Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(навчально-науковий інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

Здобувача вищої освіти Копитько Вадима Івановича
(ПІБ)
академічної групи 123м-23-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою «Комп'ютерна інженерія»
(офіційна назва)

на тему «Програмно-технічна реалізація комп'ютерної системи обліку Дніпровської залізничної станції із застосуванням модуля ідентифікації контейнерів»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Кожевников А.В.			
розділів:				
синтез системи	доц. Бешта Д.О.			
розроблення програмного забезпечення	Панферова Я.В			
Рецензент	проф. Логвін В.М.			
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ В.В. Гнатушенко
(підпис) (ініціали, прізвище)
«_____» _____ 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра
(бакалавра, магістра)

здобувача вищої освіти Копитько В.І. **академічної групи** 123м-23-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

за освітньою-професійною програмою «Комп'ютерна інженерія»
(офіційна назва)

на тему «Обґрунтування структури та параметрів комп'ютерної системи меблевої фабрики «Прогрес» з функціями відеонагляду та пожежної сигналізації»,
затверджену наказом ректора НТУ «Дніпровська політехніка» від 17 жовтня 2024 р. №1388-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів практик, інших науково-технічних джерел сформулювати наукове завдання, конкретизувати предмет та мету досліджень	11.10.2024
Теоретичний	Розглянути сучасні підходи до побудови систем відеонагляду та пожежної сигналізації, провести аналіз існуючих технологій і їх застосування на промислових підприємствах.	25.10.2024
Синтез системи	Сформулювати основні вимоги до структури системи та запропоновано функціональну схему, що охоплює всі елементи, необхідні для інтеграції відеонагляду та пожежної сигналізації	15.11.2024
Розроблення програмного забезпечення	Розробка програмного забезпечення, яке реалізує автоматичний аналіз відеопотоку для виявлення загроз, зберігання даних, а також інтерактивний клієнтський інтерфейс для моніторингу та управління системою.	29.11.2024
Експериментальний розділ	Тестування розробленої системи на меблевій фабриці «Прогрес» для перевірки її працездатності в реальних умовах.	06.12.2024

Завдання видано _____ доц. Кожевніков А.В.
(підпис керівника) (ініціали, прізвище)

Дата видачі 06 вересня 2024 р.

Дата подання до екзаменаційної комісії 20.12.2024 р.

Прийнято до виконання _____ В.І.
(підпис здобувача вищої освіти) (ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка: 92 с., 29 рис., 24 джерел, 1 додаток.

ВІДЕОНАГЛЯД, ПОЖЕЖНА СИГНАЛІЗАЦІЯ, ВІДЕОАНАЛІЗ, СИСТЕМА СПОСТЕРЕЖЕННЯ, ОБРОБКА ВІДЕОПОТОКУ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, КЛІЄНТ-СЕРВЕРНА АРХІТЕКТУРА, ДАТЧИКИ ДИМУ

Об’єктом дослідження: комп'ютерна система для відеонагляду та пожежної сигналізації на меблевій фабриці «Прогрес».

Мета кваліфікаційної роботи: обґрунтування структури та параметрів системи, що забезпечує ефективне відеоспостереження та своєчасне виявлення пожежних загроз, адаптоване до специфіки роботи меблевої фабрики.

Наукова новизна: полягає в інтеграції сучасних технологій відеонагляду та пожежної сигналізації, адаптованих до умов меблевої фабрики. Проєкт впроваджує IoT-сенсори та клієнт-серверну архітектуру для автоматизації аналізу даних, знижуючи залежність від людського фактору. Забезпечується висока надійність, адаптивність, і відмовостійкість системи, яка пройшла успішне тестування в реальних умовах, підтвердивши свою ефективність і точність у виявленні загроз.

Практична цінність: полягає у розробці комп'ютерної системи для відеонагляду та пожежної сигналізації на меблевій фабриці «Прогрес», яка дозволить значно підвищити безпеку на підприємстві, зменшити ризики для персоналу та обладнання, забезпечити ефективний моніторинг і швидку реакцію на загрози. Це також дозволить автоматизувати процеси контролю за безпекою, знизити витрати на реагування в надзвичайних ситуаціях та відповідати сучасним вимогам безпеки.

ABSTRACT

Explanatory note: 92 pages, 29 figures., 24 sources, 1 appendices.

VIDEO SURVEILLANCE, FIRE ALARM, VIDEO ANALYSIS, SURVEILLANCE SYSTEM, VIDEO STREAM PROCESSING, SOFTWARE, CLIENT-SERVER ARCHITECTURE, SMOKE DETECTORS

Object of research: computer system of video surveillance and fire alarm at the furniture factory "Progress".

Meta qualification work: justification of the structure and parameters of systems that provide effective video surveillance and verification of fire threats, adapted to the specifics of the work of a furniture factory.

Scientific news: conflict in the integration of modern technologies of video surveillance and fire alarm, adapted to the conditions of a furniture factory. The project implements IoT sensors and client-server architecture to automate data analysis, reducing dependence on the human factor. High reliability, adaptability and fault tolerance of the system are ensured, which has been successfully tested in real conditions, confirming its effectiveness and accuracy in eliminating threats.

Practical value: will be carried out in the development of a computer system for video surveillance and fire alarm at the furniture factory "Progress", which will significantly increase safety at the enterprise, reduce risks to personnel and equipment, ensure effective monitoring and rapid response to threats. This will also allow automating security control processes, reducing emergency response costs and meeting modern security requirements.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DVR – Digital Video Recorder;

i-LIDS – Imagery Library for Intelligent Detection Systems;

NVR – Network Video Recorder;

CCTV –·Closed-Circuit Television;

IP – Internet Protocol;

LAN – Local Area Network;

BVMS – Bosch Video Management System;

IoT – Internet of Things;

БД – База Даних;

ПЗ – Програмне Забезпечення.

ЗМІСТ

Вступ……... 8
Розділ 1 Стан питання та постанова завдання…… 9
1.1Стан питання……. 9
1.2 Аналіз існуючих систем відеонагляду та пожежної сигналізації на підприємствах……. 10
1.2.1 Аналіз існуючих систем відеонагляду…… 10
1.2.2 Аналіз існуючих систем пожежної сигналізації…… 22
1.3 Проблеми існуючих систем відеонагляду та пожежної сигналізації на підприємствах…… 26
1.4 Постановка завдання дослідження……. 29
Розділ 2 Теоретична частина…… 31
2.1 Характеристика і структура об’єкта впровадження меблевої фабрики «Прогрес»…… 31
2.2 Стислі відомості про комп'ютерну систему меблевої фабрики «Прогрес» з функціями відеонагляду та пожежної сигналізації…….. 36
2.3 Аналіз підходів до моделювання комп'ютерної системи з функціями відеонагляду та пожежної сигналізації……. 38
2.3.1 Модель відеоданих…… 39
2.3.2 Сегментація відео…….. 41
2.3.3 Вилучення ознак…… 42
2.3.4 Аналіз підходів до моделювання пожежної сигналізації…….. 43
2.4 Загальна модель системи відеонагляду та пожежної сигналізації….. 45
2.4.1 Математичний опис роботи системи…….. 46
2.5 Висновки до розділу…… 49
Розділ 3 Синтез системи контролю мережевого трафіку……... 51
3.1 Розробка схеми функціональної структури……... 51
3.2 Вибір елементної апаратної бази системи……. 59
3.3 Розробка та налаштування обладнання та сервісів системи iot…….. 61
3.4 Висновки до розділу…… 66
Розділ 4 Розробка програмного забезпечення системи відеонагляду та пожежної сигналізації…… 67
4.1 Призначення й область застосування програмного забезпечення….. 67
4.2 Розробка інтерфейсу користувача…….. 68

4.2.1 Технічні аспекти реалізації інтерфейсу…….. 69
4.3 Розробка серверної частини…… 70
4.4 Опис логічної частини програми…… 71
4.5 Вхідні та вихідні дані……... 75
4.6 Висновки до розділу…… 76
Розділ 5 Експерементальна частина……. 78
5.1 Формування вимог до експерименту для розроблення алгоритму виявлення пожежі……... 78
5.2 Метрики для оцінки алгоритму експерименту…….. 79
5.3 Проведення експерименту за допомогою тестового набору відеоданих……... 80
5.4 Характеристика новизни результатів……. 83
5.5 Висновки до розділу…… 84
Висновки……. 86
Перелік посилань……... 88
Додаток а. Текст програми відеонагляду……. 91

ВСТУП

У сучасних умовах розвитку промислових підприємств безпека та автоматизація виробничих процесів стають пріоритетними завданнями для забезпечення стабільної та ефективної роботи. Меблеві фабрики, зокрема, піддаються підвищеним ризикам через використання легкозаймистих матеріалів, що робить питання пожежної безпеки особливо актуальним. Водночас, впровадження систем відеонагляду є необхідним для забезпечення безпеки на виробничих майданчиках, контролю за технологічними процесами та запобігання можливим інцидентам.

Меблева фабрика «Прогрес» прагне підвищити рівень безпеки та автоматизувати моніторинг виробничих процесів, інтегруючи сучасні технології у свою інфраструктуру. Одним з ефективних підходів до вирішення цієї задачі є впровадження комп’ютерної системи, що поєднує функції відеонагляду та пожежної сигналізації. Така система дозволяє своєчасно виявляти пожежні загрози, аналізувати відео в реальному часі та забезпечувати ефективне управління безпекою на підприємстві.

Актуальність дослідження обумовлена необхідністю розробки інтегрованої системи, що відповідає вимогам сучасного виробництва, забезпечує надійний захист від пожеж, автоматизує процеси моніторингу та є адаптивною до змін умов на виробничих майданчиках.

Метою цієї роботи є обґрунтування структури та параметрів системи, що забезпечує ефективне відеоспостереження та своєчасне виявлення пожежних загроз, адаптоване до специфіки роботи меблевої фабрики.

РОЗДІЛ 1
СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стан питання

У сучасному виробничому середовищі забезпечення безпеки та безперебійної роботи підприємств стає першочерговим завданням. Для меблевої фабрики «Прогрес», яка займається виготовленням складної продукції, питання моніторингу та своєчасного реагування на надзвичайні ситуації є критично важливими. Безпека на виробництві впливає не лише на захист персоналу, а й на збереження матеріальних активів та уникнення збитків, що можуть виникати внаслідок пожеж або інших аварійних ситуацій.

Сучасні комп'ютерні системи з функціями відеонагляду та пожежної сигналізації відіграють ключову роль у зменшенні ризиків. Системи відеонагляду забезпечують постійний моніторинг виробничих приміщень, дають змогу фіксувати потенційно небезпечні ситуації, аналізувати поведінку персоналу та контролювати дотримання правил безпеки. Це дозволяє виявляти можливі загрози на ранніх етапах та оперативно реагувати, запобігаючи розвиткові інцидентів. Функції пожежної сигналізації, своєю чергою, спрямовані на своєчасне виявлення ознак загоряння, таких як дим, підвищення температури або полум'я. Ці системи автоматично сповіщають відповідні служби та активують заходи пожежогасіння, що значно знижує ризик поширення вогню та мінімізує збитки. Проте інтеграція відеонагляду та пожежної сигналізації на рівні підприємства вимагає ретельного проектування структури, вибору відповідних параметрів та урахування специфічних умов роботи меблевої фабрики. Проте інтеграція цих систем на рівні підприємства вимагає ретельного проектування структури, вибору відповідних параметрів, а також урахування специфічних умов роботи меблевої фабрики. Багато існуючих систем мають обмежені можливості у плані адаптації до різних виробничих умов, інтеграції

різних компонентів і забезпечення достатньої швидкості реагування на критичні події.

Іншою проблемою є високі вимоги до сумісності програмного забезпечення та апаратних засобів. Застарілі системи або неповна інтеграція можуть призвести до втрати даних або затримок у виявленні та реакції на загрози. Крім того, значення має забезпечення централізованого контролю та управління системою, що дозволяє оперативно отримувати інформацію та приймати рішення [1].

Існуючі рішення часто мають обмеження щодо адаптації до різних виробничих умов, а також проблеми з інтеграцією різних компонентів, що впливає на швидкість та ефективність реагування на події. Застарілі системи або неповна інтеграція призводять до втрати даних чи затримок у роботі, що може бути критичним під час надзвичайних ситуацій. Крім того, важливим аспектом є забезпечення централізованого контролю та управління, що дозволяє оперативно отримувати інформацію та приймати обґрунтовані рішення.

Отже, актуальність проблеми обумовлюється необхідністю створення сучасної, надійної та функціональної комп'ютерної системи для меблевої фабрики «Прогрес», яка буде поєднувати функції відеонагляду та пожежної сигналізації, а також відповідатиме специфічним вимогам виробничого середовища.

1.2 Аналіз існуючих систем відеонагляду та пожежної сигналізації на підприємствах

1.2.1 Аналіз існуючих систем відеонагляду

Сучасні системи відеоспостереження можна класифікувати за різними критеріями, такими як середовище використання (внутрішні чи зовнішні системи), кількість камер (одно- чи багатоканальні системи) та типи камер (рухомі чи стаціонарні). На сьогоднішній день більшість систем мають спільну рису — вони забезпечують постійне спостереження за допомогою оператора.

Однак така залежність від людського фактору є значним недоліком, оскільки ефективність роботи системи залежить від кількості операторів та їхньої пильності.

Дослідження Національного інституту юстиції США показало, що увага операторів значно знижується після 20 хвилин безперервного спостереження за моніторами. Це призводить до потенційних прогалин у безпеці, оскільки оператори можуть не помітити важливі події. Для зменшення цього ризику було впроваджено практику запису відео для подальшого використання у криміналістичних цілях. Проте цей підхід також має свої недоліки, що добре ілюструють приклади з практики.

Зокрема, після терористичних атак у Лондоні 7 липня 2005 року, ідентифікація підозрюваних вимагала понад 6000 людино-годин на перегляд записів. Подібна ситуація склалася у США під час розслідування спроби вибуху на Таймс-сквер у травні 2010 року, коли правоохоронні органи також були змушені витрачати значний час на перегляд відеозаписів.

Щоб подолати ці проблеми та зменшити залежність від людини, зростає попит на автоматизовані системи спостереження. Відповіддю на цю потребу стала ініціатива Міністерства внутрішніх справ Великобританії у 2007 році, коли було створено еталонний набір даних Imagery Library for Intelligent Detection Systems (i-LIDS) [2]. Ця база даних стала основою для розробки та тестування сучасних алгоритмів комп’ютерного зору, які дозволяють автоматизувати аналіз відео та допомагають правоохоронцям ефективніше реагувати на подібні ситуації в майбутньому.

Зараз автоматизовані системи відеоспостереження активно використовуються у багатьох країнах. Наприклад, системи з підтримкою штучного інтелекту від таких компаній, як Hikvision та Axis Communications, здатні розпізнавати обличчя, ідентифікувати об'єкти та виявляти підозрілу активність у режимі реального часу. Це значно підвищує продуктивність систем безпеки та дозволяє скоротити час реагування на потенційні загрози, звільняючи

операторів від перегляду тривалих записів і зосереджуючи їхню увагу на критичних моментах.

Існують цифрові і аналогові камери. Аналогові системи відеоспостереження (рис.1.1) використовують камери, які захоплюють аналоговий відеосигнал. Цей сигнал передається через коаксіальний кабель на цифровий відеореєстратор (DVR), де він перетворюється у цифровий формат, стискається та записується на жорсткий диск. DVR також забезпечує можливість перегляду відзнятого матеріалу на підключених моніторах або передає сигнал через мережу для перегляду на комп'ютерах. Ця технологія дозволяє передавати відео в Інтернеті за допомогою єдиної IP-адреси, що забезпечує високу ефективність передачі даних [3].

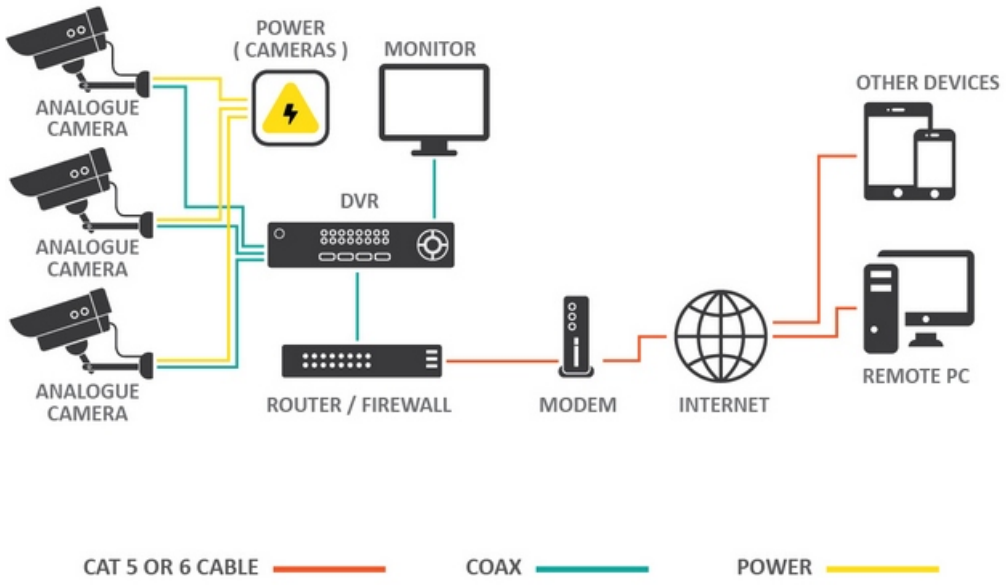

Рисунок 1.1 – Архітектура аналогових систем відеоспостереження

Однією з переваг аналогових камер є простота використання та відносна дешевизна. Проте вони мають обмежену роздільну здатність, що обмежує деталізацію зображення. З цієї причини аналогові камери зазвичай використовуються в середовищах, де не потрібна висока якість зображення.

