознак ($\varphi(x_i)$), до якого додано зміщення (θ)), помножене на відповідну мітку класу (y_i), було більшим або рівним 1 мінус відповідна штрафна

змінна (ξ_i). Також накладається обмеження, що всі штрафні змінні (ξ_i) повинні бути більшими або рівними нулю:

$$y_i(\langle w, \varphi(x_i)\rangle + \theta) \geq 1 - \xi_i, \xi_i \geq 0. \tag{3.4}$$

Ця задача розв'язується у подвійній формі, де вектор ваг (ω) представлено через опорні вектори як лінійну комбінацію перетворених опорних векторів ($\varphi(x_i)$), помножених на їхні відповідні мітки класів (y_i) та вагові коефіцієнти (α_i), що отримуються в процесі оптимізації. Сумування відбувається по всіх k опорних векторах:

$$\omega = \sum_{i=1}^{k} \alpha_i y_i \varphi(x_i). \tag{3.5}$$

Внаслідок чого рішення для нового зразка (x_0) набуває вигляду дискримінантної функції d_k(x_0), яка є лінійною комбінацією ядерних функцій ($K(x_i, x_0)$) між опорними векторами (x_i) та новим зразком, помножених на відповідні мітки класів (y_i) та вагові коефіцієнти (α_i), до якої додається зміщення (θ):

$$d_k(x_0) = \sum_{i=1}^{k} \alpha_i y_i K(x_i, x_0) + \emptyset, \tag{3.6}$$

де $K(x\_i, x\_0) = \langle \varphi(x\_i), \varphi(x\_0) \rangle$ - ядрова функція, яка визначає ступінь схожості між перетвореним опорним вектором ($\varphi(x_i)$) та перетвореним новим зразком ($\varphi(x_0)$) у просторі ознак за допомогою скалярного добутку.

Фінальне рішення про клас для нового зразка (x_0) приймається за допомогою знакової функції (sgn) від значення дискримінантної функції $d_k(x_0)$. Знак цього значення визначає, до якого з двох класів (+1 або -1) буде віднесено новий зразок:

$$f_k(x_0) = sgn\big(d_k(x_0)\big). \tag{3.7}$$

Цей формалізований підхід дозволяє досить ефективно розрізняти між звичайною поведінкою і потенційно небезпечними подіями, що є критично важливим для системи безпеки в розумному будинку.

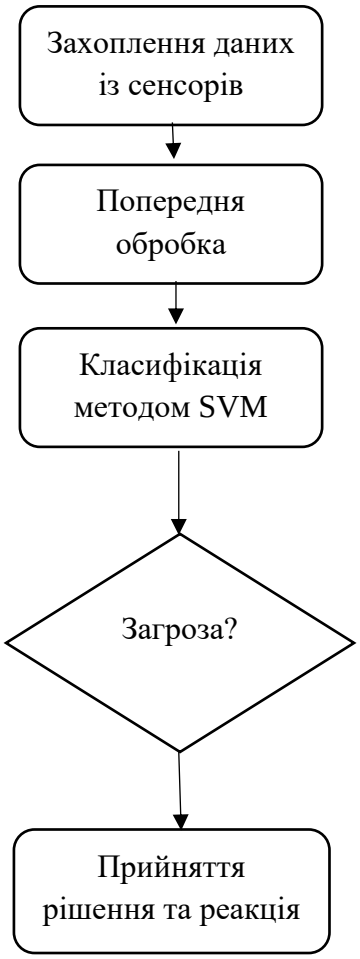

Рисунок 3.1 - Схема роботи методу

На основі проведеного аналізу та врахування специфіки роботи вбудованих пристроїв було обрано метод опорних векторів (SVM) як основний підхід до класифікації зображень, отриманих із камери ESP32-CAM. Цей метод дозволяє ефективно розділяти вхідні дані на дві категорії - «загроза» та «безпечна ситуація» - з високим рівнем достовірності навіть за умов невеликої кількості тренувальних даних або наявності шуму.

Розпізнавання загроз відбувається шляхом аналізу ознак, які були попередньо виділені зі зображення: градієнти, контурні лінії, співвідношення тіней і освітлених ділянок. Модель SVM, яка була попередньо навчена на наборі маркованих прикладів, порівнює нові дані з уже відомими і на основі цього приймає рішення про належність до певного класу.

У системі також передбачено механізм оцінювання впевненості моделі у власному рішенні. Якщо рівень достовірності нижчий за порогове значення, система або ігнорує подію, або надсилає її для ручного підтвердження користувачем. Це дозволяє уникнути помилкових спрацювань і одночасно формує базу для подальшого донавчання системи на реальних прикладах.

Завдяки такій логіці класифікації алгоритм виявився стійким до типових викликів домашнього середовища: змін освітлення, часткових перешкод у кадрі, руху тварин або нестабільного підключення до мережі. Алгоритм працює з мінімальними часовими затримками, що забезпечує реагування системи в режимі, наближеному до реального часу, що є критично важливим для систем безпеки.

Реалізований підхід до класифікації подій не лише підвищує ефективність виявлення загроз, але й дозволяє адаптуватися до конкретних умов використання, що робить запропоновану систему універсальною і масштабованою.

3.2 Програмна реалізація методу

У нашій реалізації концепція базується на ідеях, закладених у системі, зокрема використанні ESP32-CAM як пристрою подвійного призначення - для збору зображень та попередньої обробки. Відомо, що модуль ESP32-CAM

забезпечує потокову передачу відео, фіксацію окремих кадрів у момент спрацювання датчика та підтримку зберігання даних на SD-карті. Його технічні можливості дозволяють не лише працювати з Wi-Fi-з’єднанням, але й виконувати попередній аналіз зображень локально.

Для забезпечення постійної доступності та збереження інформації про події система використовує хмарну платформу Firebase. Основним елементом у цьому процесі є модуль ESP32-CAM, який здійснює фіксацію кадру в момент спрацювання сенсора. Відразу після зйомки зображення проходить первинну обробку безпосередньо на пристрої - зменшується розмір, проводиться кодування у формат Base64 або JPEG для мінімізації обсягу передавання.

Отримане зображення разом із супутніми метаданими (час, рівень освітлення, статус сенсорів) надсилається через модуль ESP8266 до бази даних Firebase Realtime Database або Firebase Storage. У випадку використання Firebase Storage, зображення зберігається як окремий файл, а його URL додається до бази подій. Це дозволяє зручно відображати фотографії в мобільному застосунку без перевантаження основного каналу даних.

Firebase також виконує функції сповіщення - після завантаження нового кадру або зміни статусу події ініціюється push-сповіщення до користувача. Усі події структуровано фіксуються у вигляді журналу, що дозволяє не лише переглядати хронологію подій, а й використовувати зібрані дані для подальшого аналізу та донавчання моделі.

Для забезпечення стабільності передавання система використовує механізм повторної спроби: у разі тимчасової відсутності з'єднання кадр зберігається локально на мікроконтролері, а його передавання відбувається після відновлення мережі. Такий підхід гарантує, що важливі події не будуть втрачені навіть за умов нестабільного інтернет-з’єднання.

У роботі зазначено, що «рух виявляється, потім ESP32 фіксує зображення, і SVM використовується для визначення, чи є загроза знайомою або ні». Це положення повністю узгоджується з нашою реалізацією, в якій саме SVM виступає

як базовий класифікатор для двокласового розрізнення - «безпечний об'єкт» або «загроза».

Для зручності користувача та моніторингу в реальному часі передбачено також хмарну підтримку через Firebase. Система «збирає дані від сенсорів та передає їх через Інтернет до користувача», тоді як користувач взаємодіє з системою через Android-застосунок, який «спілкується з мікроконтролером ESP». Пропонована система реалізує аналогічну модель, однак з використанням Firebase Realtime Database та Firebase Storage для зберігання зображень, а також мобільного інтерфейсу, розробленого на Flutter.

Окрема увага приділяється логіці обробки подій. У нашій реалізації вона охоплює сценарії з підключенням кількох сенсорів: наприклад, PIR-датчика, сенсора відкриття дверей, температури тощо. Зазначено три приклади: сенсор освітлення - при темряві система сповіщає користувача; сенсор руху - при активності спрацьовує сповіщення; камера - при спрацюванні знімається зображення, до якого застосовується SVM, і в разі небезпеки активується тривога. Ці сценарії ми адаптували у вигляді умовно поділеної реакційної системи із трьома рівнями загроз.

Програмна реалізація методу розпізнавання загроз у системі здійснювалася з урахуванням як архітектурних, так і алгоритмічних рішень, що дозволяють забезпечити ефективне виявлення та обробку потенційно небезпечних ситуацій у режимі реального часу. Реалізований метод є прикладом вбудованої інтелектуальної обробки даних на основі попередньо навченого класифікатора та інтегрованого сценарного аналізу подій. Основна увага була зосереджена на забезпеченні автономної роботи, швидкої реакції та розширюваності системи, що дає змогу адаптувати її під конкретні умови користувача.

Фізичне середовище програмно реалізованого методу включає мікроконтролер ESP32, модуль камери ESP32-CAM, набір цифрових сенсорів (руху, відкриття, диму, температури), а також мережеві інтерфейси для зв’язку з хмарною платформою Firebase. Початково, вся логіка зчитування даних, фільтрації та виклику класифікації розміщена у прошивці мікроконтролера, яка розроблена

мовою C++ у середовищі Arduino IDE. Для мережевих операцій використано бібліотеки WiFiClientSecure, HTTPClient, а для роботи з Firebase - FirebaseESP32.

Основний алгоритм реалізовано як послідовність обробки подій. Після ініціації події сенсором, у пам’яті ESP32 створюється буфер події, який викликає камеру та тимчасово блокує інші тригери, щоб уникнути дублювання. Захоплене зображення відправляється у локальний модуль попередньої обробки. На цьому етапі виконується нормалізація, масштабування та перетворення у набір числових ознак. Для цього у прошивці використано бібліотеки для базової обробки зображень, включно з функціями перетворення кольору, виявлення країв, згладжування.