Цифрові IP-камери (рис.1.2) відрізняються тим, що захоплюють аналоговий сигнал, який одразу перетворюється у цифровий сигнал

безпосередньо в камері. Завдяки цифровій обробці, сигнал передається через Ethernet-кабелі (наприклад, Cat5e) через локальну мережу (LAN). Для таких систем використовується мережевий відеореєстратор (NVR), який стискає та записує відео з камер [4].

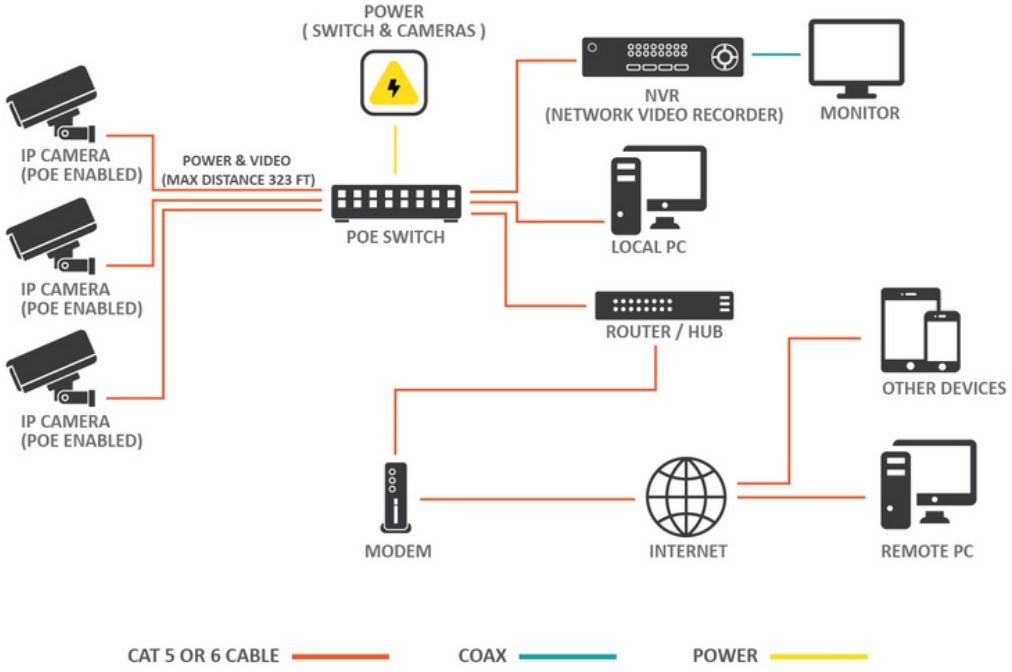

Рисунок 1.2 – Архітектура цифрових систем відеоспостереження

IP-камери мають ключову перевагу у вигляді високої роздільної здатності, яка забезпечує значно кращу деталізацію зображення порівняно з аналоговими системами. Крім того, вони надають можливість віддаленого доступу до відео в реальному часі через Інтернет, що спрощує моніторинг з різних пристроїв.

1.2.1.1 Камери CCTV

Аналогові камери CCTV обладнані датчиком, що захоплює відеозображення з максимальною роздільною здатністю до 720×575 пікселів (720 пікселів горизонтально і 575 пікселів вертикально). Передача відеосигналу від камери до цифрового відеореєстратора (DVR) і монітора здійснюється через

коаксіальний кабель. Сигнал відповідає стандартам NTSC або PAL, що забезпечує сумісність із телевізорами [5].

У сучасних системах аналогові камери (рис.1.3) передають відео через коаксіальний або UTP-кабель на DVR, де сигнал перетворюється в цифровий формат і зберігається на жорсткому диску. Сучасні DVR здебільшого є мережевими пристроями, що дозволяє віддалений доступ до відеозаписів через локальну мережу або Інтернет. Записи зберігаються за принципом FIFO (першим прийшов, першим вийшов), що забезпечує актуальність архіву відео за останні кілька днів. Таким чином, аналогові камери, хоч і передають сигнал у аналоговому форматі, дозволяють отримати доступ до записів через мережу. Вони підходять для невеликих систем спостереження, як-от офіси чи житлові приміщення [5].

Рисунок 1.3 – Архітектура мережі аналогової камери CCTV

IP-камери використовують такий самий датчик зображення, як і аналогові камери, але після захоплення зображення чи відео передають його у вигляді цифрових даних через мережеве з'єднання. Відео стискається і надсилається у форматі стиснених кадрів за допомогою мережевого протоколу, звідки й

походить їхня назва — «IP» (Інтернет-протокол). IP-камери передають цифровий потік через IP-мережу, що дозволяє більшу гнучкість у виборі способу та місця збереження відео.

Записи з IP-камер зберігаються на мережевих відеореєстраторах (NVR), які часто можуть бути просто програмним забезпеченням, оскільки немає необхідності конвертувати аналоговий сигнал. Відео можна зберігати на мережевих дисках RAID відповідно до налаштувань NVR.

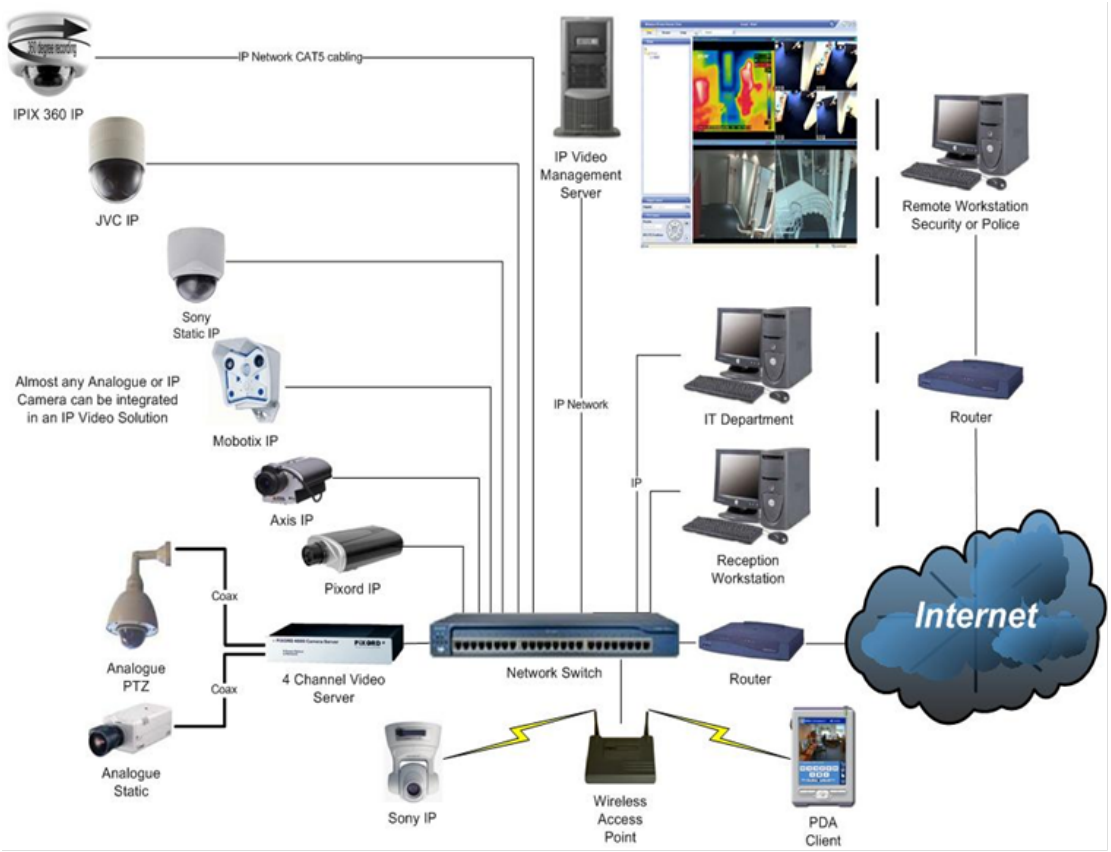

Рисунок 1.4 – Архітектура мережі ip-камери CCTV [5].

Однією з головних переваг IP-камер є їхня висока роздільна здатність. У той час як аналогові камери досягають приблизно 700/620 ТВЛ (приблизно 0,6 мегапікселя), IP-камери можуть мати роздільну здатність понад 5 мегапікселів. Це дає можливість користувачам збільшувати зображення та зберігати чіткість. IP-камери також мають кращу сумісність із бездротовими мережами. Хоча

бездротові аналогові системи також існують, вони або потребують перетворення сигналу на IP і передачі через мережу 802.11, що збільшує витрати, або зазнають перешкод на частотах, що регулюються.

Хоч IP-камери зазвичай дорожчі, вони пропонують значно вищу роздільну здатність та можливість цифрового збільшення, що покращує можливість ідентифікації об’єктів.

1.2.1.2 IP-відеосистеми MOBOTIX

IP-відеосистеми MOBOTIX оптимізовані для віддаленого використання та хмарних технологій (рис.1.5), що дозволяє ефективно зменшити пропускну здатність відеоканалу за рахунок масштабування розміру та частоти кадрів. Першим інноваційним продуктом компанії стала IP-камера з вбудованою технологією запису та керування відеореєстратором, яка змінила підхід до відеоспостереження завдяки децентралізованій архітектурі. Такий підхід знижує залежність від центральних серверів, що зменшує витрати на інфраструктуру та підвищує надійність системи. Камери MOBOTIX використовують мало обчислювальних ресурсів навіть при високій роздільній здатності, що робить їх економічно вигідними та легкими у масштабуванні [6].

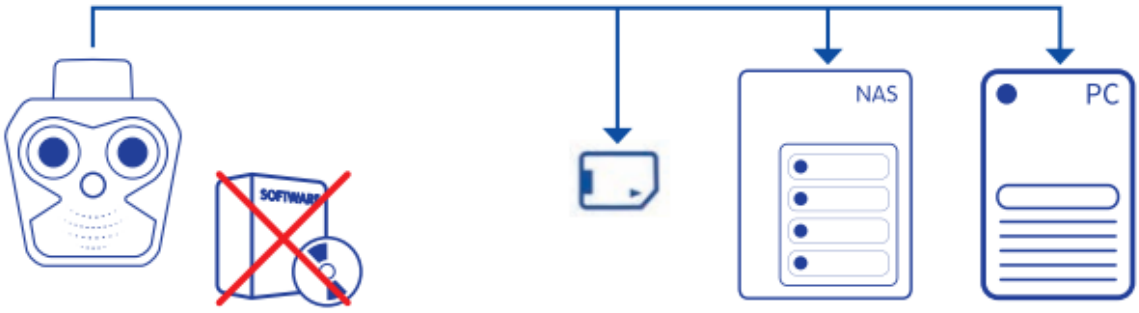

Рисунок 1.5 – Структурна схема «децентралізації» MOBOTIX камери [6].

Особливістю відеокамер MOBOTIX є підтримка збереження відео за подіями, що дозволяє інтегрувати їх у мережеві системи без зайвого

навантаження на сервери. Високий рівень безпеки забезпечується завдяки шифруванню відео безпосередньо в камері, що унеможливлює несанкціонований доступ до даних. Завдяки використанню високоякісних CMOS-сенсорів, навіть при низькій освітленості камери забезпечують деталізовані та чіткі зображення. Камери MOBOTIX підтримують регулярне оновлення програмного забезпечення, що гарантує високу продуктивність і нові функціональні можливості, такі як 3D-аналіз руху.

Одним із провідних рішень є модель M16, яка має модульний дизайн і підтримує змінні сенсори для денного, нічного та термального режимів. Камера оснащена сучасними технологіями безпеки, включаючи вбудовані засоби кіберзахисту, та відповідає стандарту IP66, що забезпечує захист від пилу і вологи. Використання власного відеокодека MxPEG+ і підтримка стандарту H.264 роблять M16 універсальною для інтеграції в різні системи безпеки.

1.2.1.3 MxActivity Sensor

MxActivitySensor — інноваційна технологія від MOBOTIX, що дозволяє фіксувати рух тільки людей і об'єктів, ігноруючи несуттєві зміни в кадрі, як-от дощ, сніг, рух хмар, дерев чи кущів під час вітру. Ця технологія зменшує кількість помилкових спрацьовувань на 90 % у порівнянні зі звичайними системами виявлення руху (VMD). Завдяки цьому MOBOTIX вивела відеодетекцію руху на новий рівень. MxActivitySensor перевершує традиційне виявлення руху, точно фіксуючи людей та транспортні засоби. Вона надає високоякісну та ефективну систему, яка значно покращує продуктивність відеоспостереження навіть у складних умовах. Система також забезпечує погодну компенсацію, що дозволяє зберігати точність роботи навіть при несприятливих погодних умовах, без необхідності додаткових налаштувань. Автоматичне налаштування підвищує зручність використання, а також знижує витрати на систему (рис.1.6) [6].

Камери MOBOTIX, оснащені MxAnalytics, ідеально підходять для моніторингу магазинів та інших комерційних об’єктів. Цей вбудований аналітичний інструмент дозволяє створювати теплові карти для візуалізації активності та вести підрахунок об'єктів у визначених користувачем зонах із автоматичною генерацією звітів. MxAnalytics також аналізує поведінку рухомих об'єктів і може генерувати автоматичні сповіщення у випадках, коли об'єкт зупиняється, змінює напрямок чи повертається. Весь аналіз виконується безпосередньо на борту камери, що знижує навантаження на мережу і виключає потребу у додаткових робочих станціях. Це збільшує стабільність роботи і знижує загальні витрати на обслуговування системи. Ці переваги роблять технології MOBOTIX одними з найкращих рішень для точного, надійного і економічного відеоспостереження.

Рисунок 1.6 – Відеоспостереження під час туману [6].

Інші виробники, такі як Bosch і Hikvision, також пропонують високотехнологічні рішення для відеоспостереження з функціями інтелектуального аналізу відео, що включають розпізнавання облич, детекцію руху та підрахунок відвідувачів. Їхні системи підтримують хмарне збереження даних та інтеграцію з іншими пристроями системи безпеки.

1.2.1.3 Відеосистема Bosch

Відеосистеми Bosch використовують камери з високою роздільною здатністю, що дозволяють отримувати чітке та детальне зображення, навіть у складних умовах освітлення. Камери підтримують роздільну здатність від 1080p до 4K для забезпечення високої якості відео.

Вбудовані технології аналізу відео дозволяють автоматично виявляти певні події, як-от вторгнення, рух в заборонених зонах, покинутий багаж чи підозрілі поведінки. Це забезпечує більшу ефективність у моніторингу та зменшує кількість помилкових тривог.

Камери Bosch використовують технології, що забезпечують чіткість відео навіть за умов низького освітлення, завдяки функціям WDR (Wide Dynamic Range) та Noise Reduction. Це дозволяє отримувати якісне зображення в умовах висококонтрастного освітлення та за низької освітленості.

Відеосистеми Bosch оптимізують використання смуги пропускання через технології стиснення відео, зокрема H.265 та H.264, що дозволяє зменшити витрати на зберігання даних без втрати якості зображення.

Bosch пропонує зручні рішення для інтеграції з іншими системами безпеки, такими як системи контролю доступу або сигналізації. Також забезпечується віддалений доступ до відео через програмне забезпечення Bosch Video Management System (BVMS) для моніторингу та управління в режимі реального часу.

Системи Bosch можуть використовувати хмарні рішення для зберігання відеоархівів, що забезпечує більшу гнучкість в управлінні даними та доступ до них з будь-якої точки світу [7].

1.2.1.4 Відеосистема Hikvision

Камери Hikvision підтримують роздільну здатність від 1080p до 4K та оснащені технологією Darkfighter, що дозволяє отримувати високоякісне відео навіть при низькому освітленні, а також підтримують функції WDR для досягнення високої чіткості зображення в умовах контрастного освітлення.

Hikvision оснащені потужними алгоритмами для відеоаналітики, включаючи виявлення руху, розпізнавання облич, ідентифікацію номерних знаків, виявлення порушень і тривог. Це дозволяє ефективно фільтрувати важливі події та зменшити кількість помилкових тривог.

Камери Hikvision використовують стиснення H.265+ для зниження вимог до смуги пропускання та зберігання, що дозволяє зберігати більше відео без втрати якості та знижує вимоги до мережевої інфраструктури.

Hikvision впровадила технології, такі як ColorVu, які дозволяють камерам працювати з високою чіткістю в умовах дуже низького освітлення (до 100 лк), що є важливим для цілодобового моніторингу.

Hikvision надає платформу iVMS-4200, а також мобільні додатки для віддаленого доступу, що дозволяє користувачам керувати системою, переглядати відео в реальному часі та отримувати сповіщення про тривоги через Інтернет чи мобільні пристрої.

Відеосистеми Hikvision підтримують хмарні рішення для зберігання відеоархівів, що надає користувачам зручний доступ до записів через Інтернет і дозволяє зберігати дані в захищених дата-центрах.

Hikvision також забезпечує інтеграцію з іншими елементами системи безпеки, такими як контроль доступу, охоронні датчики та системи оповіщення. Це дозволяє створювати комплексні рішення для безпеки на підприємствах і в приватних об'єктах [8].

1.2.1.5 Відеоаналітика

Відеоаналітика — це програмне забезпечення, призначене для автоматичного аналізу відеопотоків та виявлення подій за допомогою порівняння пікселів із заданими шаблонами для отримання відповідної реакції. Це дозволяє системам відеоспостереження швидко і точно виявляти конкретні об'єкти або поведінку, такі як людина, яка входить у захищену зону, або незаконно припаркований автомобіль. Відеоаналітика перетворює відеозапис на корисні дані, які можна архівувати для аналізу або використовувати для прийняття оперативних рішень, таких як автоматичне блокування дверей чи активація сигналізації. Це зменшує потребу в безперервному моніторингу людиною, підвищуючи ефективність системи.

Значний попит на програмні рішення відеоаналітики обумовлений декількома ключовими факторами:

– покращені обчислювальні ресурси. Сучасні обчислювальні технології зробили можливим впровадження складних алгоритмів відеоаналітики, які працюють безпосередньо на камерах або в мережевих вузлах. Завдяки компаніям, таким як Texas Instruments та NVIDIA, з'явилися камери з потужною обробкою даних "на краю мережі". Це дозволяє обробляти відео в реальному часі навіть у мережах з обмеженою пропускною здатністю;

– камери високої чіткості. Високоякісне відео є критично важливим для успішного впровадження алгоритмів відеоаналітики. Поява камер високої роздільної здатності, таких як 4K та 8K, дала можливість створювати більш точні та надійні системи спостереження, здатні працювати в складних умовах;

– загрози тероризму та безпека громадських місць. Після терактів 11 вересня 2001 року значно зріс інтерес до безпеки в громадських місцях. Уряди багатьох країн вклали значні ресурси у встановлення систем відеоспостереження в аеропортах, на вокзалах та у великих торгових центрах. Це стимулювало розвиток систем відеоаналітики, які можуть допомогти правоохоронцям швидко реагувати на потенційні загрози;

– інфраструктура IP-мереж. Розвиток IP-мереж також сприяв поширенню інтелектуальних систем відеоаналітики. Завдяки високій швидкості

передачі даних та легкій масштабованості IP-мереж, інтерес до таких систем значно зріс. За даними досліджень, кількість IP-систем відеоспостереження перевищила 45% ще до 2012 року, що сприяло розвитку і впровадженню відеоаналітичних технологій.

Сучасні системи відеоаналітики, такі як Deep Sentinel або програмні рішення від Axis Communications, здатні виконувати різні завдання, від розпізнавання облич до виявлення підозрілих рухів у реальному часі. Це значно підвищує ефективність безпеки та допомагає скоротити час реагування на інциденти, дозволяючи операторам зосередитися на важливих ситуаціях [10].

1.2.2 Аналіз існуючих систем пожежної сигналізації

Системи пожежної сигналізації є критично важливим елементом у забезпеченні безпеки будівель і споруд. Вони здатні швидко виявити наявність пожежі та сповістити про це відповідальні органи для швидкого реагування. Одним з важливих аспектів таких систем є панелі керування, які дозволяють централізовано моніторити стан сигналізації та здійснювати контроль за її роботою [8].

1.2.2.1 Compact панелі керування

Панель керування Compact є одноконтурною інтелектуальною адресною панеллю для пожежної сигналізації, яка ідеально підходить для невеликих і середніх приміщень з підвищеними вимогами до надійності та безпеки. Система оснащена шиною esserbus-PLus, що є стійкою до короткого замикання і обриву, і може підтримувати до 127 пристроїв на кожному контурі (рис.1.7).

Основні технічні характеристики [11]:

– напруга: 230 В змінного струму, частота 50...60 Гц, струм 0,08 А;
– акумулятор: Максимальна ємність - 2 x 12 В / 12 Ач;

– температурний діапазон: робоча температура - від -5 °C до 45 °C, температура зберігання від -5 °C до 50 °C;

– тип захисту: IP30;

– корпус: Виготовлений з армованого ABS, стійкий до механічних пошкоджень;

– габарити: 450 мм (Ш) х 320 мм (В) х 185 мм (Г), вага без батарей 5 кг.

Основні функції:

– адресна система: підтримка до 127 інтелектуальних шинних пристроїв, таких як детектори диму, теплові датчики та ручні сповіщувачі;

– інтерфейси та комунікації: наявність вбудованих інтерфейсів для підключення до системи управління пожежною безпекою, таких як RS485 для підключення периферійних пристроїв і пожежних графічних сповіщувачів;

– реле та виходи: панель забезпечує до 4 програмованих реле і 2 виходи для підключення акустичних та оптичних генераторів сигналів, що відповідають вимогам EN 54-13;

– інтеграція з іншими системами: можливість підключення до систем управління вогнем, пожежних графічних сповіщувачів і генераторів сигналів.

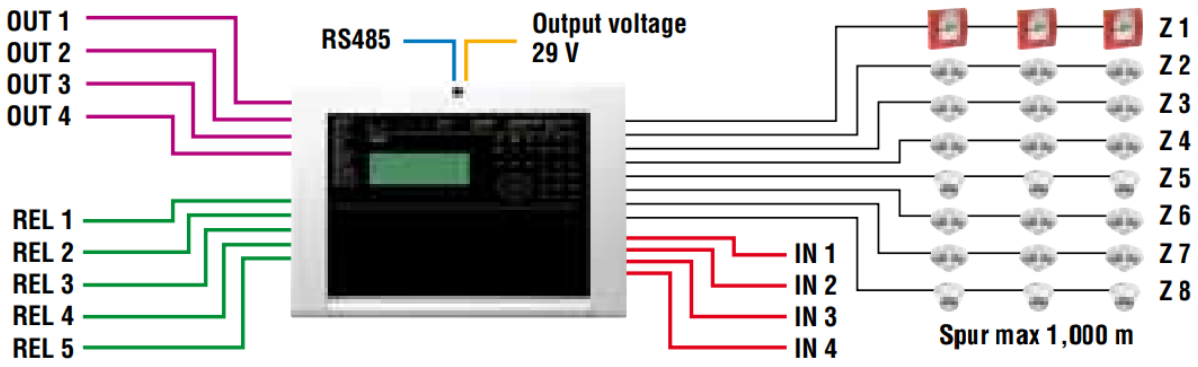

Рисунок 1.7 – Схема підключення виходів, реле, входів, та зон детекторів до пожежної сигналізації з підключенням по шині RS485

Переваги використання Compact:

– система має резервування за допомогою кільцевого підключення, що забезпечує безперебійну роботу навіть при обриві проводки;

– підтримує широкий спектр периферійних пристроїв і може бути використана для різних типів приміщень, таких як школи, дитячі садки, лікарні, магазини, малі підприємства і т.д.;

– система легко налаштовується і конфігурується за допомогою програмного забезпечення 8000, що дозволяє швидко здійснити введення в експлуатацію та обслуговування.;

– завдяки цьому система може охопити великі об'єкти, що потребують пожежної безпеки.

Панель керування Compact є оптимальним вибором для невеликих і середніх приміщень, де необхідно забезпечити високу надійність і швидку реакцію на сигнали про пожежу. Це ідеальний варіант для установ, де потрібна інтеграція різних елементів системи сигналізації та можливість їх централізованого моніторингу і управління.

1.2.2.2 IQ8Control Panels IQ8Control C панелі керування

Панель управління IQ8Control C — це інтелектуальна адресна панель, призначена для використання в системах пожежної безпеки. Вона забезпечує надійне управління пожежними сигналами та є частиною мережі з кількома пристроями, що працюють по шині essernet.

Технічні параметри панелі IQ8Control C [12]:

– номінальна напруга: 230 В змінного струму;

– номінальна частота: 50...60 Гц;

– номінальний струм: 0,35 А;

– при підключенні шлейфу з живленням: 0,7 А;

– струм споживання на зовнішні пристрої: 2 А;

– ємність акумулятора: 2 x 12 Ah або 2 x 24 Ah в корпусі розширення;

– температурний діапазон:робоча температура: від -5 °C до 45 °C; температура зберігання: від -5 °C до 50 °C;

– вологість повітря: до 95% (без конденсації);

– тип захисту: IP30;

– матеріал корпусу: ABS, армований скловолокном (10%), вогнестійкість V-0;

– колір корпусу: сірий, схожий на Pantone 538;

– вага: близько 6,5 кг;

– розміри корпусу: Ш: 450 мм, В: 320 мм, Г: 185 мм.

Панель IQ8Control C може бути інтегрована з іншими пристроями (рис.1.8) за допомогою різних інтерфейсів. Вона підтримує підключення до мережі через essernet та дозволяє управляти до 254 адресами цифрових шлейфів. Панель також сумісна з системами пожежного сповіщення FACP 8000, що дозволяє інтегрувати її у більш складні мережі управління безпекою.

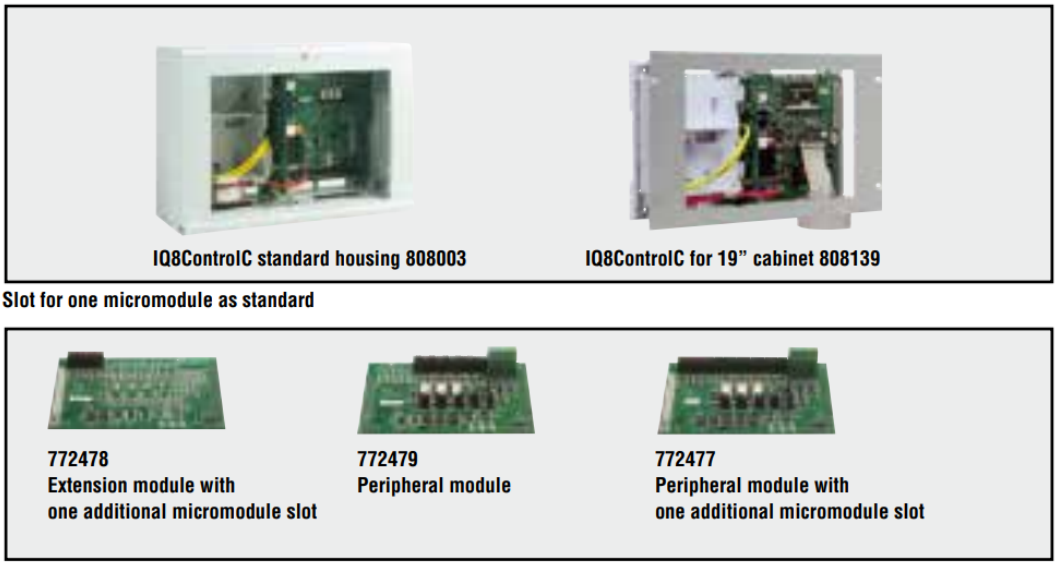

Рисунок 1.8 – Зовнішній вид панелі IQ8Control C

Особливості підключення:

– максимальна довжина петлі: до 1 км (до 3 км за допомогою ретранслятора);

– підключення до 127 пристроїв (пожежні сповіщувачі, ручні сповіщувачі) на одну петлю;

– інтерфейси: підтримка TTY, RS485, RS232, а також підключення до графічного супервізора FlexES Guard через послідовний інтерфейс.

Додаткові можливості:

– підтримка до двох мікромодулів, що дозволяє розширити систему;

– підключення зовнішніх сигналізаційних пристроїв та управління ними за допомогою синхронізованого живлення;

– пам'ять на 10 000 подій для зберігання історії сигналів;

– панель має великий LCD-дисплей (8 рядків по 40 символів), що дозволяє зручно переглядати події.

Ця панель є частиною модульної системи, яка дозволяє легко адаптувати систему пожежної безпеки до вимог конкретного об'єкта. Вона забезпечує надійне та ефективне управління сигналізацією і дозволяє інтегрувати різні типи пристроїв для покращення безпеки [12].

1.3 Проблеми існуючих систем відеонагляду та пожежної сигналізації на підприємствах

Системи відеонагляду та пожежної сигналізації є невід'ємною частиною безпеки на підприємствах. Вони забезпечують оперативне виявлення небезпечних ситуацій, зменшують ризики та сприяють збереженню майна. Однак існуючі технології відеонагляду та пожежної сигналізації стикаються з кількома важливими проблемами, які можуть впливати на їх ефективність і надійність.

Одна з головних проблем – це відсутність ефективної інтеграції між різними системами безпеки, такими як відеонагляд і пожежна сигналізація. Багато підприємств використовують окремі, не з'єднані між собою системи, що ускладнює координацію та реагування на надзвичайні ситуації. Це може

призвести до затримок в реакції на аварійні ситуації або до втрати частини інформації, необхідної для правильного прийняття рішень.

Хоча сучасні системи відеонагляду надають високу якість зображення та функції запису, вони можуть бути неефективними в певних умовах:

– відеокамери можуть мати труднощі з якісним зображенням у темряві або в умовах змінного освітлення (наприклад, у великих промислових приміщеннях, де освітлення не завжди є постійним);

– камери можуть не охоплювати всю необхідну територію або мати мертві зони, де вони не фіксують рух або події;

– відеоаналітика, що використовується в деяких системах, може давати помилкові спрацьовування, наприклад, через зміну освітлення або рух сторонніх об'єктів, що не є загрозою.

Деякі існуючі системи пожежної сигналізації можуть бути застарілими і не відповідати сучасним вимогам або стандартам:

– старі системи можуть не забезпечувати необхідну точність і швидкість виявлення пожежі, що може призвести до запізнілої реакції і збільшення шкоди;

– технології пожежних датчиків можуть не відрізняти справжню пожежу від інших природних явищ, таких як дим від куріння або пари, що знижує ефективність сигналізації;

– у великих або складних об'єктах пожежні системи можуть мати затримки в передачі сигналів до диспетчерських пунктів або інших підрозділів, що призводить до уповільнення процесу реагування.

Інтеграція та обслуговування сучасних систем відеонагляду та пожежної сигналізації можуть бути досить складними і дорогими:

– для забезпечення належної роботи таких систем необхідне регулярне обслуговування, калібрування сенсорів, а також оновлення програмного забезпечення, що вимагає додаткових ресурсів;

– для великих підприємств з широкими площами покриття витрати на установку та підтримку таких систем можуть бути значними. Крім того, деякі системи потребують спеціалізованих знань для їх налаштування і обслуговування.

Існуючі системи можуть бути вразливими до різноманітних зовнішніх факторів:

– відеонаглядні камери можуть бути пошкоджені або виведені з ладу через механічні впливи або погіршення умов навколишнього середовища (наприклад, у випадку сильних злив або пилу на виробництві);

– пожежні системи можуть не працювати в разі перебоїв з електропостачанням, якщо не передбачена належна резервна енергетична система або акумулятори.

Системи відеонагляду також стикаються з питаннями безпеки і конфіденційності даних:

– відеодані можуть бути вразливими до несанкціонованого доступу, що становить загрозу для конфіденційності персоналу або бізнесу;

– збереження великих обсягів відеоданих і обробка їх в режимі реального часу вимагають значних потужностей з боку серверів та програмного забезпечення, що може призвести до проблем з обробкою або зберіганням даних.

Всі вищеописані проблеми вказують на необхідність удосконалення існуючих систем відеонагляду та пожежної сигналізації, впровадження новітніх технологій для забезпечення більшої надійності, швидкості реагування та інтеграції. Оновлені системи повинні бути більш стійкими до зовнішніх впливів, мати можливість легко інтегруватися з іншими елементами безпеки і забезпечувати високий рівень захисту даних та конфіденційності.

1.4 Постановка завдання дослідження

Метою даного дослідження є обґрунтування структури та параметрів комп'ютерної системи для меблевої фабрики «Прогрес» з функціями

відеонагляду та пожежної сигналізації, з урахуванням специфіки роботи підприємства та потреби в забезпеченні високого рівня безпеки. Основним завданням є розробка комплексної системи, яка поєднує відеоспостереження та автоматичну пожежну сигналізацію для ефективного моніторингу території фабрики в реальному часі. Система повинна забезпечити надійний захист від пожеж, а також дозволити здійснювати контроль за виробничими процесами та відслідковувати всі події, що відбуваються на території підприємства.

Задачі, які необхідно вирішити:

– провести аналіз сучасних систем відеонагляду та пожежної сигналізації: необхідно вивчити переваги та недоліки існуючих рішень на ринку для того, щоб обрати оптимальні компоненти для побудови системи;

– на основі аналізу існуючих рішень та потреб підприємства, потрібно визначити, чи доцільно використовувати готові рішення або розробляти індивідуальну систему, що буде максимально ефективною для конкретних умов роботи меблевої фабрики;

– визначити, як повинна функціонувати система відеоспостереження та пожежної сигналізації. Це включає в себе планування архітектури системи, інтеграцію з іншими підсистемами фабрики, а також обрання відповідних технічних параметрів (типи камер, датчиків, серверів);

– розробити схему, що включає підключення всіх компонентів системи до корпоративної мережі фабрики. Це включає відеокамери для спостереження за територією, датчики пожежної сигналізації, сервери для зберігання даних і аналізу інформації, а також користувацькі пристрої для моніторингу;

– розробити програмний інструмент, що буде працювати за клієнт-серверною архітектурою, де сервер буде відповідати за зберігання відеоархівів і обробку сигналів від датчиків пожежної сигналізації, а клієнт — за надання доступу до реального часу та архівних записів;

– клієнтський додаток повинен забезпечити користувачам можливість перегляду відео з камер спостереження в реальному часі, а також переглядати

відеоархіви та отримувати сповіщення про події, пов'язані з пожежною безпекою;

– Реалізувати функцію відстеження потенційних загроз пожежі за допомогою датчиків диму, температури та інфрачервоних сенсорів, що дозволяє системі виявляти пожежу на ранній стадії.

РОЗДІЛ 2
ТЕОРЕТИЧНА ЧАСТИНА

2.1 Характеристика і структура об’єкта впровадження меблевої фабрики «Прогрес»

Меблева фабрика «Прогрес» є сучасним підприємством, яке спеціалізується на виробництві різноманітної меблевої продукції, зокрема м’якої, корпусної мебелі, а також продукції зі шкіри. Фабрика організована за принципом функціональної структури, де кожен підрозділ має чітко визначені завдання, а всі разом вони формують єдину систему для виконання виробничих і комерційних функцій. Підприємство забезпечує високоякісне виробництво та широкий спектр послуг, що включає не тільки виготовлення меблів, але й їх постачання і реалізацію.