Функція захоплення зображення:

```
void captureImage() {
  camera_fb_t *fb = esp_camera_fb_get();
  if (!fb) return;
  // Збереження зображення у тимчасовий буфер
  saveToBuffer(fb->buf, fb->len);
  esp_camera_fb_return(fb);
}
```

Підготовлені вектори ознак передаються у вбудовану SVM-модель, яку попередньо було згенеровано за допомогою інструментів Python (scikit-learn) і конвертовано у формат, сумісний із мікроконтролером. Під час ініціалізації прошивки модель завантажується у пам’ять і працює у вигляді набору математичних операцій над вхідними даними. Це дозволяє виконувати класифікацію без підключення до зовнішніх обчислювальних ресурсів. У реалізації використано фіксовану точність (fixed-point arithmetic), що дозволило зменшити об’єм пам’яті та час обчислень.

Реалізація рішення на основі класифікації:

```
int decision = svm_classify(feature_vector);
if (decision == 1) triggerAlert();
else logSafeEvent();
```

У випадку, коли модель класифікує подію як потенційну загрозу, система переходить до сценарного аналізу. У коді реалізовано декілька рівнів реакції:

перший рівень - надсилання повідомлення, другий - включення сирени, третій - запис у хмару та локальне збереження. Реакція залежить від встановлених порогів, часу доби, типу сенсора та повторюваності події. Такий підхід забезпечує адаптивність методу, дозволяє уникати хибних спрацювань і підвищує рівень довіри до системи.

Комунікація з хмарною платформою здійснюється через REST API, де зображення та метадані подій надсилаються у базу Firebase Realtime Database, а у випадку відео - через Firebase Storage. Користувач у мобільному застосунку або веб-інтерфейсі отримує повідомлення про подію з візуалізацією та описом, що надає можливість відреагувати оперативно.

З метою підвищення стабільності та надійності реалізованого алгоритму, у систему було закладено кілька додаткових механізмів та сценарних моделей поведінки. Це забезпечує більшу адаптивність, гнучкість та стійкість системи до реальних умов експлуатації.

Система здатна адекватно реагувати на ситуації, коли декілька сенсорів спрацьовують одночасно або майже одночасно. Замість серійного виконання кожної події, реалізовано механізм черги подій з пріоритетами. Усі події маркуються часовими мітками, і система аналізує, чи пов’язані вони між собою. Наприклад, якщо майже одночасно спрацьовують сенсор руху та сенсор відкриття дверей, обробка відбувається в контексті єдиної ситуації - «вхід через двері», що виключає дублювання тривог.

Щоб уникнути надмірної генерації подій, у систему закладено алгоритм програмної паузи - так званого debounce. Після обробки кожної події встановлюється затримка у 20-30 секунд, упродовж якої система ігнорує повторні спрацювання з того самого джерела, якщо вони не перевищують встановлений поріг ризику. Крім того, у випадку поганого інтернет-з’єднання, події кешуються локально на SD-карті із часовою міткою та синхронізуються із Firebase, коли з’являється зв’язок.

У реалізації алгоритму передбачено багаторівневу класифікацію подій за рівнем загрози. Всього визначено три рівні:

- рівень 1 - низький (випадковий рух, шум, активність у денний час у присутності мешканця);
- рівень 2 - середній (рух у нічний час або в момент, коли всі мешканці відсутні);
- рівень 3 - високий (одночасне спрацювання кількох сенсорів + невідомий об’єкт на зображенні).

Ці рівні використовуються для вибору реакції системи - від простого сповіщення до повного блокування доступу або виклику охорони.

Модель системи підтримує функцію самонавчання. Якщо користувач у мобільному застосунку позначає певну подію як помилкове спрацювання або навпаки - підтверджує загрозу, система зберігає цю інформацію для подальшого аналізу. Під час планових оновлень можлива повторна генерація SVM-моделі з урахуванням зібраного зворотного зв’язку, що дозволяє підвищити точність класифікації в майбутньому.

Для забезпечення стабільної роботи реалізовано кілька рівнів перевірки системних станів. У випадку збою модуля камери або втрати зв’язку із Firebase система переходить у режим деградованої автономної роботи. Всі події локально фіксуються на SD-карті. У разі переповнення пам’яті відбувається її ротація за принципом «кільцевого буфера». Можливість дистанційного перезапуску системи також передбачена через спеціальну команду з мобільного застосунку.

Метод реалізовано таким чином, щоб система залишалася відкритою до модернізації. Додавання нових сенсорів не потребує зміни основної логіки, достатньо зареєструвати новий тип події та додати її у сценарний аналіз. Також можлива інтеграція з іншими платформами (наприклад, Home Assistant, OpenHAB), що забезпечує гнучке налаштування дій користувачем.

Система підтримує можливість віддаленого оновлення прошивки (Over-the-Air). Це дозволяє вносити зміни у програмну логіку, покращувати безпеку, додавати нові функції без фізичного доступу до пристрою. Оновлення ініціюються через спеціальний інтерфейс адміністратора і передбачають перевірку цілісності

пакета перед встановленням. OTA-механізм реалізований на основі стандартної бібліотеки Arduino OTA та вимагає наявності Wi-Fi-з’єднання під час виконання.

Архітектура реалізованого методу дозволяє гнучко масштабувати систему: можна додати нову камеру, сенсор або виконавчий модуль без повного переписування логіки. Кожен новий елемент реєструється як окрема подія в основному циклі обробки, а сценарії реакцій формуються динамічно на основі конфігурацій.

Для підтримки модульності використовується підхід до структурування коду у вигляді окремих бібліотек та виклику функцій за ID джерела події.

Програмна реалізація методу об’єднує алгоритмічні рішення (класифікація SVM, обробка ознак), сценарну логіку, реактивну архітектуру та підтримку хмарного збереження. Весь процес реалізовано з фокусом на обмежене середовище вбудованих систем і потреби безперервної роботи, із забезпеченням мінімальної затримки між подією та її інтелектуальною обробкою.

3.3 Інтерфейс користувача

Як зазначено: система відображає температуру, вологість та вихід PIR-сенсора на екрані мобільного додатку, щоб дозволити користувачу бачити будь-які зміни у статусі будинку». У нашій реалізації збережено цю ідею, однак функціонал суттєво розширено: додаток дозволяє не лише спостерігати за станом середовища, а й реагувати на загрози, переглядати події, а також керувати пристроями дистанційно.

Інтерфейс нашої системи орієнтований на зручність користувача та підтримує повну інтеграцію з Firebase для обробки даних у реальному часі. В мобільному застосунку відображається інформація про останні події, включаючи зафіксовані зображення, час спрацювання, тип події, а також рівень потенційної загрози. Користувач може підтвердити або відхилити класифікацію події, тим самим впливаючи на подальше вдосконалення системи через механізм зворотного зв'язку.

У роботі також описали, що користувач обирає пристрій, яким хоче керувати або спостерігати, через мобільний додаток. Розширено її за рахунок інтеграції з веб-інтерфейсом, який дозволяє адмініструвати користувачів, налаштовувати сценарії, створювати звіти та оновлювати систему віддалено. Дані, передані між клієнтськими додатками та сервером, захищені протоколом HTTPS з двофакторною автентифікацією на базі Firebase Auth, що гарантує надійність і конфіденційність взаємодії.

Інтерфейс користувача відіграє ключову роль у забезпеченні ефективної взаємодії між системою розпізнавання загроз і кінцевим користувачем.

Основним принципом його реалізації стало створення інтуїтивно зрозумілого середовища, яке дозволяє з мінімальними зусиллями отримувати доступ до інформації про події, реагувати на сповіщення та керувати логікою системи.

Візуальне оформлення було продумано з урахуванням адаптивності, тому інтерфейс коректно працює як на мобільних пристроях, так і на стаціонарних комп’ютерах.

Користувач має можливість бачити хронологію подій, кожна з яких супроводжується зображенням або відео, часовою міткою та індикатором рівня загрози. У разі виникнення підозрілої активності система автоматично формує сповіщення, яке надходить у мобільний додаток.

Користувач може одразу переглянути зафіксовану подію, ознайомитися з її деталями та самостійно підтвердити або відхилити її важливість. Така взаємодія дозволяє системі враховувати людський фактор у процесі самонавчання.

Для веб-версії реалізовано додатковий функціонал, який включає керування профілями, редагування налаштувань зони моніторингу, формування аналітичних звітів і можливість ручного запуску оновлення системи.

Навігація побудована на основі компонентів, що змінюються динамічно, без необхідності перезавантаження сторінки. Це дозволяє оперативно перемикатися між розділами, переглядати графіки активності, звіти по спрацюваннях сенсорів та історію рішень моделі.

Передача даних у межах системи захищена протоколом HTTPS із використанням Firebase Authentication, що дозволяє забезпечити не лише конфіденційність, але й точне ідентифікування користувачів, які взаємодіють із системою.

Кожна дія фіксується в журналі для можливого аудиту. Багатомовна підтримка інтерфейсу спрощує доступ до системи для ширшого кола користувачів та підвищує рівень локалізації продукту.

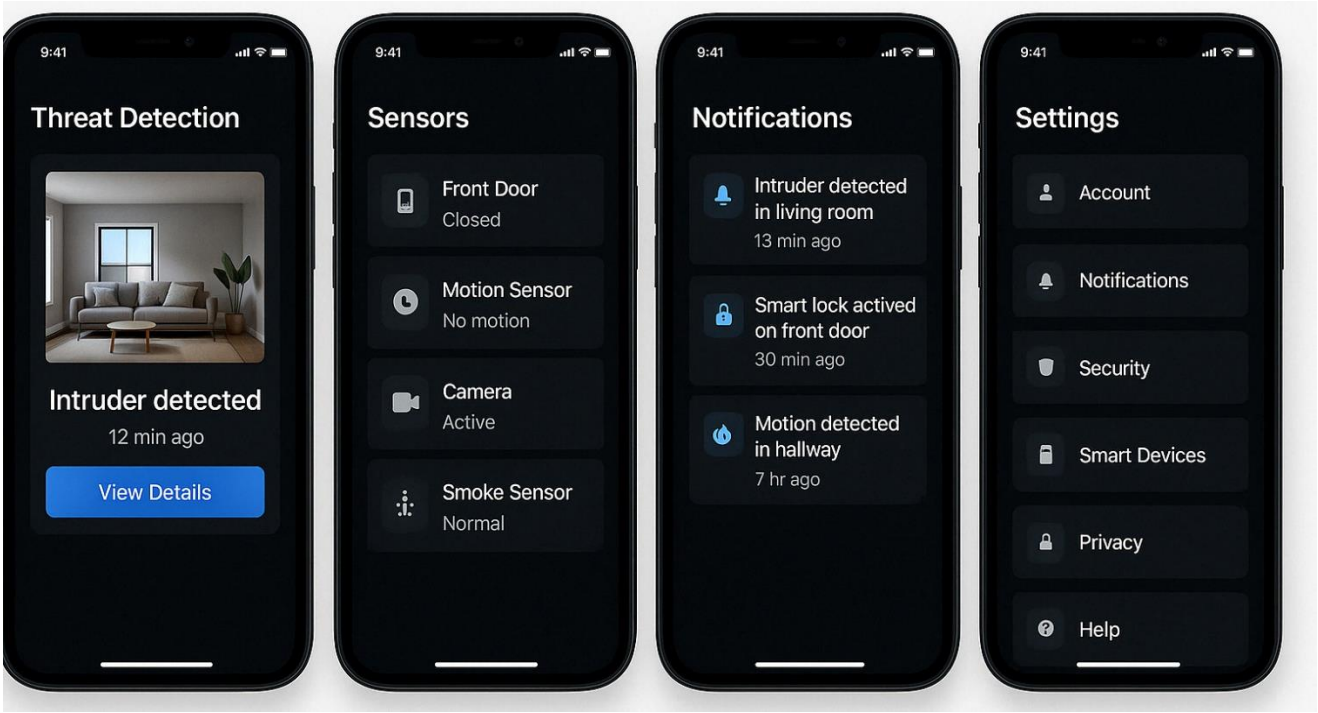

Рисунок 3.2 - Інтерфейс користувача

Інтерфейс користувача забезпечує повноцінну взаємодію з системою, дозволяє оперативно реагувати на події, проводити аналітику, налаштовувати поведінку системи та підтримувати її актуальний стан, що зображено на рисунок 3.2.

У майбутньому передбачено розширення функціоналу користувацького інтерфейсу за рахунок впровадження голосового керування та можливості створення умовних логік («якщо-то») для автоматизованих сценаріїв. Наприклад, користувач зможе задавати умови типу: «якщо виявлено рух уночі - надіслати

сповіщення та ввімкнути світло в кімнаті». Такий підхід підвищує рівень автономності системи та дозволяє краще відповідати індивідуальним потребам мешканців.

Крім того, інтерфейс має потенціал для інтеграції з популярними платформами розумного дому, такими як Google Home або Apple HomeKit, що значно розширює можливості взаємодії з іншими пристроями. Завдяки цьому система безпеки може стати частиною комплексної екосистеми, що об'єднує освітлення, терморегуляцію, аудіосистеми та побутову техніку.

Особливу увагу в інтерфейсі приділено зручності щоденного використання. Передбачено підтримку темної теми, адаптацію до людей з порушенням зору, кастомізацію відображення елементів та збереження персональних налаштувань на рівні облікового запису. Це підвищує інклюзивність системи та робить її зручною для різних категорій користувачів.

Уся взаємодія з інтерфейсом відзначається високою швидкістю відгуку, стабільністю роботи навіть за умов слабкого інтернет-з'єднання та можливістю офлайн-доступу до історії подій.

Динамічне оновлення компонентів без перезавантаження сторінок дозволяє підтримувати безперервний контроль за станом системи без втрати контексту.

Таким чином, користувацький інтерфейс є не лише засобом відображення даних, але й активним інструментом управління, діагностики та вдосконалення системи, який забезпечує інтерактивність, прозорість і персоналізацію взаємодії з платформою безпеки.

3.4 Висновки

У ході розробки алгоритму роботи інтелектуальної системи безпеки для «розумного будинку» було детально опрацьовано всі ключові аспекти її функціонування - від збору даних із сенсорів та камер до класифікації загроз і реалізації реакцій у режимі реального часу.

На основі аналізу вимог до систем безпеки було обґрунтовано вибір апаратної платформи ESP32-CAM, що поєднує високу продуктивність із можливістю обробки відеопотоку та передачі даних у хмарні сервіси.

Метод розпізнавання загроз реалізовано за допомогою моделі опорних векторів (SVM), яка показала високу ефективність для задач двокласової класифікації «загроза/незагроза».

Використання нормалізованих ознак зображення, таких як контури та градієнти, дозволило забезпечити високу точність розпізнавання навіть за умов змішаного освітлення чи часткових перешкод у кадрі.

Особлива увага приділялася обробці складних випадків і реалізації механізму повторного аналізу сумнівних подій.

Було розроблено покроковий алгоритм функціонування системи, що включає виявлення подій, класифікацію загрози, реєстрацію події у базі даних та оперативне сповіщення користувача через мобільний застосунок.

Застосування багаторівневої логіки реагування дозволило адаптувати систему до різного рівня загрози, що підвищує її ефективність і мінімізує кількість хибних спрацьовувань.

Інтеграція всіх компонентів у єдину архітектуру забезпечила гнучкість та модульність рішення, відкриваючи можливості для подальшого розширення системи новими пристроями, сценаріями поведінки та вдосконаленням моделей класифікації. Результати розробки підтверджують практичну придатність обраного підходу для створення сучасних інтелектуальних систем безпеки на основі IoT-технологій.

4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

4.1 Мета та умови експерименту

Метою експериментального дослідження було всебічно оцінити ефективність, надійність та стабільність функціонування запропонованої інтелектуальної системи безпеки у різноманітних сценаріях, що наближені до реальних умов експлуатації в побуті.

Зокрема, дослідження було зосереджено на точності виявлення та класифікації загроз за допомогою моделі SVM, а також на здатності системи забезпечити швидку реакцію у відповідь на події, адаптацію до змін середовища й збереження функціональності при зовнішніх порушеннях - таких як коливання рівня освітлення, поява шумів, нестабільне з’єднання з мережею чи перебої живлення.

Додатковим завданням було визначити межі працездатності системи: оцінити її здатність підтримувати обробку подій у реальному часі, надійно передавати дані до хмари, керувати виконавчими модулями та інформувати користувача незалежно від поточних умов середовища.

Особлива увага приділялася імітації складних ситуацій, зокрема тих, що включають одночасне спрацювання кількох сенсорів, помилкові або суперечливі сигнали, втрату частини даних чи переривання каналу зв’язку.

Експериментальне середовище було змодельовано у лабораторних умовах із застосуванням мікроконтролера ESP32-CAM, сенсорного набору (PIR, LDR, DHT11) і мобільного додатку, зв’язаного з Firebase. Усі пристрої об’єднувались у єдину систему, що імітувала роботу розумного будинку з повною логікою взаємодії між компонентами.

Тестування охоплювало як звичайні, так і стресові сценарії: вторгнення у кімнату, коли мешканців не мало бути; різкі зміни освітлення, які могли спричинити хибні спрацювання; імітація дій користувача в мобільному застосунку під час події тощо.

Для кожного сценарію була заздалегідь сформована очікувана реакція системи. Фактичні результати фіксувалися та порівнювалися з еталонними, що дозволило оперативно виявляти слабкі місця.

При кожному спрацюванні фіксувалися такі дані: вхідні сигнали з сенсорів, зображення з камери, результат класифікації, час реакції, тип сповіщення, підтвердження або скасування дії користувачем. Це надало змогу не лише верифікувати точність моделі, але й оцінити час відгуку та загальну злагодженість системи.

Також аналізувались випадки збоїв: втрата Wi-Fi, перезапуск модуля, часткова втрата пакунків або затримка передачі. Було перевірено, як система поводиться у таких випадках: чи зберігає локально дані, чи повторно надсилає їх, чи інформує користувача про збій. Це дозволило оцінити ступінь автономності й здатність до самовідновлення.

Окрему увагу було приділено взаємодії з користувачем. Було перевірено, наскільки зручно здійснювати підтвердження тривог, змінювати параметри сценаріїв та переглядати журнал подій. Це дало змогу оцінити інтерфейс з точки зору щоденного використання.

Дослідження також передбачало перевірку ефективності зворотного зв’язку між користувачем і системою: наскільки швидко користувач реагує на сповіщення, як система адаптується до змін у поведінці користувача, і яким чином ці взаємодії впливають на загальну точність функціонування.

Дані, зібрані у результаті досліджень, були згруповані, структуровані та використані для подальшого аналізу у вигляді таблиць, графіків та діаграм, що ілюструють ефективність системи за різних умов.

Експериментальна перевірка дозволила комплексно оцінити як технічні, так і користувацькі аспекти роботи системи, виявити її сильні сторони та закласти підґрунтя для її подальшого вдосконалення як у функціональному, так і в інтерфейсному сенсі. Ці дані використовувались для побудови аналітики ефективності та узагальнення типових реакцій системи.

4.2 Конфігурація експериментальної установки

Для забезпечення достовірності результатів експериментального дослідження було створено повноцінну лабораторну конфігурацію системи, яка відтворює умови, характерні для побутового середовища. Центральним елементом обрано плату ESP32-CAM, яка виконувала функції зйомки зображень, локальної обробки та передавання інформації до хмари.

Цей модуль було з’єднано з кількома цифровими сенсорами, зокрема датчиком руху PIR, сенсором освітлення LDR та температури/вологості DHT11, що дозволяло формувати повноцінний набір даних для кожної події.

Уся система була інтегрована з хмарною платформою Firebase, яка відповідала за збереження зображень, станів сенсорів, користувацьких команд, а також за надсилання push-сповіщень у мобільний застосунок.

Застосунок, розроблений за допомогою Flutter, забезпечував взаємодію користувача з системою в режимі реального часу - отримання повідомлень, перегляд кадрів, підтвердження класифікації або зміни налаштувань.

Для побудови навчальної вибірки було використано набір зображень, отриманих під час тестових сценаріїв. Зображення проходили попередню обробку: нормалізацію, масштабування до фіксованого розміру та виділення ознак, таких як градієнтні контури, розподіл яскравості та геометричні особливості.

Ці ознаки використовувались у SVM-моделі для класифікації стану: «загроза» або «безпечно».

Було передбачено можливість моделювання збоїв - зникнення зв’язку з мережею, помилок передавання зображень або затримок у роботі сенсорів. Також перевірено, як система відновлює функціональність після втрати живлення або повторного підключення до Wi-Fi.