Структура фабрики «Прогрес» представлена на рис.2.1. На вершині ієрархії знаходиться Генеральний директор, який здійснює загальне керівництво підприємством, розподіляє ресурси та відповідає за стратегічне управління. Під генеральним директором функціонують кілька основних підрозділів:

Виробничий підрозділ, який займається безпосереднім виготовленням меблів. До нього входять [13]:

– цехи м’якої мебелі, що виробляють різноманітні види м’якої мебелі;

– цех шкіряної мебелі (Voyage) та Цех корпусної мебелі, які спеціалізуються на виготовленні меблів зі шкіри та корпусних конструкцій;

– відділ технології, ТК та планування, який відповідає за технологічний процес і планування виробництва;

– відділ постачання, що забезпечує постачання матеріалів і комплектуючих;

– склади матеріалів і склад готової продукції, що займаються зберіганням матеріалів та готових виробів.

Служба продажів, яка охоплює кілька підрозділів для забезпечення збуту продукції:

– оптові та роздрібні продажі, а також Продажі через дистриб'юторів, що займаються реалізацією продукції різними каналами;

– магазини при фабриці, які продають меблі кінцевим споживачам;

Фінансова служба, що відповідає за управління фінансами підприємства, включає:

– фінансовий відділ, що займається фінансовим контролем і плануванням;

– бухгалтерію, яка здійснює облік фінансових операцій;

– ревізійний відділ, що контролює фінансову діяльність і проводить аудит;

Інші служби, які забезпечують підтримку основних функцій фабрики:

– відділ кадрів, що займається управлінням персоналом;

– IT-відділ, який забезпечує технічну підтримку та автоматизацію бізнес-процесів;

– секретаріат та Диспетчерський відділ, які виконують адміністративні функції.

На рис.2.2 зображено виробничий комплекс, на якому розташовані різноманітні підрозділи, що забезпечують повний цикл виготовлення меблів, зберігання матеріалів і готової продукції, адміністративну підтримку та обслуговування персоналу. Пояснимо основні елементи та умовні позначення на плані:

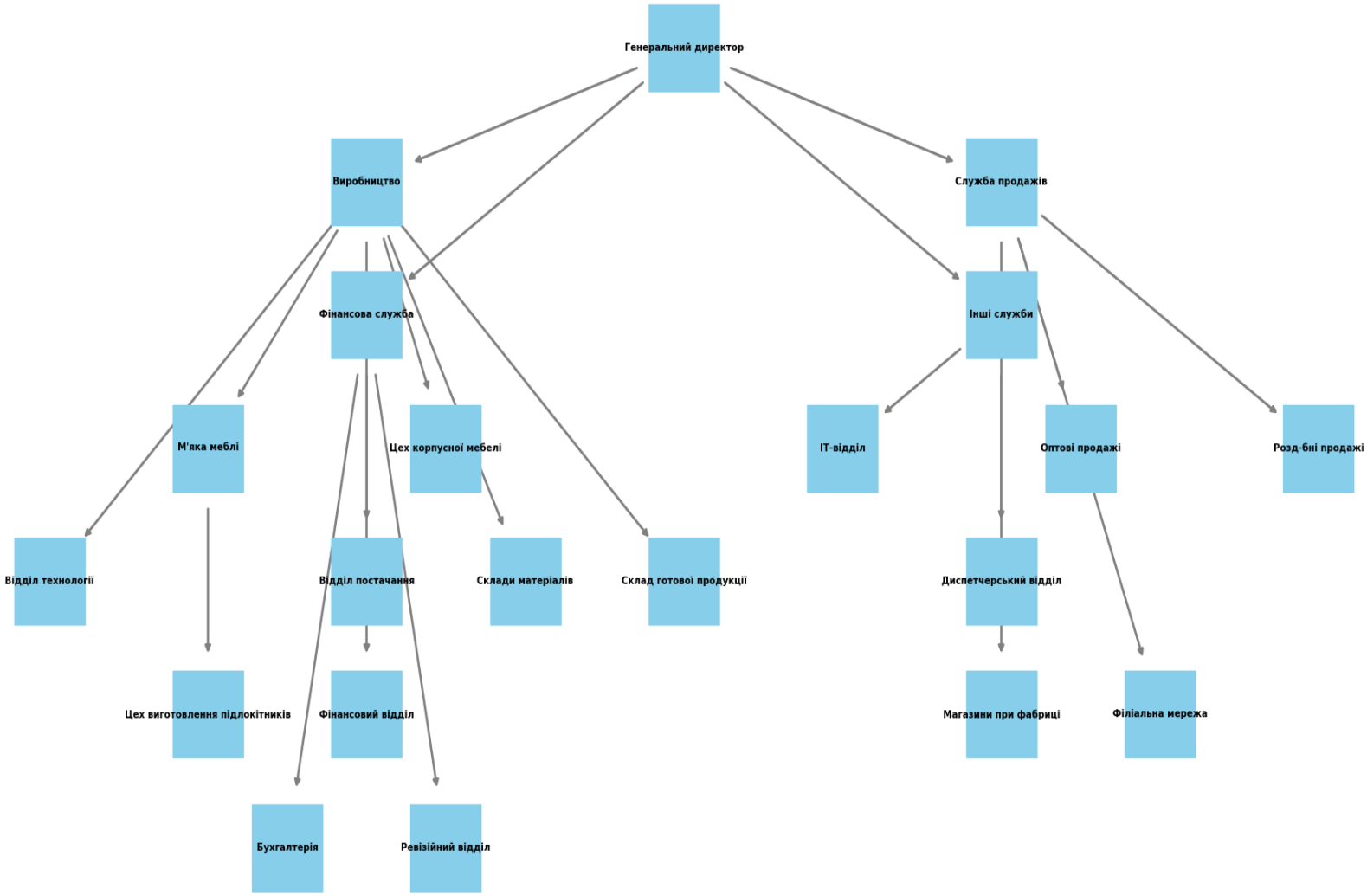

Рисунок 2.1 – Структурна схема меблевої фабрики «Прогрес» [13].

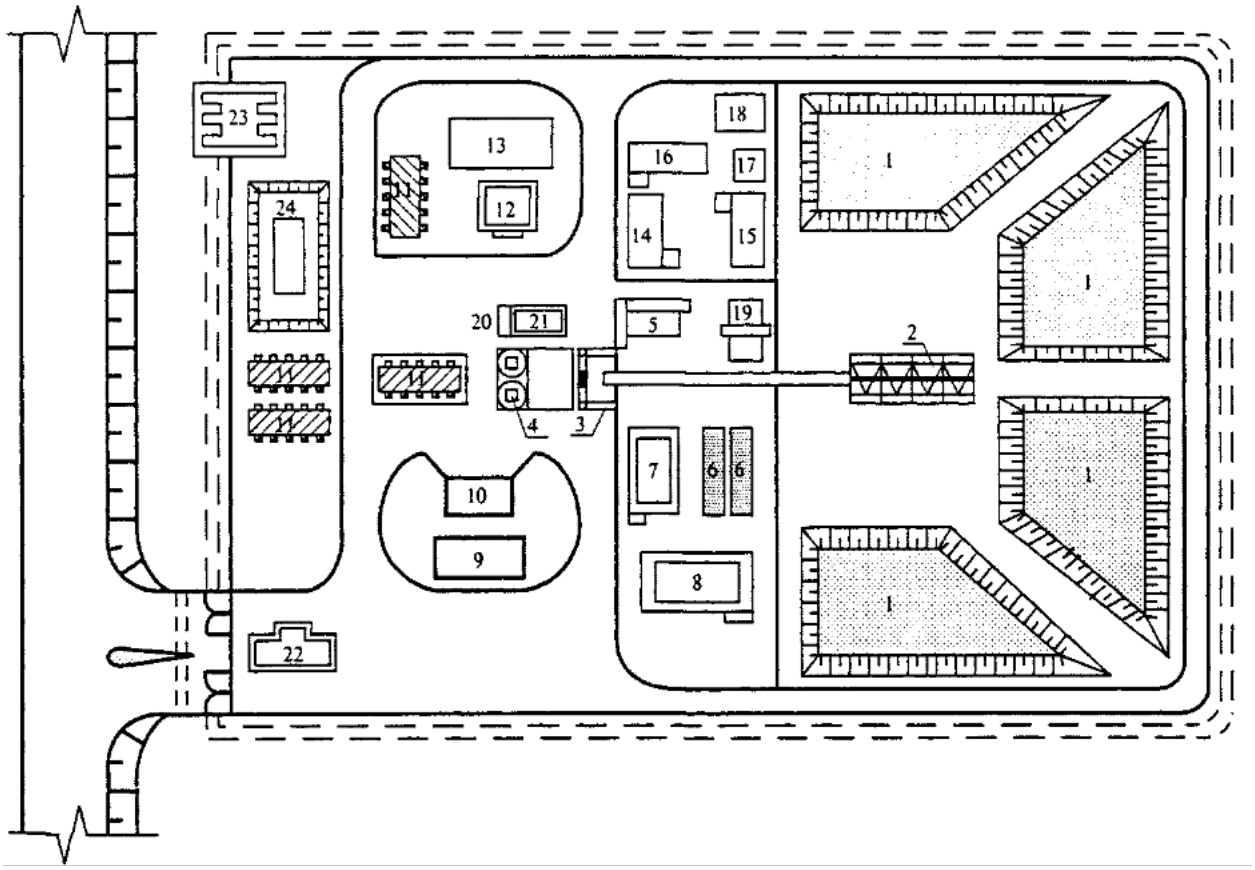

Рисунок 2.2 – План виробничого комплексу фабрики

Корпуси м’якої мебелі (№ 1) – три великі будівлі, у яких розташовані цехи, що спеціалізуються на виготовленні м'якої мебелі різних типів. Тут відбувається більшість виробничих операцій, пов'язаних з обробкою матеріалів і складанням продукції.

Транспортний коридор і навантажувальна зона (№ 2) – зона, призначена для транспортування матеріалів і готової продукції між виробничими корпусами та складськими приміщеннями. Тут здійснюється навантаження та розвантаження продукції.

Склад готової продукції (№ 3) – приміщення для зберігання виготовлених меблів перед їх відправленням на продаж.

Склад сировини і матеріалів (№ 4) – зона, де зберігаються матеріали та комплектуючі для виробничого процесу, такі як тканини, дерево та інші необхідні ресурси.

Цех шкіряної мебелі (Voyage) і цех корпусної мебелі (№ 6 і № 7) – ці будівлі використовуються для виготовлення меблів зі шкіри, а також корпусних конструкцій, що включають різні каркасні меблі.

Відділ технології, ТК та планування (№ 5) – відділ, який відповідає за технологічне управління виробництвом, планування процесів та контроль якості на всіх етапах виготовлення.

Відділ постачання (№ 8) – приміщення, в якому організовано роботу зі зберігання та забезпечення матеріалів для виробництва. Цей відділ також відповідає за логістику та комплектацію.

Склади матеріалів та готової продукції (№ 3 і № 4) – зони, що займаються зберіганням матеріалів і готових меблів перед відправленням.

Їдальня для персоналу (№ 9) – приміщення, де співробітники підприємства можуть харчуватися під час робочих змін.

Медпункт (№ 10) – забезпечує медичну допомогу для працівників та може включати кімнату першої допомоги для надання невідкладної допомоги.

Служба продажів (№ 11) – окремий відділ, який займається реалізацією продукції, зокрема організує оптові, роздрібні продажі та продажі через дистриб'юторів.

Магазини при фабриці (№ 12) – приміщення, де кінцеві споживачі можуть придбати меблі безпосередньо на території фабрики.

Фінансова служба (№ 13, 14, 15) – включає фінансовий відділ, бухгалтерію та ревізійний відділ. Ці підрозділи здійснюють фінансовий контроль, облік і аудит діяльності підприємства.

IT-відділ (№ 17) – відповідає за технічну підтримку, автоматизацію бізнес-процесів та забезпечення роботи IT-інфраструктури.

Секретаріат та диспетчерський відділ (№ 18 і № 19) – адміністративні підрозділи, що виконують функції документування, розподілу завдань та організації роботи підприємства.

Компресорна або технічна зона (№ 20) – приміщення, де може знаходитися технічне обладнання, необхідне для підтримки виробничих процесів, як-от компресори.

Пожежна станція або протипожежне обладнання (№ 21) – забезпечує безпеку на випадок пожежі та відповідає за протипожежний захист об'єктів.

Контрольно-пропускний пункт (КПП) (№ 22) – місце для контролю в'їзду та виїзду транспорту та персоналу на територію підприємства.

Підсобні приміщення або комунальна зона (№ 23) – приміщення для зберігання інструментів, матеріалів та іншого допоміжного обладнання.

Гараж або технічне обслуговування (№ 24) – забезпечує обслуговування транспорту підприємства.

2.2 Стислі відомості про комп'ютерну систему меблевої фабрики «Прогрес» з функціями відеонагляду та пожежної сигналізації

Однією із вимог замовника для побудови мережі меблевої фабрики «Прогрес» з функціями відеонагляду та пожежної сигналізації було використання обладнання Cisco. Головні переваги даного обладнання:

− забезпечення високого рівня адаптивності бізнесу завдяки автоматизації мережі;

− автоматичне відновлення даних та їх резервування після можливих збоїв;

− відмінні показники параметрів надійності та відмовостійкості; − виняткова продуктивність бездротових мереж із високою щільністю підключення;

− комплексний підхід до контролю нормальної працездатності мереж та докладне інструктування щодо усунення збоїв;

− мінімізація вразливості у будь-яких точках мережі;

− можливість застосування аналітики для оптимізації продуктивності та програмного забезпечення;

− підтримка IoT-рішень для інтеграції систем відеоспостереження та пожежної сигналізації.

Для вирішення поставлених завдань у комп'ютерній системі меблевої фабрики використано сервіс DHCP, який дозволяє пристроям автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Було обрано протокол динамічної маршрутизації OSPF, оскільки це вдосконалений дистанційно-векторний протокол, який забезпечує надійну маршрутизацію та швидке відновлення при зміні маршруту. Система використовує NAT для забезпечення зв'язку між різними підмережами, що дозволяє ефективно розподіляти ресурси та забезпечувати безпеку передачі даних.

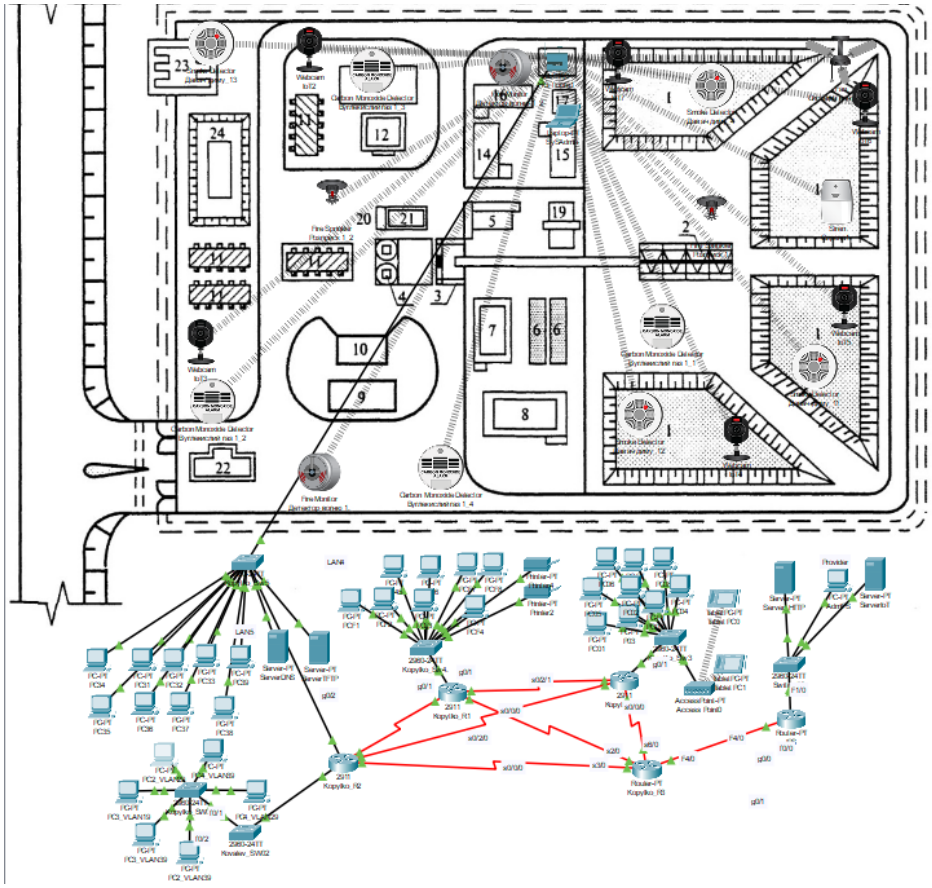

Рисунок 2.3 – Архітектура комп’ютерної мережі меблевої фабрики «Прогрес»

На представленій схемі мережі рис.2.3 видно, що використовуються різні IoT-сенсори, такі як датчики диму та моноксиду вуглецю, інтегровані з

відеокамерами та контролерами, що дозволяє відстежувати стан пожежної безпеки та записувати відео у випадку активації тривоги. Сервери для обробки та зберігання відеозаписів розташовані у безпечному середовищі, з резервуванням на випадок збоїв.

Таким чином, архітектура загальної мережі, розроблена для меблевої фабрики «Прогрес», представлена на рисунку, демонструє ефективне поєднання технологій Cisco, які забезпечують безпеку, відмовостійкість та підтримку IoT-рішень для контролю та моніторингу систем відеоспостереження та пожежної сигналізації.

2.3 Аналіз підходів до моделювання комп'ютерної системи з функціями відеонагляду та пожежної сигналізації

Обробка відеоданих є ключовим завданням при розробці комп’ютерних систем, особливо тих, що передбачають моніторинг і забезпечення безпеки. Незважаючи на простоту збирання та зберігання відеоінформації, процес отримання релевантної інформації з відеоданих є значно складнішим. Основний етап обробки відео полягає в перетворенні неструктурованих відеоданих у структуровану форму, яка підходить для подальшого аналізу.