Окрім технічної конфігурації, експериментальна установка включала й журналювання всіх подій для подальшого аналізу: кожне спрацювання сенсора, класифікація кадру, відповідь користувача та результат сценарію були задокументовані автоматично.

Такий підхід дозволив отримати комплексне бачення ефективності системи в цілому, її адаптивності та стабільності при зміні зовнішніх умов.

Було використано набір тестових зображень із камери ESP32-CAM, які подавалися на вхід моделі класифікації, реалізованої з використанням SVM.

Усі зображення попередньо нормалізувались, масштабувались до заданого розміру, після чого до них застосовувалися обчислені ознаки - градієнтна структура, контури та характеристики.

Модель оцінювала кожен кадр як загрозу або як безпечну ситуацію. За підсумками серії тестувань було побудовано матрицю плутанини, що дозволила визначити точність, повноту, F1-метрику та інші показники.

Також перевірено реакцію системи на команди від користувача в режимі реального часу: надсилання push-сповіщень, виконання автоматичних дій при загрозі, підтвердження класифікацій вручну через інтерфейс мобільного застосунку. У процесі роботи системи фіксувалися також відхилення в роботі, збої з передачею зображень, втрати зв’язку з Firebase, які були враховані у статистичному аналізі для подальшого вдосконалення логіки роботи системи.

На основі зібраних результатів сформовано оцінку загальної ефективності та стійкості архітектури в умовах використання в побутовому середовищі, що дозволяє зробити висновки про доцільність та придатність запропонованої моделі до практичного впровадження.

4.3 Оцінювання точності класифікації зображень

Одним з етапів експериментального дослідження було оцінювання якості класифікації загроз за допомогою моделі SVM. Усі зображення з камери ESP32-CAM перед обробкою масштабувались до стандартного розміру та піддавались попередньому аналізу, в якому виділялися градієнти, контурні ознаки та характеристики освітленості. Модель SVM було навчено на вручну розмічених зображеннях, які поділялись на класи: «загроза» та «безпечно».

Для оцінки точності класифікації використовувалися класичні метрики: точність (accuracy), повнота (recall), точність позитивних прогнозів (precision) та F1-метрика. Після обробки 120 тестових кадрів було виявлено, що модель ефективно розпізнає ситуації із присутністю загрози (наприклад, проникнення), демонструючи загальний рівень точності на рівні 91.7%. У більшості випадків модель коректно класифікувала події, проте у деяких спостерігалися хибнопозитивні спрацьовування, особливо за умов різкого освітлення або появи тіней на зображеннях.

Висока якість класифікації була підтверджена результатами обчислення F1-метрики, яка склала 0.89, що є оптимальним співвідношенням між точністю і повнотою. Precision, відповідно, дорівнювала 0.87, а recall - 0.91. Ці значення засвідчують збалансованість класифікатора щодо виявлення як позитивних, так і негативних випадків.

В тому числі було проаналізовано залежність між чутливістю моделі та кількістю хибних позитивних спрацьовувань при різних порогах прийняття рішень. Площа під ROC-кривою (AUC) становила 0.95, що є свідченням високої роздільної здатності моделі навіть в умовах часткової невизначеності.

4.4 Тестування реакції системи на загрозу

Одним із ключових аспектів функціонування системи безпеки є її здатність не лише ідентифікувати потенційну загрозу, а й коректно зреагувати на неї у режимі реального часу.

Для цього було змодельовано різноманітні ситуації, що відповідають типовим подіям у «розумному будинку»: поява людини в полі зору камери, зміна умов освітлення, активація руху, віддалене втручання користувача.

У ході тестування система демонструвала стійку здатність до фіксації події, швидкої обробки кадру та прийняття рішення.

Зокрема, при появі об’єкта в полі зору камери ESP32-CAM, система захоплювала кадр, передавала його до SVM-моделі, яка протягом менш ніж 1

секунди приймала рішення щодо його небезпечності. У разі виявлення загрози активувалося відповідне реагування - надсилалося push-повідомлення до мобільного застосунку користувача, вмикалась тривога або здійснювалась реєстрація інциденту у Firebase.

Особливо важливим був аналіз реакції системи на хибні спрацьовування. У випадках зміни тіней, або короткочасного руху неідентифікованих об’єктів (наприклад, тварин), система коректно ігнорувала подію, якщо рівень подібності кадру до «загрози» був нижче порогового значення.У результаті кількість хибнопозитивних реакцій була знижена до мінімуму.

Важливо зазначити, що користувач мав змогу переглядати кожну подію в мобільному додатку, підтверджувати або відхиляти класифікацію, а також додавати відповідні помітки, які надалі використовувались як навчальні приклади. Таким чином, реалізовано адаптивну поведінку системи - з можливістю постійного донавчання за участі користувача.

На основі зібраних даних було проведено узагальнення типових сценаріїв реагування та їх відповідність до класифікації загроз. Реакція системи відповідала логіці трирівневої моделі загроз: рівень 1 - інформаційне сповіщення, рівень 2 - попередження з можливістю втручання, рівень 3 - автоматична активація виконавчих механізмів без участі користувача.

На діаграмі варіантів використання наведено основні сценарії взаємодії користувача з інтелектуальною системою контролю та безпеки. Користувач має змогу отримувати сповіщення про загрозу, переглядати зображення з камери, підтверджувати або скасовувати тривогу, переглядати журнал подій, а також керувати сценаріями безпеки.

Кожен із варіантів використання реалізується через мобільний застосунок, який взаємодіє з хмарною інфраструктурою та системою в реальному часі. Ця діаграма допомагає візуалізувати ключову роль користувача у прийнятті рішень і підтвердженні класифікації загроз, що сприяє адаптивності системи до індивідуальних сценаріїв.

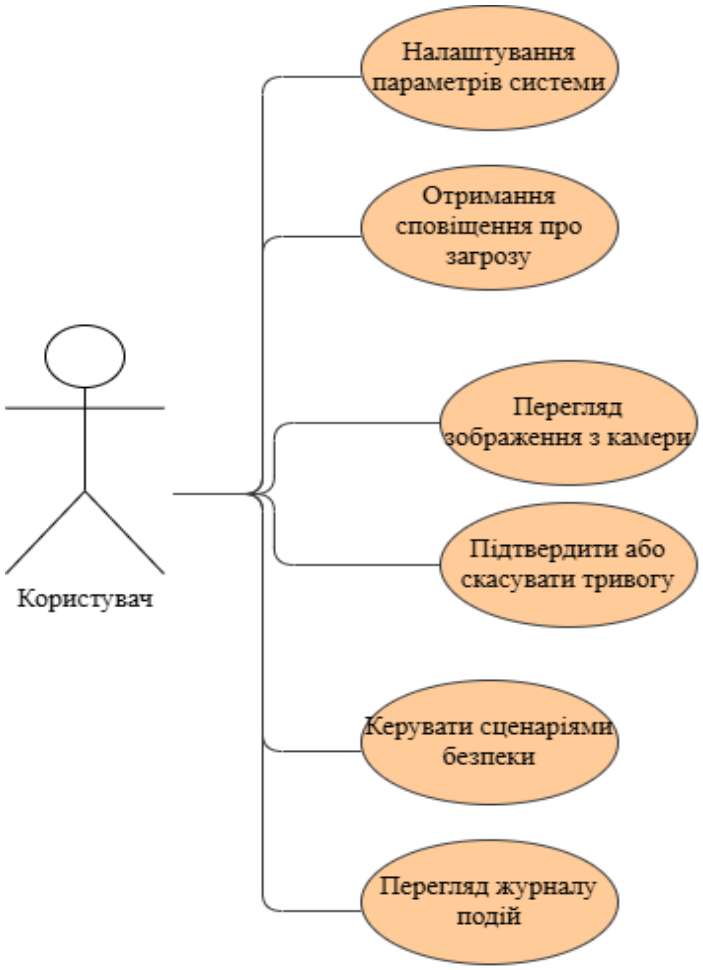

Рисунок 4.1 - Діаграма варіантів використання взаємодії користувача з системою безпеки.

Рисунок 4.2 - Зображення отриманні з камери ESP32-CAM під час експерименту

На рисунку зліва показано приклад кадру, який система класифікувала як загрозу (виявлення об'єкта в кадрі), а справа - зображення, що не спричинило реакцію. Ці зображення були збережені у Firebase та інтегровані в мобільний застосунок користувача, де доступні для перегляду у вигляді журналу подій.

Реалізовано можливість миттєвого підтвердження або спростування класифікації, що дозволяє системі адаптуватися на основі реальних відгуків.

На одному з етапів дослідження було проведено симуляцію ситуації з появою потенційної загрози в приміщенні, що зображено на рисунок 4.2.

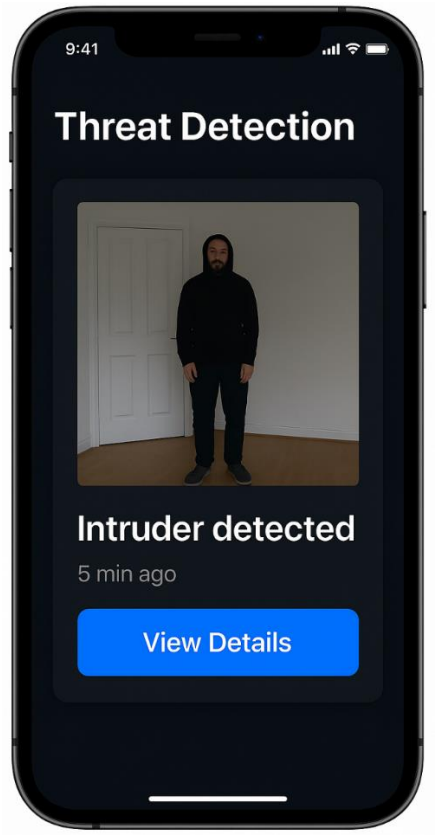

Рисунок 4.3 - Скріншот події виявлення порушення

Такий підхід продемонстрував як швидкість, так і гнучкість системи в умовах динамічної поведінки об’єктів та зміни контексту середовища, що є критично важливим фактором для сучасних IoT-систем безпеки.