Перший етап обробки відеоданих передбачає їхнє перетворення в структурований формат. Відеодані, зібрані з камер або інших джерел, мають бути упорядковані для подальшої обробки, що вимагає застосування технік обробки зображень та методів комп'ютерного зору. Це включає виділення ключових елементів, таких як кадри, аудіо, текстові метадані, а також видалення цифрового шуму та компенсацію змін освітлення для уникнення хибних спрацьовувань.

Відеобази даних можуть мати різні структури, залежно від характеру відеоматеріалу. Сценарійні відео, наприклад, організовані за сценарієм і включають фільми, новини або інші матеріали з наперед визначеними сценами. У випадку несценарійних відео, таких як відео з камер

спостереження або спортивні записи, структура сцени відсутня, і вони представляють собою "необроблений" матеріал, що потребує особливих підходів для поділу на ключові елементи.

Одним із фундаментальних завдань при обробці відео є поділ довгих відеопослідовностей на окремі кадри з виділенням ключових кадрів, що полегшує індексування і пошук інформації. Для цього застосовуються методи візуального індексування та аналізу структури відео. Наприклад, деякі дослідники запропонували методи для виявлення меж кадрів, виділення ключових кадрів, а також аналізу даних для візуалізації змін у сценах. Такі підходи значно підвищують ефективність обробки відео та дозволяють забезпечити автоматизоване визначення подій.

Крім того, виділення специфічних ознак із відео, таких як форма об’єктів, рух, текстура чи колір, є важливим етапом для подальшого аналізу та класифікації. Сучасні технології дозволяють використовувати методи трансформації та аналізу ознак для виявлення патернів і автоматизації розпізнавання подій, що особливо актуально в системах відеоспостереження та безпеки [14].

2.3.1 Модель відеоданих

Ефективне керування та пошук відеоконтенту потребують спеціалізованих моделей даних, оскільки традиційні реляційні чи об’єктно-орієнтовані моделі мають обмежені можливості для роботи з відеоінформацією. Основними причинами цього є: (1) відсутність засобів для управління просторово-часовими зв’язками, (2) недостатність методів інтерпретації необроблених даних у семантичний зміст, та (3) брак підтримки складних запитів для структурованого пошуку.

Модель відеоданих – це спосіб представлення інформації про відео, його характеристики та зміст, що спрямований на підтримку специфічних завдань, таких як сегментація чи анотація відеоматеріалів. Ефективна модель дозволяє

відображати відеодані на різних рівнях, полегшуючи інтелектуальний аналіз. Наприклад, Петкович і Йонкер запропонували модель пошуку даних на основі вмісту, яка складається з чотирьох рівнів:

–рівень необроблених відеоданих – включає послідовність кадрів та базові атрибути відео;

–рівень функцій – містить незалежні від домену характеристики, такі як кольори, текстури, форми та рухи, які можна автоматично витягнути з необроблених даних;

–рівень об’єктів – описує сутності з просторовими характеристиками, що пов’язують області між кадрами;

–рівень подій – зосереджується на часових аспектах, що включають рухи та взаємодії об’єктів у просторі-часі.

Іншою перспективною моделлю є ієрархічна структура бази даних, запропонована Чжу та ін., яка використовує семантичні одиниці відео для створення структурованих індексів бази даних. Ця модель дозволяє відображати зв’язки між концепціями високого рівня (сцени, події) і ознаками низького рівня (кадри, об’єкти).

Ієрархічний підхід забезпечує поділ і організацію відеовмісту в набір ієрархічно керованих одиниць, таких як кластери, підкластери, об’єкти, кадри чи площини відео. Це значно підвищує ефективність представлення, індексації та доступу до відеоданих. Модель також підтримує автоматизацію процесів аналізу завдяки гнучкості у роботі з різними рівнями деталізації відеовмісту.

Застосування таких підходів є важливим для розробки систем відеоспостереження, які потребують швидкого й точного доступу до інформації. Використання багаторівневих моделей дозволяє створити інструменти, здатні відповідати на складні запити, забезпечуючи релевантну аналітику та ефективний пошук у відеобазах даних [20].

2.3.2 Сегментація відео

Сегментація відео є першим і важливим етапом у будь-якій системі керування відеоданими. Цей процес передбачає поділ відеодоріжки на менші одиниці, що дозволяє ефективно виконувати подальші операції, такі як індексування відео, семантичне представлення, відстеження обраної інформації та визначення кадрів, у яких відбувається перехід між різними сценами або знімками. Візуальна сегментація полягає у виявленні меж кадрів, тоді як сегментація на основі руху визначає такі дії, як панорамування або масштабування.

Більшість відеоконтенту, зокрема з повсякденного життя, можна представити у вигляді ієрархії рівнів як показано на рис.2.4. Ця ієрархія включає поняття "відео", "сцена", "відеогрупа", "знімок" і "ключовий кадр".

Відео – це мультимедійна послідовність, яка складається з аудіоданих і ряду зображень.

Сцена – семантично пов’язана та темпорально згуртована сукупність знімків, яка фокусується на одній точці або місці інтересу. Вона відображає високорівневу концепцію, пов’язану з відеовмістом.

Відеогрупа – проміжна сутність між окремими кадрами та сценою, яка слугує містком між фізичними кадрами та семантичним контекстом. Відеогрупа складається з двох видів кадрів:

Тимчасово пов’язані кадри – серії кадрів, схожих за часовими характеристиками.

Просторово пов’язані кадри – кадри, подібні за візуальними ознаками.

Знімок – послідовність кадрів, зроблених однією камерою без значних змін у візуальному вмісті. Одним із головних завдань сегментації є виявлення меж знімків, що є складним через різноманіття змін у відео, таких як різкі або поступові переходи між кадрами.

Ключовий кадр – це кадр, який найкраще представляє зміст конкретного знімка. Оскільки більшість сусідніх кадрів мають схожий візуальний зміст, з

них можна вибрати один або кілька ключових кадрів залежно від складності відео. Витягнуті ключові кадри слугують важливими репрезентаціями візуального змісту відеопотоку.

Сегментація відео є важливою для ефективної організації та аналізу відеоданих, оскільки вона забезпечує структурування інформації для індексування, доступу та подальшої аналітики. Використання ключових кадрів, знімків і семантичних груп дозволяє створити багаторівневу модель для оптимізації обробки та зберігання відеоінформації [21].

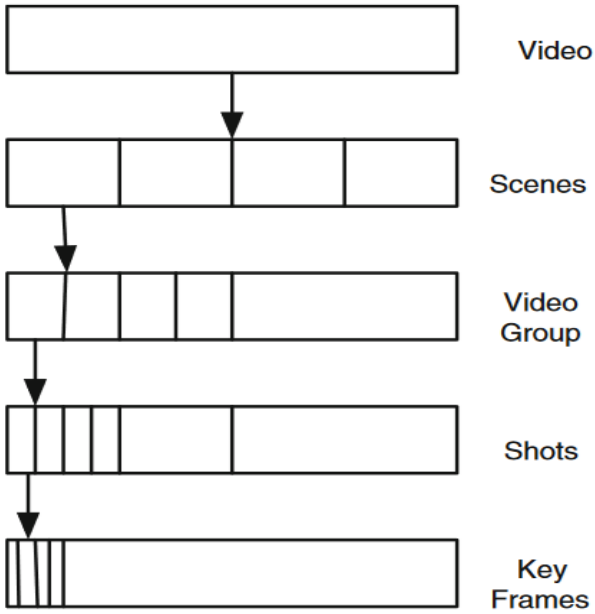

Рисунок 2.4 – Ієрархія відео даних

2.3.3 Вилучення ознак

Після сегментації відео та вибору ключових кадрів із них можна витягти ознаки на рівні зображення. Візуальні ознаки низького рівня, такі як колір, текстура, крайові елементи та форми, витягуються і подаються у вигляді дескрипторів ознак. Ознака визначається як параметр, що описує вміст зображення або відео. Розрізняють два види ознак, які можуть бути витягнуті з відео [19]:

– ознаки на основі опису – використовують метадані, такі як текстовий опис, підпис, розмір файлу та час створення;

– ознаки на основі вмісту – базуються на візуальному змісті самого об’єкта. Вони поділяються на: глобальні ознаки, виділені з усього зображення; та локальні або регіональні ознаки, що описують вибрані області зображення.

Кожна область обробляється для витягнення ознак, що характеризують її зорові властивості, включаючи колір, текстуру, рух та структуру регіону. Існують також ознаки на основі кадру та на основі об'єкта, які використовуються для доступу до відеоконтенту в базах даних. Так, в роботі [18] проаналізували ознаки відео, як-от гістограми кольорів, колірні домени, краєві елементи та текстури, зберігаючи їх у форматі XML для подальшої обробки відео. Автори в [19] представили низькорівневі ознаки, такі як положення об'єктів, розміри, корелограми кольору, а також семантично значущі ознаки високого рівня, зокрема категорії об'єктів і траєкторії руху.

Для виявлення важливих патернів у відео можуть використовуватися просторові (візуальні), звукові та часозалежні ознаки рухомих об'єктів [20]. Ці шаблони оцінюються та інтерпретуються для отримання знань, корисних для різних додатків. Виявлення об'єктів, подій і сцен у відео є важливим для багатьох застосувань, наприклад, як точки входу для пошуку та перегляду відео або як основа для його узагальнення. В роботі [21] ідентифікували футбольні події шляхом виділення кількох ознак, таких як візуальні та слухові характеристики, текст та аудіо ключові слова.

2.3.4 Аналіз підходів до моделювання пожежної сигналізації

Питання виявлення небезпеки у системах пожежної сигналізації стало об'єктом численних наукових досліджень останніх років. Одним з ключових напрямів є розвиток автоматичного виявлення пожеж з використанням інтелектуальних технологій. Такі системи виявлення можна класифікувати за

кількома основними категоріями: сповіщувачі пожежі, методи зменшення кількості помилкових спрацювань, аналіз даних про пожежі та прогнозування їх розвитку. Цей підхід дозволяє детальніше вивчити важливі аспекти надійності систем пожежної сигналізації, зокрема в умовах розподілених систем.

Зокрема, хімічні сенсорні системи, що використовуються для виявлення отруйних газів, що виникають під час пожеж, значно вдосконалюються завдяки новітнім алгоритмам обробки даних. Використання багатовимірних моделей дозволяє корелювати дані, що надходять з різних сенсорів, що підвищує точність виявлення небезпеки.

Для підвищення ефективності системи виявлення пожеж застосовуються мультисенсорні методи, що використовують різні типи сенсорів, такі як димові, полум'яні та температурні датчики. Це дозволяє зменшити ймовірність помилкових спрацювань і покращити загальну ефективність системи.

Інший важливий напрямок розвитку — виявлення пожеж за допомогою відеоспостереження. Використання послідовностей кадрів із відеокамер дозволяє здійснювати детектування полум'я в реальному часі, що є особливо важливим для захисту великих відкритих територій.

Для моніторингу великих відкритих просторів також використовуються алгоритми на основі нечітких методів, що забезпечують високу точність виявлення диму. Такі методи демонструють свою ефективність на територіях, де розміщено багато потенційних джерел пожеж.

Аналіз надійності систем пожежної сигналізації має велике значення для забезпечення безпеки в екстремальних умовах, зокрема в висотних будівлях. Параметри конфігурації системи можуть істотно впливати на ефективність евакуації людей, що потребує особливого уваги при проектуванні таких систем.

Використання бездротових систем пожежної сигналізації дозволяє забезпечити мобільність та гнучкість в управлінні сигналізацією, проте це

також вимагає детального аналізу їх надійності та відповідності стандартам, таким як EN-54.

Крім того, для оцінки пожежної небезпеки активно застосовуються методи аналізу ризиків, зокрема методи дерева несправностей та мережі Байєса. Вони дозволяють розглядати взаємозв'язки між різними подіями, системами виявлення та їх наслідками, що є важливим для розробки ефективних стратегій управління ризиками..

2.4 Загальна модель системи відеонагляду та пожежної сигналізації

Система відеонагляду та пожежної сигналізації базується на центральному контролері Cisco MX Series, що забезпечує збір, обробку та передачу даних від підключених периферійних пристроїв. Основними компонентами системи є вебкамера (LogiTech), сенсор BME280 та веб-застосунок для інтерактивного моніторингу та управління (рис.2.5).

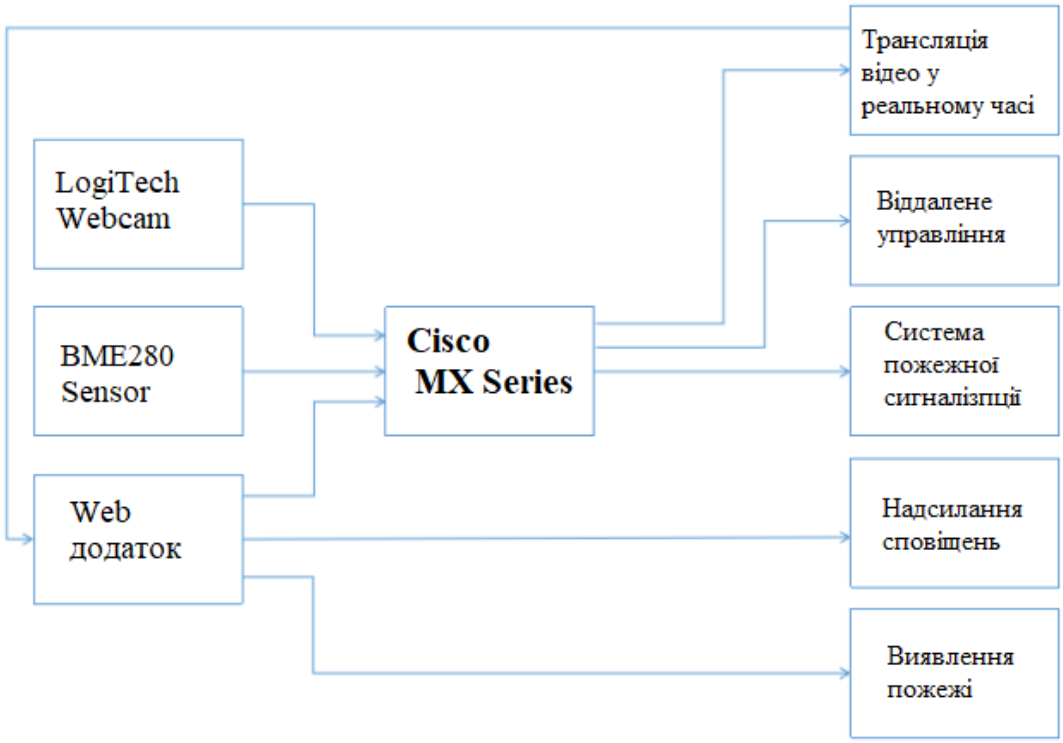

Рисунок 2.5 – Структурна схема моделі системи відеонагляду та пожежної сигналізації

LogiTech Webcam – забезпечує захоплення відеопотоку у реальному часі для моніторингу ситуації та виявлення ознак диму чи полум'я.

BME280 Sensor – вимірює параметри навколишнього середовища, такі як температура, вологість і атмосферний тиск. Ці показники використовуються для виявлення потенційних ознак пожежі.

Cisco MX Series – виконує роль центрального обчислювального вузла, який обробляє відео з вебкамери та дані від сенсора. Він також відповідає за передачу обробленої інформації на веб-застосунок та надсилання сповіщень користувачеві у разі виявлення пожежі.

Web додаток – слугує інтерфейсом для перегляду відео, моніторингу сенсорних даних, отримання сповіщень та дистанційного управління системою.

Функціональні можливості системи:

– вебкамера передає потік відео до Raspberry Pi, який транслюється на веб-застосунок для віддаленого перегляду;

– обробка даних від BME280 сенсора та аналіз відео за допомогою алгоритмів машинного навчання чи правил для виявлення ознак диму та полум'я;

– у разі виявлення пожежі система виділяє пожежу на камері і пише відповідне повідомлення та надсилає користувачу через веб-застосунок або інші канали сповіщення;

– користувач може переглядати дані в реальному часі, отримувати сповіщення та взаємодіяти з системою через веб-застосунок.

2.4.1 Математичний опис роботи системи

Нехай T(t) – температура, H(t) – вологість, P(t) – тиск у момент часу t. Значення передаються від сенсора BME280 до Cisco MX Series і для аналізу відео даних.

Система спрацьовує на основі перевищення порогових значень параметрів [20]:

$$F_{sensor}(t) = \begin{cases} 1, & \text{якщо } T(t) > T_{crit} \text{ і } H(t) < H_{crit}, \\ 0, & \text{в іншому випадку.} \end{cases}$$

(2.1)

де Tcrit і *H*crit – задані порогові значення температури та вологості.

Функція обробки відео D(V(t)) приймає кадр відео V(t) та повертає 1, якщо виявлено дим чи полум'я, і 0 в іншому випадку [22]:

$$F_{video}(t) = D(V(t)).$$

(2.2)

Система активує сигналізацію, якщо одна з умов виявлення пожежі спрацьовує [22]:

$$Alert(t) = \max(F_{sensor}(t), F_{video}(t)).$$

(2.3)

Для математичного опису системи запропоновано використати рівняння Колмогорова-Чепмена, яке описує ймовірності переходів між різними станами системи. У контексті пожежної сигналізації система описує стани: "нормальний стан", "стан тривоги", "пожежа", тощо).

Загальний вигляд рівняння Колмогорова-Чепмена для ймовірності переходу між станами в системі можна подати так [22]:

$$\frac{dP_i(t)}{dt} = \sum_{j \neq i} (P_{ij} \cdot P_j(t) - P_{ji} \cdot P_i(t))$$

(24)

де: Pi(t) – ймовірність того, що система знаходиться в стані i в момент часу t, Pij – інтенсивність переходу від стану i до стану j, Pji – інтенсивність переходу від стану j до стану i.

Для конкретної системи пожежної сигналізації можна розглядати наступні стани:

– стан 0 — система в нормальному стані (немає вогню);
– стан 1 — система виявила дим або пожежу (тривога);
– стан 2 — пожежа активована, система передає сигнал на гасіння.

Для представлення потоку даних у системі можна використати орієнтований граф, де вузли позначають компоненти системи, а ребра – потоки даних між ними.

Для представлення потоку даних у системі можна використати орієнтований граф (рис.2.6), де вузли позначають компоненти системи, а ребра – потоки даних між ними.

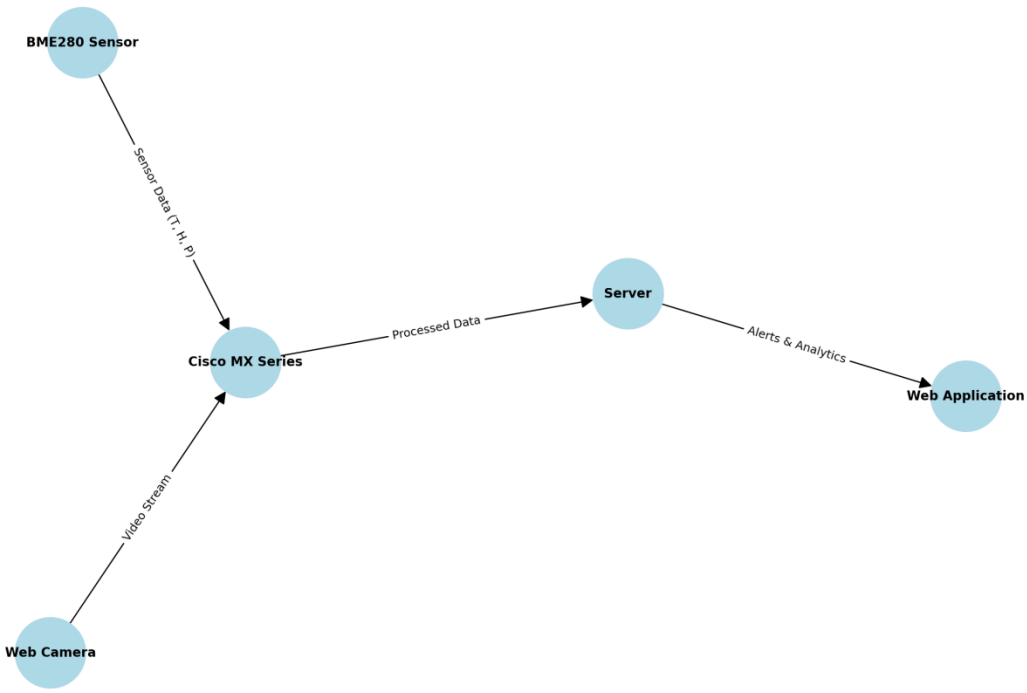

Рисунок 2.6 – Граф системи відеонагляду та пожежної сигналізації на основі потоків даних між ними

Нехай G=(V,E) – орієнтований граф, де: V – множина вузлів, що представляє компоненти системи. E – множина орієнтованих ребер, які показують, як дані передаються між компонентами.

Вузли V:

– $v1$ – BME280 сенсор;

– $v2$ – LogiTech вебкамера;

– $v3$ – Cisco MX Series;

– $v4$ – сервер для обробки та зберігання дани;

– $v5$ – веб-застосунок для сповіщення користувача;

Ребра E:

– $e1=(v1,v3)$ – передача даних про температуру, вологість та тиск від сенсора до Raspberry Pi.

– $e2=(v2,v3)$ – передача відеопотоку від вебкамери до Raspberry Pi.

– $e3=(v3,v4)$ – передача оброблених даних та відео на сервер.

– $e4=(v4, v5)$ – передача повідомлень та сигналів тривоги до веб-застосунку.

Розглянемо функції, що описують стан компонентів та передачу даних.

Сенсорні дані T(t),H(t),P(t) – передаються від $v1$ до $v3$ по $e1$.

Відеопотік V(t) – передається від $v2$ до $v3$ по $e2$.

Аналіз даних на Cisco MX Series F(t) та D(V(t)) обчислюються на $v3$.

Сигналізація: Активується, якщо Alert(t)=1, і передається через $e4$ до $v5$.

2.5 Висновки до розділу

У другому розділі було детально розглянуто структуру та характеристики комп'ютерної системи меблевої фабрики «Прогрес», що включає функції відеонагляду та пожежної сигналізації. Проаналізовано основні компоненти цієї системи, а також підходи до її моделювання, що охоплюють як відеоаналіз, так і функціонування системи пожежної сигналізації.

Моделювання відеоданих та їх сегментація виявилися важливими елементами для ефективного оброблення інформації, що надходить з камер

спостереження. Використання методів вилучення ознак дозволяє точно аналізувати ситуації, що виникають на фабриці, і оперативно реагувати на них. Важливим етапом було також вивчення методів моделювання пожежної сигналізації, що забезпечують своєчасне виявлення небезпечних ситуацій і мінімізацію ризиків для персоналу та майна.

Розглянуто загальну модель системи відеонагляду та пожежної сигналізації, що дозволяє підвищити рівень безпеки та автоматизувати процеси реагування на надзвичайні ситуації. Математичне описання роботи цих систем дає змогу не лише забезпечити точність у виявленні потенційних загроз, але й оптимізувати їх взаємодію з іншими елементами фабричної інфраструктури.

РОЗДІЛ 3
СИНТЕЗ СИСТЕМИ КОНТРОЛЮ МЕРЕЖЕВОГО ТРАФІКУ

3.1 Розробка схеми функціональної структури

Розробка функціональної схеми є важливим етапом у проектуванні системи, оскільки вона дозволяє чітко визначити основні компоненти, їх взаємодію та ролі в загальній архітектурі. Метою створення функціональної схеми є забезпечення зрозумілого й ефективного взаємозв'язку між різними блоками системи, що дозволяє спростити процеси керування, обробки даних і моніторингу.

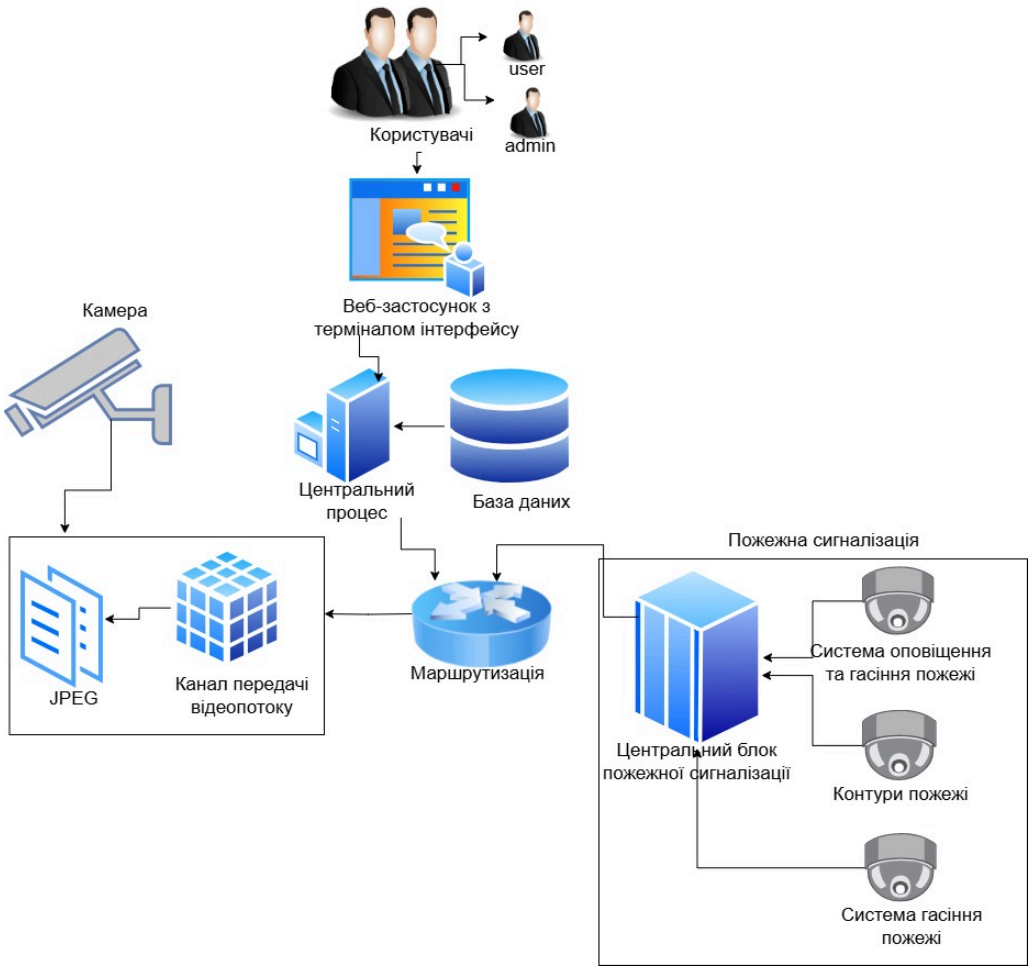

Рисунок 3.1 – Функціональна схема комп’ютерної мережі

У рамках схеми на рис.3.1 розглядаємо комплексну систему, яка включає в себе кілька основних блоків: центральний сервер, базу даних, термінали користувачів, системи відеоспостереження та пожежної сигналізації, а також інші компоненти, що забезпечують безпеку, комунікацію та інтеграцію з зовнішніми сервісами. Кожен з цих блоків має своє специфічне призначення та функції, але їх взаємодія в межах єдиної системи має бути ретельно спланована для забезпечення ефективної роботи всієї інфраструктури.

У системі передбачено два основних типи користувачів: звичайний користувач (персонал, охорона, технічний працівник) та адміністратор (керівник, відповідальний за налаштування і управління системою).

Звичайний користувач має обмежений доступ до функцій системи. Він може взаємодіяти з кількома її компонентами залежно від своїх обов'язків. Це може включати:

– перегляд відео через веб-застосунок або термінали інтерфейсу користувача, щоб моніторити стан безпеки на фабриці;

– взаємодія з системою пожежної сигналізації, наприклад, отримання сповіщень про тривоги, перевірка стану датчиків диму або температури;

– доступ до певних даних в межах своєї ролі, наприклад, перевірка актуальності записів або перегляд журналів подій на території фабрики.

Звичайний користувач, як правило, не має прав на зміну налаштувань системи або управління важливими функціями (наприклад, активуванням системи гасіння пожежі чи зміною параметрів відеоспостереження). Його доступ обмежений лише необхідним для виконання робочих завдань.

Адміністратор має повний доступ до всієї системи та може виконувати різноманітні управлінські та налаштувальні операції. Його функції включають:

– конфігурація системи: адміністратор може налаштовувати параметри всіх компонентів, таких як відеоспостереження, пожежна сигналізація, мережеві налаштування, параметри користувачів тощо.

– керування доступом: адміністратор має змогу створювати та видаляти користувачів, призначати їм різні рівні доступу, налаштовувати права для звичайних користувачів.

– моніторинг та звітність: адміністратор може переглядати детальні звіти та логи всіх подій, отримувати повну інформацію про стан системи безпеки та відеоспостереження.

– управління інтеграціями: адміністратор може налаштовувати зовнішні інтеграції через вебхуки, підключати нові сервіси та підтримувати з'єднання з іншими платформами, такими як хмарні сховища або зовнішні платформи для автоматизації, як Zapier або Slack.

– резервне копіювання та відновлення: адміністратор відповідає за налаштування політики резервного копіювання даних і може запускати процеси відновлення інформації у разі необхідності.

Основний блок керування (центральний сервер) є ядром всієї системи. Він відповідає за загальне керування, контроль за роботою всіх інших компонентів, а також за зберігання ключових даних. Центральний сервер обробляє всі запити, забезпечує зв'язок між різними модулями і забезпечує централізовану логіку. Сервер також відповідає за доступ до бази даних та надає API для взаємодії з іншими компонентами, такими як термінали користувачів, системи безпеки, відеоспостереження і зовнішні інтеграції.

База даних зберігає всю інформацію, необхідну для роботи системи. Це можуть бути дані про фабрику, записи відеоспостереження, логи пожежної сигналізації, а також інші необхідні дані. Вона забезпечує швидкий доступ до інформації та її надійне зберігання, а також підтримує взаємодію між різними компонентами системи. Запити до бази даних виконуються через центральний сервер, що дозволяє централізовано керувати даними та їх обробкою.

Термінали інтерфейсу користувача включає в себе всі пристрої, які дозволяють персоналу фабрики взаємодіяти із системою. Термінали надають доступ до всіх функцій системи через графічний інтерфейс користувача (GUI). Це можуть бути комп'ютери, планшети, монітори або спеціалізовані робочі станції, на яких персонал може здійснювати моніторинг, управління та перевірку стану системи відеоспостереження, пожежної сигналізації та інших важливих процесів на фабриці.

Блок системи відеоспостереження (IP-камери, обробка відео) відповідає за збори та обробку відеоданих з IP-камер, які встановлені по всій території фабрики. Камери записують відео, яке передається до системи для зберігання або аналізу. Блок обробки відео може включати в себе різні алгоритми для автоматичного аналізу, такі як виявлення руху, розпізнавання осіб або інші методи для забезпечення безпеки. Відео також може передаватися до віддалених моніторингів або зберігатися в спеціалізованих сховищах для подальшого перегляду чи використання.

Сховище (зберігання відео) – це компонент, який забезпечує фізичне або хмарне зберігання великих обсягів відеофайлів, що надходять від системи відеоспостереження. Сховище є локальним (на серверах всередині підприємства), але в майбутньому може бути в хмарі (наприклад, на Amazon S3, Google Cloud Storage). Важливою особливістю сховища є те, що відеофайли повинні зберігатись у форматі, який дозволяє швидкий доступ та перегляд, а також можливість довготривалого архівування та резервного копіювання.

Блок пожежної сигналізації та безпеки інтегрує різні системи безпеки на фабриці, зокрема систему пожежної сигналізації. Він складається з датчиків диму, температури та інших сенсорів, які встановлені у критичних точках фабрики для виявлення пожежі. Коли система виявляє аномальні умови, вона активує сигнал тривоги, інформуючи персонал та відповідні служби про небезпеку. Водночас, блок може активувати автоматичну систему гасіння

пожежі або інші заходи безпеки, щоб запобігти збиткам або людським жертвам.

Блок мережевої комунікації забезпечує внутрішнє підключення між усіма компонентами системи через локальну мережу (LAN). Він дозволяє централізовано обробляти та передавати дані між різними підсистемами, такими як система відеоспостереження, пожежна сигналізація, термінали інтерфейсу користувача та центральний сервер. Блок мережевої комунікації відповідає за підтримку надійної та безпечної мережі для усіх внутрішніх компонентів системи.

Інтернет-з'єднання забезпечує підключення системи до глобальної мережі Інтернет. Це необхідно для резервного копіювання даних в хмару, віддаленого моніторингу або управління системою через інтерфейси, доступні ззовні. Інтернет-з'єднання також необхідне для інтеграції з іншими зовнішніми сервісами через API або вебхуки (наприклад, для сповіщень або інтеграцій з іншими системами).

Шлюз для зовнішнього доступу дозволяє здійснювати захищений віддалений доступ до системи для моніторингу та управління. Це може включати в себе доступ для керівників підприємства, технічного персоналу або зовнішніх контрагентів, що мають право на перегляд даних або взаємодію з системою. Шлюз використовує захищені протоколи, такі як VPN або SSH, для забезпечення безпеки під час віддаленого доступу, що дозволяє уникнути несанкціонованого втручання у систему.

Веб-застосунок для перегляду відео надає користувачам доступ до відео, записаних системою відеоспостереження. Через веб-застосунок можна переглядати відео в реальному часі або доступатися до архіву відео. Користувачі можуть переглядати відео з різних камер, налаштовувати параметри перегляду, а також взаємодіяти з іншими даними, такими як записи з датчиків диму чи температури, щоб отримувати повну картину того, що відбувається на території фабрики.

Система пожежної сигналізації на меблевій фабриці «Прогрес» є комплексним рішенням для забезпечення безпеки виробничих і складських приміщень. Структурна схема представлена на рис.3.2 і складається з центрального блоку, який контролює всі підключені пристрої, а також мережі шлейфів для виявлення пожежі та сповіщення.

Центральний блок пожежної сигналізації взаємодіє з різними датчиками, такими як детектори диму і температури, і з ручними пожежними сповіщувачами, що забезпечує своєчасне виявлення загрози. Шлейфи виявлення поділяються на кілька контурів: один контролює основне виробниче приміщення, інші — складські зони та прилеглі ділянки. Додатково, система включає моніторинг технічного стану пожежного обладнання та інших важливих технічних пристроїв.