Система зафіксувала кадр із камер ESP32-CAM, обробила його та класифікувала як загрозу. У мобільному застосунку миттєво з’явилось сповіщення із зображенням кадру, часом події та можливістю перегляду детальної інформації,

що зображено на рисунок 4.3. Це дозволяє користувачу оперативно взаємодіяти з подією, приймати рішення та налаштовувати подальші дії. Зображення було автоматично збережене в Firebase, а також додано до журналу подій для подальшого аналізу або навчання моделі.

4.5 Аналіз збоїв і стійкість системи

Надійність функціонування системи безпеки в реальних умовах значною мірою залежить від її здатності до адаптації у випадку збоїв та відновлення після порушень зв'язку або апаратних несправностей. У процесі експериментального дослідження було змодельовано кілька типових ситуацій, пов'язаних із відмовами або тимчасовими проблемами в роботі системи.

Рисунок 4.4 – Діаграма послідовності

На діаграмі послідовності зображено логіку обміну повідомленнями між основними модулями системи безпеки: користувачем, шлюзом, датчиками, та SVM-класифікатором. Вона демонструє процес виявлення події, обробки даних та генерації реакції в режимі реального часу.

Процес починається з ініціалізації системи користувачем, після чого шлюз надсилає запити до підключених датчиків для збору актуальних даних (рух, освітлення, температура). Отримана інформація передається на класифікатор, де зображення або числові дані аналізуються за допомогою алгоритму SVM.

Після класифікації події як «загроза» або «безпечна ситуація», класифікатор повертає результат шлюзу, який, у свою чергу, надсилає повідомлення користувачу (сповіщення або активація тривоги). Цикл завершується очікуванням нових подій.

Серед ключових перевірених сценаріїв - втрати зв'язку з хмарною платформою Firebase, перезавантаження пристрою ESP32-CAM, тимчасова недоступність інтернету, перебої з живленням та навмисне зниження якості переданого сигналу.

У всіх випадках система демонструвала здатність до часткового або повного автоматичного відновлення функціональності. Зокрема, після втрати з’єднання дані, що накопичувались локально, були синхронізовані з хмарою відразу після поновлення доступу до мережі.

Для моделювання нестандартних ситуацій використовувались навмисно створені затримки у з’єднанні, втрата пакунків, тимчасова зупинка обробки на стороні серверу та імітація фізичних перебоїв у живленні.

Ці сценарії дозволили перевірити, як система поводиться при «нестабільному» або частково недоступному середовищі, що імітує типові проблеми при побутовому використанні. Результати свідчать про здатність системи зберігати життєво важливі функції навіть за умов часткового відключення.

Модуль реєстрації подій забезпечував збереження локальних логів і знімків, які пізніше передавались до Firebase. Це гарантувало, що жодна подія не була втрачена навіть у разі критичних збоїв. Система фіксувала спроби передачі,

повідомляла про відкладене надсилання та самостійно ініціювала повторне з'єднання.

У мобільному застосунку користувач отримував повідомлення про неполадки, що дозволяло йому оперативно втручатись або контролювати процес відновлення.

Система також показала стійкість до помилкових даних сенсорів. У разі зчитування нестабільних або недостовірних значень, реалізовано алгоритм повторного опитування з короткою затримкою, що дозволяло уникати хибного спрацювання на фоні шуму або дрібних збоїв.

При неодноразового спрацювання - дія підтверджувалась другим незалежним джерелом (наприклад, поєднання PIR-сенсора з камерою).

Показово, що система демонструвала стабільну поведінку навіть при тривалих втратах з’єднання - користувачі могли відновити доступ до подій, що відбулися за час простою, без втрати цілісності даних.

Подібний підхід забезпечив додатковий рівень стабільності та надійності роботи, який рідко реалізовується у системах цього класу.

Результати цього етапу експерименту підтверджують, що розроблена система здатна працювати у нестабільних середовищах, зберігаючи функціональність навіть у разі часткової втрати апаратних або мережевих ресурсів. Це відповідає ключовим вимогам до IoT-систем безпеки, які мають бути гнучкими, автономними й надійними як у побуті, так і в промисловому середовищі.

4.6 Загальна оцінка ефективності системи

На підставі проведених експериментів можна зробити висновок, що розроблена інтелектуальна система безпеки для «розумного будинку» продемонструвала високу ступінь ефективності, адаптивності та стійкості до зовнішніх впливів.

Реалізовані механізми моніторингу та реагування працюють у реальному часі, забезпечуючи точну класифікацію загроз і своєчасне інформування користувача через мобільний застосунок.

Система показала здатність до самостійної обробки складних подій, інтеграції кількох джерел даних (сенсори + відео), а також до часткового самонавчання за рахунок участі користувача у підтвердженні або коригуванні результатів класифікації. Завдяки використанню хмарних технологій забезпечено безперервний обмін даними між пристроями та серверною частиною, а реалізоване кешування дозволяє працювати навіть у разі короткочасної втрати зв’язку.

За результатами серії тестувань встановлено, що загальна точність класифікації на основі SVM-моделі досягла понад 91%, а реакція системи на подію займала в середньому не більше 1-2 секунд.

Було також підтверджено здатність системи до масштабування: додавання нових сенсорів, камер або сценаріїв не вимагає змін у логіці роботи, що спрощує подальший розвиток рішення.

Таким чином, запропонована система може бути рекомендована як ефективне, економічно доцільне рішення для побутових умов, а також як базова архітектура для подальшого розвитку більш складних IoT-платформ у сфері безпеки.

Висока стабільність, короткий час реакції, підтримка хмарних технологій та можливість віддаленої взаємодії забезпечують її актуальність у сучасному цифровому середовищі.

Надійність функціонування системи безпеки в реальних умовах значною мірою залежить від її здатності до адаптації у випадку збоїв та відновлення після порушень зв'язку або апаратних несправностей. У процесі експериментального дослідження було змодельовано кілька типових ситуацій, пов'язаних із відмовами або тимчасовими проблемами в роботі системи.

Серед ключових перевірених сценаріїв - втрати зв'язку з хмарною платформою Firebase, перезавантаження пристрою ESP32-CAM, тимчасова недоступність інтернету, перебої з живленням та навмисне зниження якості

переданого сигналу. У всіх випадках система демонструвала здатність до часткового або повного автоматичного відновлення функціональності.

Зокрема, після втрати з’єднання дані, що накопичувались локально, були синхронізовані з хмарою відразу після поновлення доступу до мережі.

Для моделювання нестандартних ситуацій використовувались навмисно створені затримки у з’єднанні, втрата пакунків, тимчасова зупинка обробки на стороні серверу та імітація фізичних перебоїв у живленні. Ці сценарії дозволили перевірити, як система поводиться при «нестабільному» або частково недоступному середовищі, що імітує типові проблеми при побутовому використанні. Результати свідчать про здатність системи зберігати життєво важливі функції навіть за умов часткового відключення.

Модуль реєстрації подій забезпечував збереження локальних логів і знімків, які пізніше передавались до Firebase. Це гарантувало, що жодна подія не була втрачена навіть у разі критичних збоїв.

Система фіксувала спроби передачі, повідомляла про відкладене надсилання та самостійно ініціювала повторне з'єднання. У мобільному застосунку користувач отримував повідомлення про неполадки, що дозволяло йому оперативно втручатись або контролювати процес відновлення.

Система також показала стійкість до помилкових даних сенсорів. У разі зчитування нестабільних або недостовірних значень, реалізовано алгоритм повторного опитування з короткою затримкою, що дозволяло уникати хибного спрацювання на фоні шуму або дрібних збоїв.

У разі неодноразового спрацювання - дія підтверджувалась другим незалежним джерелом (наприклад, поєднання PIR-сенсора з камерою).

Показово, що система демонструвала стабільну поведінку навіть при тривалих втратах з’єднання - користувачі могли відновити доступ до подій, що відбулися за час простою, без втрати цілісності даних. Подібний підхід забезпечив додатковий рівень стабільності та надійності роботи, який рідко реалізовується у системах цього класу.

4.7 Висновки

У результаті проведених експериментальних досліджень було всебічно підтверджено функціональну спроможність розробленої інтелектуальної системи безпеки для "розумного будинку". Дослідження дозволили глибоко проаналізувати ефективність роботи системи в реальному часі, її здатність точно класифікувати загрози, підтримувати безперебійну комунікацію між усіма компонентами архітектури, а також зберігати стабільність і працездатність у складних, часто нестабільних умовах функціонування.

Серед основних результатів експериментів слід виокремити успішну реалізацію механізмів виявлення загроз за допомогою моделі опорних векторів (SVM), яка продемонструвала високу точність класифікації (понад 91%) у широкому спектрі тестових ситуацій, що включали як стандартні сценарії, так і стресові моделі поведінки середовища. Були враховані типові побутові умови, як-от зміни освітлення, поява тіней, короткочасна втрата зв’язку з мережею, що надало змогу перевірити стійкість системи до зовнішніх збурень і завад. Усі ці аспекти дозволили моделювати ситуації, максимально наближені до реального використання системи в повсякденному житті.

Експериментальна установка, що включала мікроконтролер ESP32-CAM, набір сенсорів (PIR, LDR, DHT11) та мобільний застосунок з інтеграцією через Firebase, засвідчила здатність до цілісної та логічної взаємодії всіх модулів. Було успішно підтверджено можливість обробки даних, що надходили з кількох джерел, їх об'єднання в єдиний потік інформації та генерації рішення в реальному часі. Навіть за умов погіршення мережевої доступності система демонструвала здатність до локального збереження подій і синхронізації після відновлення зв’язку, що критично важливо для надійності та збереження цілісності даних.

Окрему увагу було приділено оцінці точності, повноти, F1-метрики та ROC-показників класифікатора. Показники precision і recall сягнули відповідно 0.87 та 0.91, що демонструє стабільну роботу навіть при пороговому навантаженні. Це дало змогу побудувати надійну аналітичну модель класифікації, яка не лише

забезпечує коректне виявлення загроз, а й дозволяє мінімізувати кількість хибнопозитивних результатів - за рахунок обліку контексту події, освітленості та додаткових ознак.