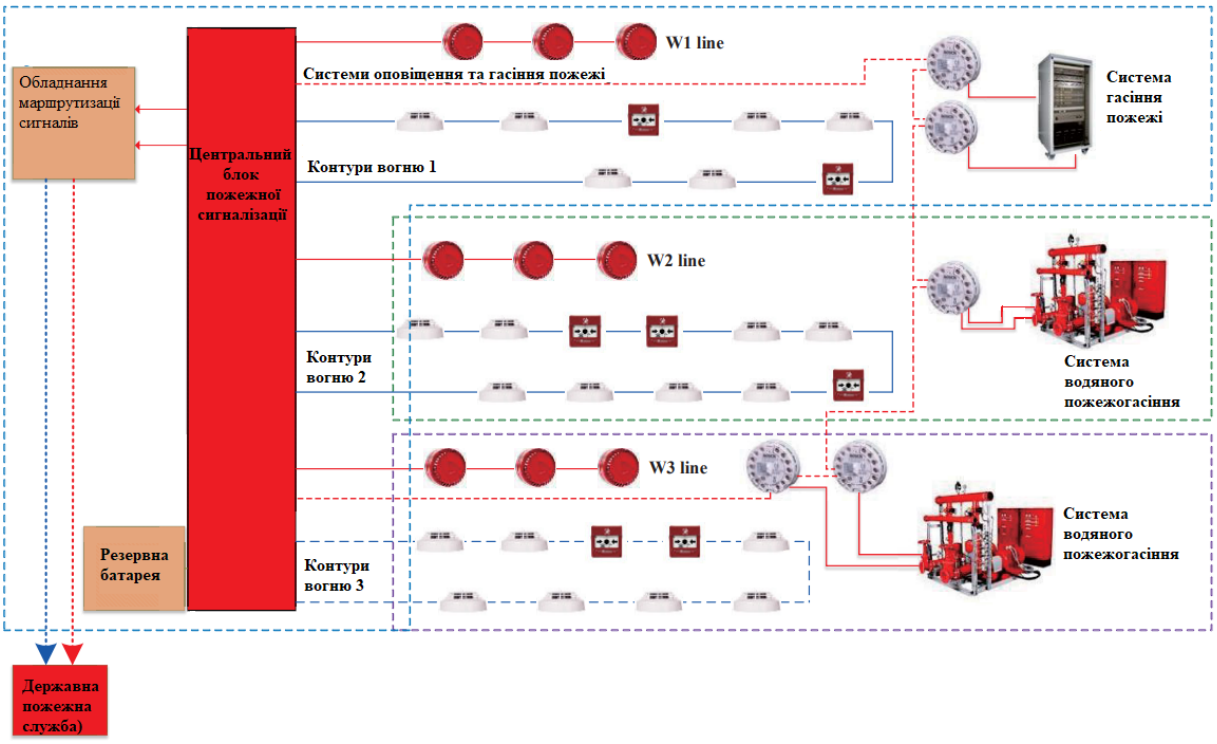

Рисунок 3.2 – Структурна схема пожежної сигналізації

Система пожежної сигналізації враховує обмеження на кількість підключених до шлейфів елементів, таких як детектори і сповіщувачі, відповідно до діючих норм і стандартів. Наприклад, відкриті лінії виявлення

можуть містити до 32 детекторів, а лінії з двома джерелами живлення — до 128 елементів.

Система складається з трьох окремих контурів для виявлення пожежі:

– контур 1 зв'язаний із різними детекторами диму та індикаторами, які передають сигнал тривоги у разі виявлення пожежі;

– контур 2 включає димові детектори, кнопки ручного увімкнення сигналізації та сирени для звукових оповіщень;

– контур 3 аналогічний іншим контурам, містить датчики диму та звукові індикатори.

Контрольні лінії (W1, W2, W3):

– лінія W1 виконує контроль та моніторинг системи акустичного оповіщення на всій станції, призначеної для оповіщення пасажирів та персоналу у випадку тривоги;

– лінія W2 відповідальна за контроль і моніторинг системи газового пожежогасіння на платформі 1;

– лінія W3 відповідає за контроль та моніторинг системи водяного пожежогасіння на платформі 2.

Крім того, на фабриці рекомендується встановити систему газового пожежогасіння, яка використовує вогнегасний агент HFC-227ea. Цей газ ефективно гасить полум'я, поглинаючи тепло та перериваючи ланцюгову реакцію горіння. Газові вогнегасники підключені до трубопроводів, які забезпечують рівномірне розподілення вогнегасного газу в охопленій зоні.

Для комп'ютерної системи меблевої фабрики «Прогрес» з функціями відеонагляду та пожежної сигналізації було обрано реляційну базу даних (РБД), оскільки вона дозволяє організувати зберігання даних у структурованому форматі, що забезпечує надійність, узгодженість та зручність доступу до інформації. Структура бази даних включає декілька основних таблиць, які забезпечують функціональність системи (рис.3.3).

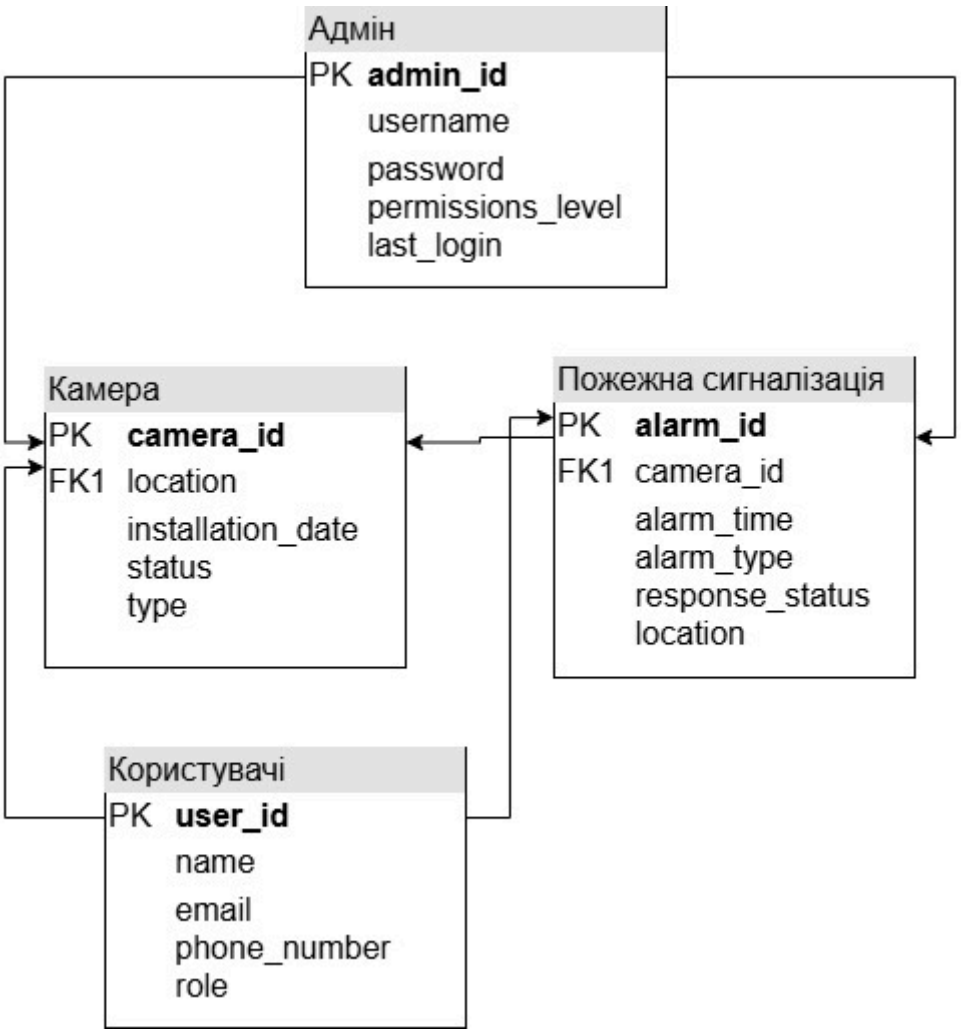

Рисунок 3.3 – Структура бази даних

Першою таблицею є «Камера», яка зберігає інформацію про камери відеонагляду. Вона містить такі поля, як camera_id (унікальний ідентифікатор камери, який є первинним ключем), location (місце розташування камери), installation_date (дата встановлення), status (статус камери: активна або неактивна), та type (тип камери: внутрішня чи зовнішня). Це дозволяє ефективно відслідковувати та управляти обладнанням на об’єкті.

Таблиця «Користувачі» містить дані про користувачів системи, включаючи user_id (унікальний ідентифікатор користувача), name (ім'я користувача), email (електронна адреса), phone_number (номер телефону) та role (роль користувача, наприклад, оператор або технік). Ця структура дозволяє керувати доступом користувачів до функцій системи відповідно до їхніх ролей.

«Адмін» є окремою таблицею, що містить інформацію про адміністраторів системи. Вона включає поля admin_id (унікальний ідентифікатор адміністратора), username (ім'я користувача адміністратора), password (зашифрований пароль), permissions_level (рівень доступу адміністратора) та last_login (час останнього входу в систему). Це забезпечує можливість управління системою та підтримки високого рівня безпеки.

Таблиця «Пожежна сигналізація» зберігає інформацію про події пожежної сигналізації. Вона включає alarm_id (унікальний ідентифікатор сигналу), location (місце розташування), alarm_time (час спрацювання сигналізації), alarm_type (тип сигналу: димова, температурна) та response_status (статус відповіді: активована, деактивована). Поле camera_id (зовнішній ключ) забезпечує зв'язок між камерами та зонами, що перебувають під наглядом, дозволяючи співвідносити події пожежної сигналізації з відповідними камерами.

Зв'язки між таблицями забезпечують цілісність даних. Таблиця «Камера» пов'язана з таблицею «Пожежна сигналізація» через поле camera_id, створюючи зв'язок типу one-to-many, що дозволяє відстежувати події пожежної сигналізації, які відбуваються в зоні спостереження кожної камери. Таблиця «Адмін» може логічно бути пов'язана з таблицею «Користувачі» для управління користувачами та їхніми доступами.

3.2 Вибір елементної апаратної бази системи

Для реалізації КС меблевої фабрики «Прогрес» розглянемо апаратну базу, яка представлена в таб 3.1 [5-8].

№	Позиція	Найменування і технічна характеристика	Тип, марка	Одиниці виміру	Кількість

1	Серверне обладнання	Центральний сервер для обробки даних (2x Intel Xeon, 128GB RAM, 2TB SSD)	Dell PowerEdge R750	Шт.	1
2	Серверне обладнання	Система зберігання даних (NAS, 8TB HDD, підтримка RAID 5)	Synology DS1821+	Шт.	1
3	Серверне обладнання	Обчислювальний модуль для локальної обробки відео та даних	Cisco MX Series	Шт.	1
4	Мережеве обладнання	Керований мережевий комутатор з підтримкою Gigabit Ethernet	Cisco Catalyst 9200	Шт.	2
5	Мережеве обладнання	Бездротова точка доступу (Wi-Fi 6, до 1.8 Гбіт/с)	Ubiquiti UAP-AC-PRO	Шт.	3
6	Мережеве обладнання	Модуль маршрутизатора з підтримкою VPN і захистом брандмауера	MikroTik CCR1009	Шт.	1
7	Мережеве обладнання	Кабельна система (Cat 6) для передачі даних	-	Метр	500
Продовження до табл. 3.1					
8	Відеокамери	Веб-камери для відеонагляду з високою роздільною здатністю (1080p)	LogiTech Webcam	Шт.	10
9	Контролери	Модулі контролерів для керування системою	Arduino Mega 2560	Шт.	5
10	Датчики диму	Датчики для виявлення диму	MQ-2 Smoke Sensor	Шт.	15
11	Датчики вогню	Інфрачервоні датчики для виявлення полум'я	Flame Sensor Module	Шт.	10
12	Датчики навколишнього середовища	Датчики для вимірювання температури, вологості та тиску	BME280 Sensor	Шт.	5
13	Датчики поливу водою	Датчики для автоматичного запуску системи зрошування	Water Sprinkler Sensor	Шт.	8

У таблиці представлено апаратне та мережеве обладнання, необхідне для створення комплексної комп'ютерної системи з функціями відеонагляду

та пожежної сигналізації на меблевій фабриці «Прогрес». До системи входять серверне та мережеве обладнання, відеокамери, контролери та різноманітні датчики, що забезпечують надійне функціонування системи та своєчасне виявлення загроз.

Серверне обладнання складається з центрального сервера для обробки великих обсягів даних, системи зберігання даних (NAS) для резервного копіювання та збереження інформації, а також обчислювального модуля Cisco MX Series, що обробляє відео та сенсорні дані. Мережеве обладнання включає керований комутатор, бездротові точки доступу для передачі даних та маршрутизатор для забезпечення безпечного з'єднання і підтримки VPN.

Система відеонагляду складається з веб-камер LogiTech, які забезпечують захоплення відеопотоку для внутрішнього і зовнішнього моніторингу. Контролери Arduino використовуються для інтеграції системних компонентів та управління процесами. Датчики диму та вогню забезпечують своєчасне виявлення ознак пожежі, а BME280 Sensor відстежує параметри навколишнього середовища для додаткової безпеки. Система зрошування обладнана датчиками, які автоматично запускають процес поливу у разі необхідності.

3.3 Розробка та налаштування обладнання та сервісів системи IoT

В Cisco Packet Tracer було розроблено макет меблевої фабрики «Прогрес» з функціями відеонагляду та пожежної сигналізації як прототип реальної системи, яку можна реалізувати на виробництві. Цей макет демонструє принципи побудови IoT-системи, яка включає датчики для виявлення пожежі, систему автоматичного пожежогасіння, а також камери відеоспостереження. Усі компоненти з'єднані через мережеву інфраструктуру Cisco, що дозволяє централізовано моніторити стан системи, отримувати сповіщення про аварійні ситуації та швидко реагувати на події.

Для системи обрано маршрутизатор DLC100 (Home Gateway), який підтримує IoT-сервер. Він забезпечує управління «розумними» пристроями та доступ до веб-інтерфейсу системи протипожежної безпеки.

Обрані та налаштовані пристрої IoT системи протипожежної безпеки фірми «Megamart» підключено до WiFi-мережі, створеної маршрутизатором DLC100. Для кожного пристрою виконано такі налаштування:

– вказано SSID (FireSmoky);
– обрано метод автентифікації WPA2-PSK AES;
– зазначено ключ автентифікації (Kopytko12323m);
– встановлено отримання IP-адреси через DHCP;
– вказано IoT-сервер як точку зв'язку.

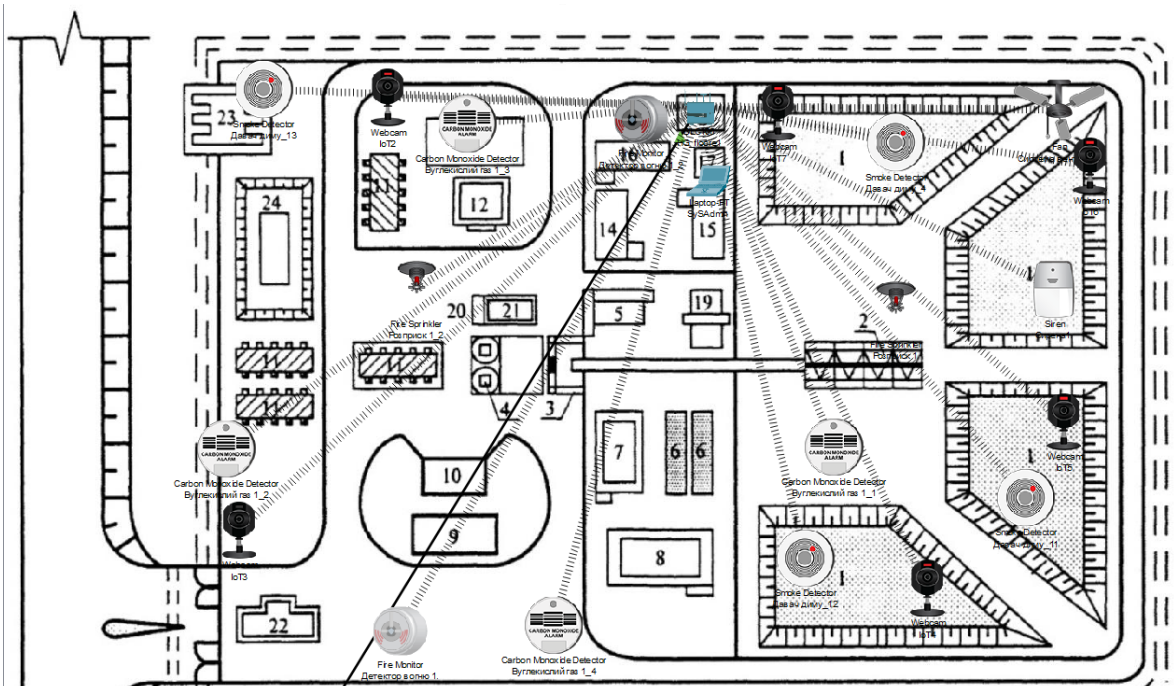

Рисунок 3.4 – Мережева топологія компонентів IoT

Алгоритми функціонування системи задаються через веб-інтерфейс IoT-сервера у вигляді сценаріїв. Система реагує на сигнали від датчиків.

Датчик диму спрацьовує при рівні диму у повітрі ≥ 40% та активує систему вентиляції та сирену (рис.3.5 та рис.3.7).

Датчик вуглекислого газу реагує на концентрацію CO у повітрі ≥ 20% та активує систему вентиляції та сирену (рис.3.6).