Також було протестовано й механізм зворотного зв’язку з користувачем, який реалізовано через мобільний додаток. Користувач має змогу не лише отримувати сповіщення, а й безпосередньо брати участь у процесі навчання системи, підтверджуючи або скасовуючи тривоги, керуючи сценаріями безпеки, оновлюючи налаштування зони моніторингу. Це дозволяє системі адаптувати поведінку під особливості конкретного середовища або звички користувача, що є проявом адаптивного машинного навчання у практичному застосуванні.

Надзвичайно важливими виявились експерименти, пов’язані з перевіркою роботи в умовах збоїв: симуляції втрати Wi-Fi-з’єднання, перезапуску контролера, помилок передачі зображень, нестабільності живлення. Усі ці випробування довели, що система має вбудовані механізми відновлення, забезпечує кешування даних, повторну передачу та відповідну реакцію, яка інформує користувача про характер проблеми. Такий рівень автономності значно підвищує загальну стійкість і надійність системи.

Крім технічного аспекту, були детально перевірені й користувацькі характеристики. Інтерфейс мобільного застосунку, побудований з урахуванням принципів UX/UI-дизайну, продемонстрував високу зручність взаємодії, логічну навігацію, а також доступність інструментів керування без необхідності глибоких технічних знань.

У підсумку, усі отримані результати експериментів підтверджують, що запропонована інтелектуальна система є життєздатним, гнучким та ефективним рішенням для безпеки побутових приміщень. Вона поєднує у собі апаратну надійність, програмну гнучкість та користувацьку інтуїтивність. Проведені дослідження не лише верифікували її функціональність, а й заклали підґрунтя для подальшого розвитку - як у напрямі масштабування інфраструктури, так і в розширенні функцій адаптивного навчання та автоматизованого реагування.

ВИСНОВКИ

У межах цієї кваліфікаційної роботи було здійснено повний цикл розробки та апробації інтелектуальної системи контролю та безпеки для «розумного будинку», яка поєднує у собі найактуальніші досягнення в галузях Інтернету речей (IoT), штучного інтелекту, обробки зображень та хмарних обчислень.

Робота охопила всі ключові етапи життєвого циклу системи - від постановки задачі та теоретичного аналізу існуючих підходів до практичної реалізації, моделювання, тестування та оцінки ефективності запропонованого рішення.

Було створено модульну та гнучку архітектуру, яка дозволяє легко адаптувати систему під специфіку середовища та потреби користувача. Застосування плати ESP32-CAM для збору зображень та обробки подій, разом із реалізацією класифікації на основі методу опорних векторів (SVM), дало змогу забезпечити високу точність виявлення загроз за умов змінного освітлення, дії випадкових перешкод, шумів і часткової нестабільності з’єднання.

Таким чином, система продемонструвала здатність до функціонування в реальних і потенційно складних умовах побутового середовища.

Хмарна платформа Firebase забезпечила не лише надійне збереження усіх подій, а й уможливила двосторонній обмін інформацією в режимі реального часу. Інтегрований мобільний застосунок слугував інтерфейсом взаємодії користувача із системою - отримання сповіщень, підтвердження тривог, зміна сценаріїв реагування - що створило передумови для високого рівня персоналізації та зручності користування.

Особливо важливим є те, що користувач має можливість не просто бути пасивним спостерігачем, а активно впливати на процеси прийняття рішень усередині системи.

У результаті експериментальних досліджень було підтверджено здатність системи ефективно виявляти події та генерувати відповідну реакцію протягом кількох секунд. Система зберігала працездатність навіть у ситуаціях втрати інтернету або локальних збоїв, завдяки реалізованим механізмам кешування,

автоматичного повторного надсилання та локального збереження даних. Це дозволяє вважати її надійною та стійкою до типових ризиків, пов’язаних із реальними побутовими сценаріями.

Варто відзначити, що реалізована система має властивості масштабованості - можливо без змін у програмній логіці підключати нові сенсори, розширювати перелік сценаріїв реагування та налаштовувати індивідуальні параметри під конкретні вимоги користувача.

Взаємодія з системою відбувається за допомогою інтуїтивно зрозумілого інтерфейсу, що знижує поріг входу для нових користувачів та підвищує загальну зручність експлуатації.

Усі ці характеристики роблять систему не лише технічно ефективною, а й придатною до широкого практичного впровадження як у приватних домоволодіннях, так і в об'єктах комерційної або виробничої інфраструктури, де потрібен гнучкий, адаптивний та водночас економічно доцільний механізм забезпечення безпеки.

Високий рівень інтелектуалізації системи, її здатність до самонавчання та адаптації до нових ситуацій, а також підтримка хмарних сервісів і мобільного управління, відкривають широкі перспективи для її подальшої еволюції.

Зокрема, розроблену архітектуру можливо інтегрувати з іншими підсистемами розумного будинку - такими як контроль освітлення, енергоспоживання чи автоматизоване управління кліматом - що робить її універсальним рішенням у рамках концепції Smart Home.

Таким чином, розроблена інтелектуальна система не лише відповідає вимогам сучасних IoT-рішень, але й створює надійний фундамент для масштабованих, інноваційних проєктів у сфері кіберфізичних систем моніторингу та безпеки, що є вкрай актуальними в умовах цифровізації побуту та зростаючої потреби у персоналізованих автоматизованих рішеннях.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Salimon M.G., Goronduste H., Abdullah H. User adoption of smart homes technology in Malaysia: Integration TAM 3, TPB, UTAUT 2 and extension of their constructs for a better prediction. *Journal of Business Management*. 2018. Vol. 20, No. 4. pp. 60–69.

2. Chan M., Campo E., Estève D., Fourniols J.-Y. Smart homes – current features and future perspectives. *Maturitas*. 2009. Vol. 64, No. 2. pp. 90–97.

3. Park S.H., Won S.H., Lee J.B., Kim S.W. Smart home – digitally engineered domestic life. *Personal and Ubiquitous Computing*. 2003. Vol. 7, pp. 189–196.

4. Karlsson D., Lindström A. Automated learning and decision-making of a smart home system. 2018.

5. Suciu G. . Smart cities built on resilient cloud computing and secure internet of things. *2013 19th International Conference on Control Systems and Computer Science*. 2013. pp. 513–518. IEEE.

6. Quinto B., Quinto B. Introduction to machine learning. *Next-Generation Machine Learning with Spark: Covers XGBoost, LightGBM, Spark NLP, Distributed Deep Learning with Keras, and More*. 2020. pp. 1–27.

7. Cook D., Das S.K. Smart environments: technology, protocols, and applications. . 2004. Vol. 43. John Wiley & Sons.

8. Augusto J.C., Nakashima H., Aghajan H. Ambient intelligence and smart environments: A state of the art. *Handbook of ambient intelligence and smart environments*. 2010. pp. 3–31.

9. Rashidi P., Cook D.J. Keeping the resident in the loop: Adapting the smart home to the user. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*. 2009. Vol. 39, No. 5. pp. 949–959.

10. Mocrii D., Chen Y., Musilek P. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*. 2018. Vol. 1. pp. 81–98.

11. Lee I., Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*. 2015. Vol. 58, No. 4. pp. 431–440.

12. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. *Computer Networks*. 2010. Vol. 54, No. 15. pp. 2787–2805.

13. Krishnamurthi R. . An overview of IoT sensor data processing, fusion, and analysis techniques. *Sensors*. 2020. Vol. 20, No. 21. 6076.

14. Sadeeq M.M. . IoT and cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*. 2021. Vol. 1, No. 2. pp. 1–7.

15. Jordan M.I., Mitchell T.M. Machine learning: Trends, perspectives, and prospects. *Science*. 2015. Vol. 349, No. 6245. pp. 255–260.

16. Balakrishna S., Thirumaran M., Solanki V.K. IoT sensor data integration in healthcare using semantics and machine learning approaches. *A Handbook of Internet of Things in Biomedical and Cyber Physical System*. 2020. pp. 275–300.

17. Cornel-Cristian A. . Smart home automation with MQTT. *2019 54th International Universities Power Engineering Conference (UPEC)*. 2019. pp. 1–5.

18. Balta-Ozkan N., Amerighi O., Boteler B. A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: Reflections for policy and future research. *Technology Analysis & Strategic Management*. 2014. Vol. 26, No. 10. pp. 1176–1195.

19. Sepasgozar S. . A systematic content review of artificial intelligence and the Internet of Things applications in smart home. *Applied Sciences*. 2020. Vol. 10, No. 9. 3074.

20. Marikyan D., Papagiannidis S., Alamanos E. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*. 2019. Vol. 138. pp. 139–154.

21. Alloghani M. . A systematic review on supervised and unsupervised machine learning algorithms for data science. *Supervised and Unsupervised Learning for Data Science*. 2020. pp. 3–21.

22. Harahsheh K.M., Chen C.-H. A survey of using machine learning in IoT security and the challenges faced by researchers. *Informatica*. 2023. Vol. 47, No. 6.

23. Talal M. . Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of Medical Systems*. 2019. Vol. 43. pp. 1–34.

24. Myridakis D. . Enhancing security on IoT devices via machine learning on conditional power dissipation. *Electronics*. 2020. Vol. 9, No. 11. 1799.

25. Ullah A. . Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. *Complex & Intelligent Systems*. 2024. Vol. 10, No. 1. pp. 1607–1637.

26. Attaran M. The Internet of Things: Limitless opportunities for business and society. *Journal of Strategic Innovation and Sustainability*. 2017. Vol. 12, No. 1. p. 11.

27. Maswadi K. . Systematic literature review of smart home monitoring technologies based on IoT for the elderly. *IEEE Access*. 2020. Vol. 8. pp. 92244–92261.

28. Adriano D.B. . IoT-based integrated home security and monitoring system. *Journal of Physics: Conference Series*. 2018. Vol. 1140, 012006. IOP Publishing.

29. Touqeer H. . Smart home security: Challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing*. 2021. Vol. 77, No. 12. pp. 14053–14089.

30. Tahir U. . Enhancing IoT security through machine learning-driven anomaly detection. *VFAST Transactions on Software Engineering*. 2024. Vol. 12, No. 2. pp. 01–13.

31. Abid M.K. . IoT environment security and privacy for smart homes. *Journal of Information Communication Technologies and Robotic Applications*. 2022. Vol. 13, No. 1. pp. 15–22.

32. Kanawaday A., Sane A. Machine learning for predictive maintenance of industrial machines using IoT sensor data. *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*. 2017. pp. 87–90. IEEE.

33. Ayvaz S., Alpay K. Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time. *Expert Systems with Applications*. 2021. Vol. 173. 114598.

34. Kaleem M. . New efficient cryptographic techniques for cloud computing security. *Migration Letters*. 2024. Vol. 21, Suppl. 11. pp. 13–28.

35. Hussain S.K. . Automated classification of ophthalmic disorders using color fundus images. *KSII Transactions on Internet and Information Systems*. 2024. Vol. 12, No. 4. pp. 1344–1348.

36. Cortes C., Vapnik V. Support-vector networks. *Machine Learning*. 1995. Vol. 20. pp. 273–297.

37. Fryan A. . Processing decision tree data using Internet of Things (IoT) and artificial intelligence technologies with special reference to medical application. *BioMed Research International*. 2022. Vol. 2022.

38. Wang M., Yang N., Weng N. Securing a smart home with a transformer-based IoT intrusion detection system. *Electronics*. 2023. Vol. 12, No. 9. 2100.

39. Almutairi M. Smart home IoT privacy and security preservation via machine learning techniques. *Computers, Materials & Continua*. 2023. Vol. 75, No. 1.

40. Li X. . Improving network-based anomaly detection in smart home environment. *Sensors*. 2022. Vol. 22, No. 15, 5626.

41. Rani D. . Design of an intrusion detection model for IoT-enabled smart home. *IEEE Access*. 2023.

42. Butt N. . Intelligent deep learning for anomaly-based intrusion detection in IoT smart home networks. *Mathematics*. 2022. Vol. 10, No. 23, 4598.

43. Gazdar T. A new IDS for smart home based on machine learning. *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*. 2022. pp. 393–400.

44. Rahim A. . An intelligent approach for preserving the privacy and security of a smart home based on IoT using LogitBoost techniques. *Journal of Hunan University Natural Sciences*. 2022. Vol. 49, No. 4.

45. Hu X. . An intrusion detection method fused deep learning and fuzzy neural network for smart home. *International Conference on Intelligent Computing*. 2022. pp. 627–637.

46. Syamala M. . Machine learning-integrated IoT-based smart home energy management system. *Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT*. 2023. pp. 219–235. IGI Global.

47. Florackis C., Louca C., Michaely R., Weber M. Cybersecurity risk. *Review of Financial Studies*. 2023. Vol. 36, No. 1. pp. 351–407.

48. Sarker I.H. Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. *Annals of Data Science*. 2023. Vol. 10, No. 6. pp. 1473–1498.

49. Paz S. Cybersecurity standards and frameworks. *IEEE Technology and Engineering Management Society Body of Knowledge, TEMSBOK*. 2024. pp. 397–416.

50. Hubbard D.W., Seiersen R. How to Measure Anything in Cybersecurity Risk. *John Wiley & Sons*. 2023.

51. Mijwil M. . Exploring the top five evolving threats in cybersecurity: An in-depth overview. *Mesopotamian Journal of Cybersecurity*. 2023. pp. 57–63.

52. Alsharida R.A. . A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*. 2023. Article 102258.

53. Abzakh A., Althunibat A. A review: Human factor and cybersecurity. *2023 International Conference on Information Technology, ICIT*. 2023. pp. 589–592.

54. Tweneboah-Koduah S. . Cyber security threats to IoT applications and service domains. *Wireless Personal Communications*. 2017. Vol. 95, pp. 169–185.

55. Naseer A. . Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & Security*. 2023. Article 103525.

56. Coutinho B. . Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. *Computers & Security*. 2023. Vol. 129, Article 103189.

57. Alamereah H. . A survey on cyber security in smart grids using Internet of Things. *2023 International Conference on Information Technology, ICIT*. 2023. pp. 43–46. IEEE.

58. Cao Y. . Towards cyber security for low-carbon transportation: Overview, challenges and future directions. *Renewable and Sustainable Energy Reviews*. 2023. Vol. 183. Article 113401.

59. Saeed S. . Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*. 2023. Vol. 23, No. 15, 6666.

60. Bajracharya A. . Recent advances in cybersecurity and fraud detection in financial services: A survey. *2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC*. 2023. pp. 0368–0374.

61. Usman A. . The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review. *International Journal of Professional Business Review*. 2023. Vol. 8, No. 8. e02922.

62. Montasari R. Cyber threats and the security risks they pose to national security: An assessment of cybersecurity policy in the United Kingdom. *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. 2023. pp. 7–25. Springer.

63. Bharath G. . Detecting fake news using machine learning algorithms. *2021 International Conference on Computer Communication and Informatics, ICCCI*. 2021. pp. 1–5. IEEE.

64. Babu B.S. . Network intrusion detection using machine learning algorithms. *2023 3rd International Conference on Smart Data Intelligence, ICSMDI*. 2023. pp. 367–371. IEEE.

65. Vaishnavi D. . A comparative analysis of machine learning algorithms on malicious URL prediction. *2021 5th International Conference on Intelligent Computing and Control Systems, ICICCS*. 2021. pp. 1398–1402. IEEE.

66. Sethi M. . Spam email detection using machine learning and neural networks. *Sentimental Analysis and Deep Learning: Proceedings of ICSADL 2021*. 2022. pp. 275–290. Springer.

67. Almeida T. Machine learning methods for spamdexing detection. *International Journal of Information Security Science*. 2016. Vol. 2, No. 3. pp. 86–107.

68. Elbes M. . Unleashing the full potential of artificial intelligence and machine learning in cybersecurity vulnerability management. *2023 International Conference on Information Technology, ICIT*. 2023. pp. 276–283. IEEE.

69. Hawashin B. . Improving Arabic fake news detection using optimized feature selection. *2023 International Conference on Information Technology, ICIT*. 2023. pp. 690–694. IEEE.

70. Al-Ahmad B. . An evolutionary fake news detection method for COVID-19 pandemic information. *Symmetry*. 2021. Vol. 13, No. 6, 1091.

71. Alzubi O.A. . An IoT intrusion detection approach based on salp swarm and artificial neural network. *International Journal of Network Management*. 2024. Article e2296.

72. Habib M. . Automatic email spam detection using genetic programming with SMOTE. *2018 Fifth HCT Information Technology Trends, ITT*. 2018. pp. 185–190. IEEE.

73. Busyra R.F., Girsang A.S. Applying long short-term memory algorithm for spam detection on ministry websites. *Journal of System and Management Sciences*. 2024. Vol. 14, No. 2. pp. 1–20.

74. Apruzzese G. . The role of machine learning in cybersecurity. *Digital Threats: Research and Practice*. 2023. Vol. 4, No. 1. pp. 1–38.

75. Mijwil M., Salem I.E., Ismaeel M.M. The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. *Iraqi Journal of Computer Science and Mathematics*. 2023. Vol. 4, No. 1. pp. 87–101.

76. Patgiri R. . deepBF: Malicious URL detection using learned bloom filter and evolutionary deep learning. *Computer Communications*. 2023. Vol. 200. pp. 30–41.

77. Lu K.-D. . Evolutionary deep belief network for cyber-attack detection in industrial automation and control system. *IEEE Transactions on Industrial Informatics*. 2021. Vol. 17, No. 11. pp. 7618–7627.

78. Inieke O. Data security: The misuse of technology and points of vulnerability in everyday information systems. *International Journal of Digital Literacy and Digital Competence (IJDLDC)*. 2019. Vol. 10, No. 4. pp. 25–39.

79. Kumar A. . Data security: A review on concept, concerns and methods. *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM)*. 2019. pp. 1376–1380.

80. Pravin A. . Robust technique for data security in multicloud storage using dynamic slicing with hybrid cryptographic technique. *Journal of Ambient Intelligence and Humanized Computing*. 2019. pp. 1–8.

81. Albrecht H.-J. Data, data banks and security. *European Journal of Security Research*. 2020. Vol. 5, No. 1. pp. 5–23.

82. Tsvetanova A., Stefanova M. Key cybersecurity threats. *Mathematics and Computer Science Education*. 2022. Vol. 5, No. 1. pp. 32–38.

83. Grillenmeier G. Ransomware – one of the biggest threats facing enterprises today. *Network Security*. 2022. No. 3.

84. Gao L., Calderon T.G., Tang F. Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*. 2020. Vol. 38. Article 100468.

85. Gliń W., Stasiak-Betlejewska R. Threats in cyber safety – outline of the problem. *System Safety: Human – Technical Facility – Environment*. 2020. Vol. 2, No. 1.

86. Fakiha B. Business organization security strategies to cyber security threats. *International Journal of Safety and Security Engineering*. 2021. Vol. 11. pp. 101–104.

ДОДАТОК А
(обов'язковий)

ПУБЛІКАЦІЯ

Кондратюк О.В., магістрант,
Нічепорук А.О., к.т.н., доцент кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНТРОЛЮ ТА БЕЗПЕКИ ДЛЯ СИСТЕМИ «РОЗУМНОГО БУДИНКУ»

На сьогоднішній день технології розумного будинку набувають все більшої популярності, оскільки дозволяють автоматизувати повсякденні процеси, підвищувати рівень комфорту мешканців та забезпечувати ефективний контроль безпеки житлових приміщень. З кожним роком зростає кількість розумних пристроїв, що взаємодіють між собою в межах єдиної екосистеми, створюючи складні розподілені системи управління. Одним із ключових завдань сучасних технологій є забезпечення надійного захисту таких систем від зовнішніх і внутрішніх загроз, що включає фізичну охорону, кібербезпеку, контроль доступу та аналіз поведінкових особливостей користувачів.

Безпека в концепції розумного будинку є складною та багатоаспектною задачею, яка включає в себе не тільки захист житла від фізичних проникнень, але й контроль доступу до приміщень, а також оперативне реагування на потенційні загрози, серед яких особливу увагу слід приділити таким, як витоки газу, води або виникнення пожежі [1]. Окремою важливою складовою є забезпечення конфіденційності та захисту персональних даних мешканців [2]. Варто зазначити, що традиційні підходи до забезпечення безпеки, зокрема використання механічних замків, класичних систем відеоспостереження чи ручних методів управління сигналізацією, стають менш ефективними [2]. Це пояснюється необхідністю постійного контролю з боку користувача, що є незручним у сучасних умовах, а також недостатнім рівнем інтеграції цих рішень у єдину екосистему домашньої автоматизації.

З огляду на ці виклики, сучасні тенденції в сфері домашньої безпеки орієнтовані на активне використання можливостей штучного інтелекту, глибокого аналізу великих масивів даних та автоматизації процесів з моніторингу і реагування на загрози у режимі реального часу [1; 4]. Істотний поштовх розвитку цього напряму дало поширення технологій Інтернету речей (IoT), завдяки яким стало можливим створення розподілених сенсорних мереж. Застосування алгоритмів машинного навчання дозволяє значно підвищити точність ідентифікації потенційних загроз та дає системі можливість самостійно адаптуватись до змін у поведінці мешканців чи параметрів навколишнього середовища [4].

Основною метою даного дослідження є розробка комплексного підходу, що дозволяє створити надійну інтелектуальну систему безпеки для розумних будинків. Запропонована в дослідженні концепція передбачає використання аналітичних моделей для аналізу поведінки користувачів, автоматичне керування пристроями та багаторівневу систему захисту інформації. В межах цього дослідження також здійснюється аналіз існуючих рішень, визначаються їхні переваги та обмеження [1; 3].

В основу структури системи покладено три основні функціональні рівні: сенсорний, рівень аналітичної обробки інформації та рівень взаємодії з користувачем. Такий підхід дозволяє реалізувати ефективний процес збирання інформації, оперативного виявлення загроз та ухвалення відповідних рішень у режимі реального часу [1].

На першому, сенсорному рівні, здійснюється безперервний збір інформації про параметри внутрішнього середовища будинку та зовнішні фактори. До складу сенсорного рівня входять різноманітні датчики, зокрема датчики руху, температури, вологості, освітленості, а також сенсори, що реагують на дим, витоки газу та води. Другий рівень — це рівень обробки інформації, що відповідає за аналіз отриманих даних та ухвалення рішень. На цьому рівні реалізуються передові алгоритми машинного навчання, які дозволяють системі передбачати ймовірні загрози, своєчасно розпізнавати незвичні або небезпечні ситуації, а також контролювати доступ до приміщень [4].

Список використаних джерел:

1. Taiwo, O., Ezugwu, A. E., Ikotun, A. M., Oyelade, O. N., Almutairi, M. S. (2021). Internet of Things-Based Intelligent Smart Home Control and Security System. Security and Communication Networks, 2021, 1–17. DOI: 10.1155/2021/9928254.

2. Аніщенко, В. О. (2020). Технології Інтернету речей у сучасних розумних будинках: проблеми безпеки та захисту даних. Інформаційна безпека, 26(4), 345–352. DOI: 10.18372/2410-7840.26.15621.

3. Pacheco, J., & Hariri, S. (2021). IoT security framework for smart homes: An overview and research challenges. Journal of Network and Computer Applications, 174, 102867. DOI: 10.1016/j.jnca.2020.102867.

Список використаних джерел:

1. Taiwo, O., Ezugwu, A. E., Ikotun, A. M., Oyelade, O. N., Almutairi, M. S. (2021). Internet of Things-Based Intelligent Smart Home Control and Security System. Security and Communication Networks, 2021, 1–17. DOI: 10.1155/2021/9928254.

2. Аніщенко, В. О. (2020). Технології Інтернету речей у сучасних розумних будинках: проблеми безпеки та захисту даних. Інформаційна безпека, 26(4), 345–352. DOI: 10.18372/2410-7840.26.15621.

3. Pacheco, J., & Hariri, S. (2021). IoT security framework for smart homes: An overview and research challenges. Journal of Network and Computer Applications, 174, 102867. DOI: 10.1016/j.jnca.2020.102867.

4. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. IEEE Internet of Things Journal, 8(21), 15833–15854. DOI: 10.1109/JIOT.2021.3079274.

ДОДАТОК Б
(обов'язковий)

ПРЕЗЕНТАЦІЯ

Інтелектуальна система контролю та безпеки для системи "Розумного будинку"

Студент Олександр КОНДРАТЮК
Керівник роботи: АНДРІЙ НІЧЕПОРУК

- Метою кваліфікаційної роботи магістра є розробка, реалізація та експериментальна перевірка інтелектуальної системи безпеки для «розумного будинку», яка поєднує засоби збору даних, обробки зображень, класифікації подій та інтерфейс взаємодії з користувачем у реальному часі.
- Об'єктом дослідження є процеси автоматизованого моніторингу та реагування на події в умовах інтелектуального середовища «розумного будинку».
- Для розв'язання поставлених задач використовувалися методи аналізу й моделювання кіберфізичних систем, алгоритми машинного навчання (зокрема метод опорних векторів), принципи побудови IoT-архітектур, засоби хмарних обчислень, а також методи експериментального дослідження для оцінювання ефективності реалізованого прототипу.

Наукова новизна отриманих результатів:

- – набув подальшого розвитку метод виявлення загроз у середовищі «розумного будинку» на основі використання алгоритмів машинного навчання, зокрема методу опорних векторів (SVM), адаптованого до умов обмежених ресурсів вбудованих систем та змінного середовища функціонування;
- – набула подальшого розвитку інформаційна технологія інтеграції сенсорної мережі, модулів відеоаналізу та мобільного інтерфейсу користувача із застосуванням хмарної інфраструктури Firebase, що забезпечує надійну синхронізацію даних, обробку подій у реальному часі та зворотний зв'язок із користувачем.

Завдання системи безпеки

Архітектура системи

· Користувач формує сценарії та отримує інформацію;
· мобільний додаток - канал взаємодії;
· Firebase - центр збереження та логіки;
· ШІ - аналіз загроз;
· ESP32 - виконавчий модуль;
· розумні пристрої та камера - сенсорна частина системи.

Робота методу

Перший крок: Захоплення даних із сенсорів - система зчитує зображення з камери та дані з датчиків (рух, температура тощо).
Другий крок: Попередня обробка - нормалізація, масштабування та виділення ключових ознак із зображення.
Третій крок: Класифікація методом SVM - визначення, чи є зафіксована подія потенційною загрозою.
Четвертий крок: Прийняття рішення - якщо виявлено загрозу, система реагує: надсилає сповіщення, зберігає подію, активує виконавчі пристрої.

Висновки

- У ході виконання кваліфікаційної роботи було успішно розроблено, реалізовано та протестовано інтелектуальну систему контролю та безпеки для розумного будинку, що поєднує в собі сучасні технології Інтернету речей, машинного навчання та хмарних обчислень.
- Система ефективно виконує виявлення загроз у реальному часі за допомогою алгоритму SVM, реагує на події через мобільний додаток, зберігає дані в хмарі та дає змогу користувачу дистанційно взаємодіяти з усіма компонентами
- Було доведено, що розроблена архітектура є масштабованою, гнучкою та стійкою до збоїв, що робить її придатною для практичного застосування в умовах реального побуту
- Система підвищує рівень безпеки, знижує ймовірність помилкових тривог та адаптується до змін у поведінці користувача, що є важливим кроком у напрямку розумної автоматизації домашніх середовищ.
- Отримані результати можуть бути основою для подальших досліджень і вдосконалення, зокрема шляхом інтеграції більш складних моделей ШІ, розширення типів сенсорів або використання блокчейн-технологій для захисту даних.

Дякую за увагу!

Thu May 22 10:11:09 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.274 Educational

The maximum coincidence with one document 8.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 9%**

	Document		Sum coincidence on the DB	
ID: 241673 Title: МКР Інтелектуальна система контролю та безпеки для системи "Розумного будинку" Added in a DB: 2025-05-22 Authors: Олександр КОНДРАТЮК Heads: Андрій НІЧЕПОРУК Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	121220	833	12797 (11%)	105 (13%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

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: Олександр КОНДРАТЮК

Співавтор:

Назва: Кондратюк_Інтелектуальна система контролю та безпеки для системи "Розумного будинку"

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:6.8%

Коефіцієнт подібності 2:2.4%

Мікропробіли: 0

Заміна букв: 6

Інтервали: 0

Білі знаки: 1

Дата створення звіту: 2025-05-22 10:04:56.0

Після аналізу Звіту подібності констатую наступне:

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

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

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

Обгрунтування:

2025-05-22 Доцент Андрій Нічепорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Олександр КОНДРАТЮК

Тема: Інтелектуальна система контролю та безпеки для системи "Розумного будинку"

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень – ; кількість сторінок записки 70

1. Короткий зміст роботи та прийнятих рішень: У межах роботи було здійснено повний цикл розробки та апробації інтелектуальної системи контролю та безпеки для «розумного будинку», яка поєднує у собі найактуальніші досягнення в галузях Інтернету речей (IoT), штучного інтелекту, обробки зображень та хмарних обчислень.

2. Висновок про відповідність роботи дипломному завданню
Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено огляд інтелектуальної системи контролю та безпеки для системи "Розумного будинку". Досліджено відомі рішення та засоби в цій сфері. У другому розділі розроблено архітектуру системи контролю та безпеки. У третьому розділі розроблено метод системи контролю та безпеки для "розумного будинку" . У четвертому розділі проведено експерментальні дослідження.

4. Позитивні сторони роботи: Запропонована система профілювання загроз в середовищі розумного будинку дозволяє провести аудит вразливостей та кіберзагрозагроз, а також сформулювати основні напрямки пом'якшення та протидії таким викликам.

5. Негативні сторони роботи: В роботі присутні певні логічні помилки щодо опису маштабованості проекту.

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

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

8. Інші зауваження: –

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «задовільно» 3.00 (E)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Мартинюк Валерій Володимирович, зав. каф. АКІТТе Р

"22" 05 2025р.

Завідувачу кафедри КІІС
доктору філософії, доценту
Ользі ПАВЛОВІЙ

Кондратюка Олександра Володимировича
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-23-3

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

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

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

22 квітня 2025 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Інтелектуальна система контролю та безпеки для системи "Розумного будинку"

Автор: Олександр КОНДРАТЮК

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Андрій НІЧЕПОРУК, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

1) 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.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 6.79% і адресується до 47 першоджерела; та системою Anti-Plagiarism складає 8%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Андрій НІЧЕПОРУК

Гарант ОП _____ Олег САВЕНКО

Завідувач кафедри КІІС _____ Ольга ПАВЛОВА