Датчик вогню фіксує полум'я за рівнем властивості «IK» у встановленому діапазоні; увімкнення розпилювачів води та сирени.

```
from gpio import *
from time import *
from ioeclient import *
from physical import *
import math
from environment import *

ENVIRONMENT_NAME = "Smoke"

state = 0
level = 0
ALARM_LEVEL = 40

def main():
    setup()
    while True:
        loop()

def setup():
    IoEClient.setup({
        "type": "Smoke Detector",
        "states": [{
            "name": "Alarm",
            "type": "bool",
            "controllable": False
        },
        {
            "name": "Level",
            "type": "number",
            "controllable": False
        }]
    })

    restoreProperty("Alarm Level", 40)
    IoEClient.onInputReceive(onInputReceiveDone)
    add_event_detect(0, detect)

    state = restoreProperty("state", 0)
    setState(state)

def onInputReceiveDone(data):
    processData(data, True)

def detect():
    processData(customRead(0), False)

def restoreProperty(propertyName, defaultValue):
    value = getDeviceProperty(getName(), propertyName)
    if  not (value is "" or value is None):
        if  type(defaultValue) is int :
            value = int(value)

        setDeviceProperty(getName(), propertyName, value)
        return value
```

Рисунок 3.5 – Фрагмент коду налаштування датчику диму

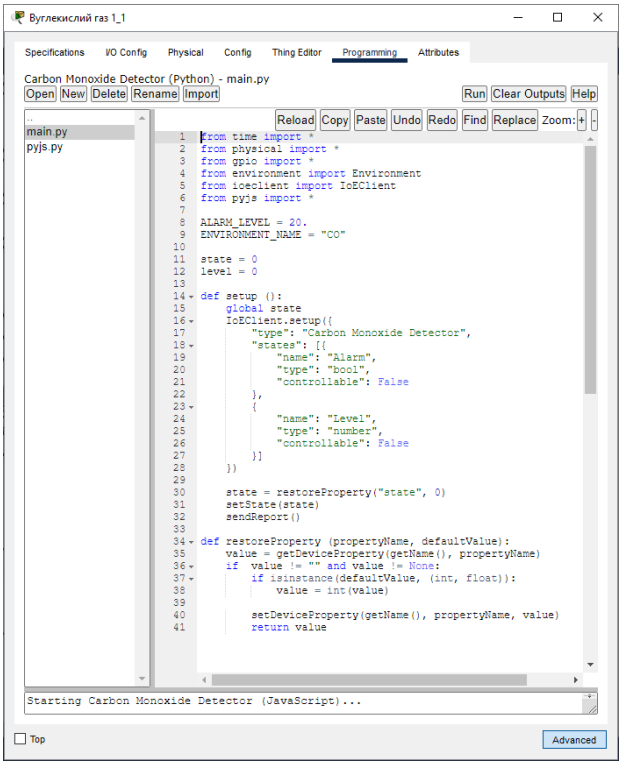

Рисунок 3.5 – Фрагмент коду налаштування датчику вуглекислого газу

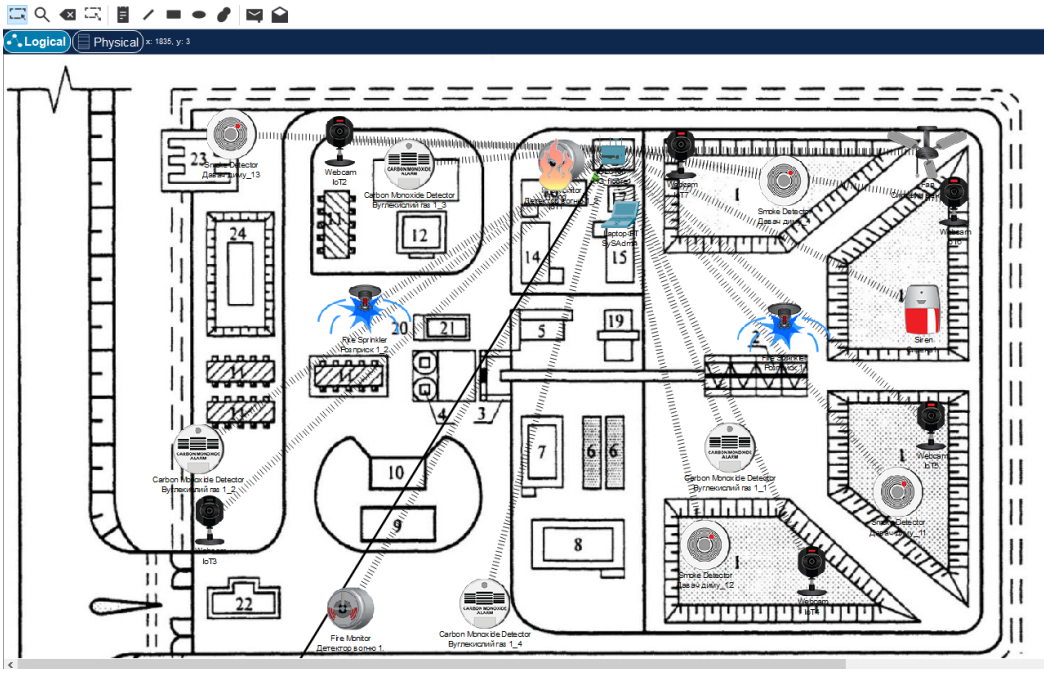

Рисунок 3.7 – Результат сценарію роботи систему під час пожежі

Для забезпечення стабільної та безпечної роботи мережі було виконано її базове налаштування. Спочатку налаштовано паролі для захисту доступу до налаштувань обладнання та встановлено надійні паролі для автентифікації

доступу до бази даних. Для оптимізації маршрутизації в мережі застосовано динамічний маршрутизаційний протокол EIGRP, який дозволяє автоматично визначати та оновлювати маршрути. Використано статичні або динамічні VLAN для управління трафіком і підвищення ефективності мережі, а також призначено IP-адреси на інтерфейсах кожної підмережі та для керованих інтерфейсів обладнання.

Було налаштовано статичну або динамічну IP-адресацію залежно від потреб пристроїв, а також впроваджено фільтрацію пакетів та правила безпеки для захисту трафіку. Для бази даних застосовано механізми автентифікації та авторизації, що забезпечують додатковий рівень безпеки. Конфігурація DHCP дозволила автоматично присвоювати IP-адреси пристроям мережі та передавати інші параметри конфігурації, такі як шлюз за замовчуванням і DNS-сервери.

Окрім цього, було налаштовано системи моніторингу стану мережі та журналювання подій для аналізу змін і забезпечення безпеки. Усі ці дії спрямовані на оптимізацію продуктивності, спрощення управління та підвищення рівня захисту мережі (рис.3.8).

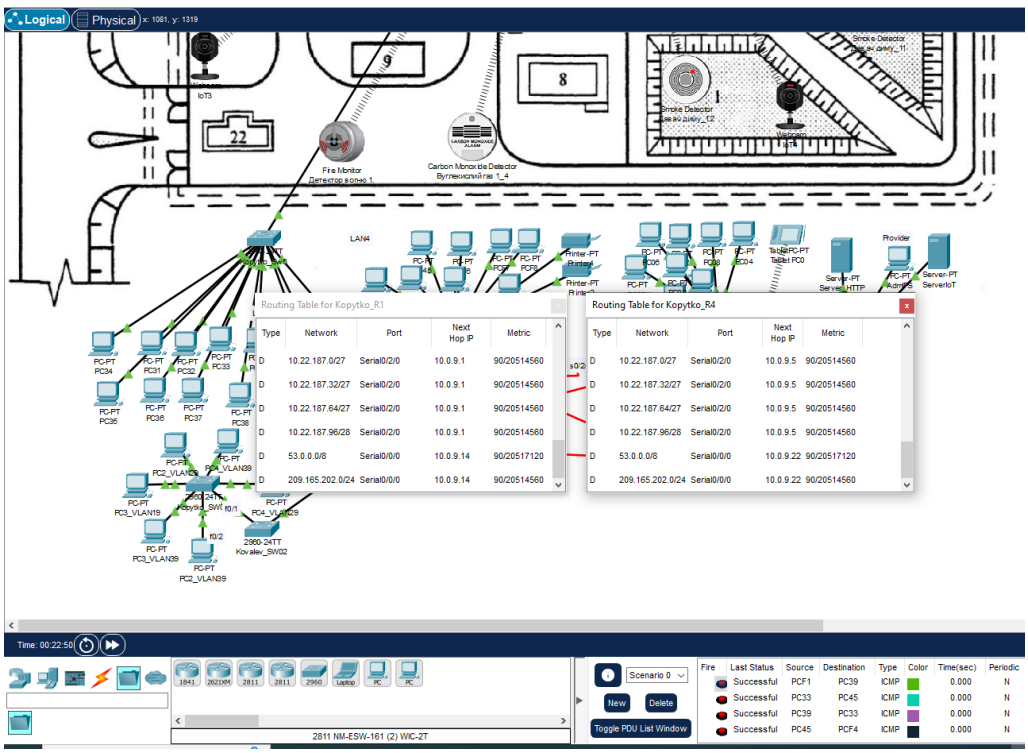

Рисунок 3.8 – Тестування працездатності мережі

3.4 Висновки до розділу

У розділі проведено комплексний аналіз і реалізацію ключових етапів розробки системи відеонагляду та пожежної сигналізації меблевої фабрики «Прогрес», що ґрунтується на сучасних технологіях IoT.

Розроблено функціональну схему структури системи, яка забезпечує ієрархічний підхід до управління елементами відеонагляду та пожежної сигналізації. Функціональна структура системи враховує зв’язок між компонентами, що дозволяє забезпечити інтеграцію обладнання, серверів і мережних шлюзів.

Обґрунтовано вибір елементної апаратної бази системи. Проведено аналіз технічних характеристик і можливостей обладнання, що дозволило визначити оптимальні пристрої для реалізації запропонованої системи. Зокрема, обрано мережеві шлюзи, маршрутизатори, датчики диму, вогню та оприскувачі, які забезпечують безперебійну роботу системи.

Описано процес розробки та налаштування обладнання і сервісів системи IoT. Налаштовано мережеві шлюзи, конфігуровано пристрої IoT, а також реалізовано алгоритми взаємодії компонентів системи. Впроваджено сценарії роботи системи, які забезпечують автоматичну реакцію на спрацювання датчиків вогню, диму та вуглекислого газу.

РОЗДІЛ 4
РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ВІДЕОНАГЛЯДУ ТА ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ

4.1 Призначення й область застосування програмного забезпечення

Програмне забезпечення призначене для надання користувачам можливості ефективно працювати з відео даними, зокрема для здійснення потокового відео з камер в реальному часі, запису відео та збереження його в хмарі. Це рішення забезпечує інтеграцію з системами аутентифікації, дозволяючи керувати доступом до відео за допомогою ролей користувачів (адміністратор, користувач). Програмне забезпечення також підтримує зберігання метаданих про відеофайли, а також надає можливість переглядати відео в реальному часі через веб-браузер.

Основні функції:

– програмне забезпечення дозволяє отримувати відеопотік з камери користувача та транслювати його в браузер через веб-сервер. Це забезпечує перегляд відео в реальному часі без необхідності використання додаткових плагінів;

– програма дозволяє записувати відео з камери на сервер або в хмару для подальшого використання або зберігання;

– записані відео зберігаються у хмарному сховищі, що дозволяє економити локальні ресурси сервера, забезпечує масштабованість і доступність файлів з будь-якої точки світу;

– користувачі мають змогу входити в систему через аутентифікацію за допомогою логіну та пароля, а також мають різні ролі (адміністратор або користувач), що дозволяє контролювати доступ до функцій і відео;

– користувачі можуть переглядати відео в реальному часі за допомогою інтуїтивно зрозумілого веб-інтерфейсу, що підтримує доступ до відеопотоку через HTTP протокол;

– програмне забезпечення дозволяє зберігати метадані (наприклад, URL відео в хмарному сховищі) в базі даних для подальшого доступу або аналізу.

4.2 Розробка інтерфейсу користувача

Інтерфейс користувача (UI) є важливою складовою програмного забезпечення, оскільки забезпечує взаємодію користувача з системою. Правильно спроектований інтерфейс дозволяє користувачам ефективно та інтуїтивно працювати з функціоналом програми, спрощує виконання завдань і підвищує загальну задоволеність користувачів.

У рамках нашої програми інтерфейс складається з кількох основних екранів, кожен з яких виконує свою функцію.

На головній сторінці користувачі повинні мати можливість увійти в систему за допомогою логіна та пароля. Візуально ця сторінка має бути лаконічною, з полями для введення даних і кнопкою "Увійти". Якщо дані введені неправильно, система повинна повідомляти про помилку. Для зручності користувача має бути кнопка для відновлення пароля (рис.4.1).

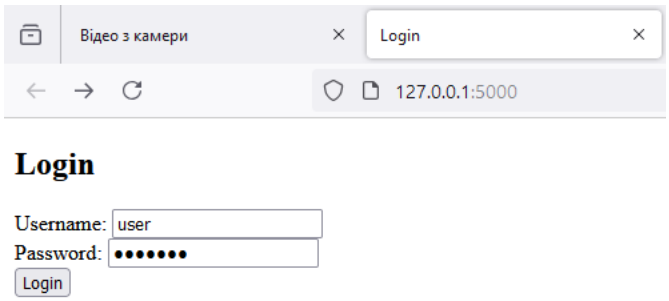

Рисунок 4.1 – Головна сторінка

Сторінка авторизації відображається після введення правильних даних для входу. Залежно від ролі користувача (адміністратор або користувач), система перенаправляє на відповідний інтерфейс. Адміністратор має доступ до всіх функцій програми, включаючи перегляд відео, керування записами,

управління користувачами. Користувач має доступ до перегляду відео в реальному часі, записів відео та історії переглядів.

Перегляд відео в реальному часі відображається відеопотік із камери. Користувач може переглядати відео в реальному часі через потокове передавання.

Для адміністраторів передбачений окремий інтерфейс для управління користувачами та перегляду метаданих записаних відео (рис.4.2). Адміністратор може переглядати інформацію про кожен відеофайл, видаляти старі записи, управляти правами доступу користувачів.

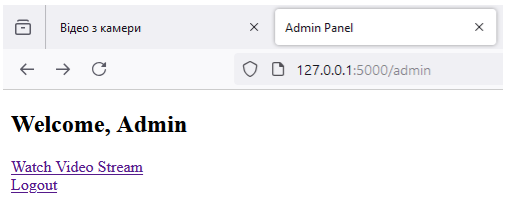

Рисунок 4.2 – Панель адміністратора

4.2.1 Технічні аспекти реалізації інтерфейсу

Для розробки інтерфейсу користувача використовуються стандартні веб-технології, такі як HTML для розмітки та CSS для стилізації сторінок. Це дозволяє створити сучасний та адаптивний інтерфейс.

Для забезпечення динамічних елементів, таких як відеопотік в реальному часі, застосовується JavaScript. Він дозволяє забезпечити безперервну передачу відео без перезавантаження сторінки за допомогою механізму "streaming".

Для спрощення розробки інтерфейсу використовується система шаблонів Jinja2, яка дозволяє генерувати HTML-код на сервері на основі даних, що надходять від користувача чи з бази даних.

Інтерфейс розробляється з урахуванням мобільних пристроїв. Використовуються адаптивні дизайни та медіа-запити CSS, щоб програма

коректно відображалась на різних типах екрану (телефони, планшети, ноутбуки).

Усі користувачі програми проходять аутентифікацію через систему входу за логіном та паролем. Додатково для безпеки передбачено механізм авторизації для доступу до різних частин інтерфейсу в залежності від ролі користувача (адміністратор чи звичайний користувач).

Для забезпечення безпеки передавання даних між користувачем і сервером використовується шифрування за допомогою SSL (Secure Sockets Layer). Це дозволяє захистити персональні дані користувачів та відео-потік від несанкціонованого доступу.

Всі записані відеофайли зберігаються у хмарному сховищі з належним рівнем захисту. Також у базі даних зберігаються тільки метадані, а самі відеофайли доступні лише авторизованим користувачам.

4.3 Розробка серверної частини

Серверна частина програми була розроблена за допомогою мови програмування Python [23] та фреймворка Flask [24] для реалізації веб-додатку, що підтримує потокову передачу відео та взаємодію з клієнтським інтерфейсом. Основним завданням серверної частини є забезпечення отримання та передачі відеопотоку, а також його обробка для подальшої класифікації або аналізу.

Серверна частина була розроблена як прототип для потокової передачі відео. Вона дозволяє користувачам переглядати відео в реальному часі через веб-браузер, отримуючи дані від серверу через сокети. Це є базовою архітектурною частиною програми, яку можна вдосконалювати та адаптувати для реалізації класифікаційної роботи, де на сервері можуть проводитись різноманітні обробки відео, наприклад, виявлення об'єктів або класифікація кадрів.

Прототип серверної частини включає в себе наступні компоненти:

– за допомогою фреймворка Flask реалізовано веб-сервер, який обробляє запити від клієнтів. Flask надає легкий механізм для створення веб-додатків і інтеграції з іншими бібліотеками, що дозволяє зручно працювати з відео та іншими мультимедійними даними;

– для обміну даними між сервером та клієнтом використовується сокет. Сервер приймає відеофрейми від клієнта через мережу за допомогою сокет-з'єднання. Використовується бінарний формат для передачі кадрів через сокет, що дозволяє знизити затримки та забезпечити швидку передачу;

– кожен кадр відеопотоку десеріалізується з використанням бібліотеки pickle, після чого перетворюється в формат JPEG для подальшої передачі через HTTP-протокол до клієнта. Завдяки цьому забезпечується можливість перегляду відео в реальному часі через веб-браузер;

– відеофрейми відправляються клієнту за допомогою формату multipart/x-mixed-replace, що дозволяє клієнтському браузеру отримувати кадри по мірі їх надходження, забезпечуючи безперервний перегляд відео.

4.4 Опис логічної частини програми

Алгоритм обробки запитів клієнта від відео камери починається з перевірки доступності камери (рис.4.3). Спочатку сервер перевіряє, чи підключена камера до системи і чи працює вона коректно. Якщо камера недоступна або не функціонує, процес обробки запиту припиняється, і користувач отримує відповідне повідомлення про помилку. У разі, коли камера працює нормально, сервер переходить до перевірки підключення клієнта.

Наступним етапом сервер перевіряє, чи є активний клієнт, який здійснив запит на відеопотік. Якщо клієнт не підключений або його сесія закрита, сервер припиняє виконання запиту. Якщо клієнт підключений, сервер ініціалізує з'єднання з ним через HTTP.

Після цього сервер починає захоплення кадрів з відеокамери. Якщо камера не може надавати кадри або виникає інша помилка при захопленні, сервер припиняє передачу відео і виводить повідомлення про помилку. Якщо кадри успішно отримано, сервер перетворює їх на формат JPEG для подальшої передачі через HTTP.

Рисунок 4.3 – Алгоритм обробки запитів клієнта від відео камери

Далі сервер передає кожен кадр клієнту у вигляді потоку. Кожен кадр передається по черзі через HTTP, і це триває до тих пір, поки клієнт залишається підключеним. Під час трансляції сервер постійно перевіряє, чи

клієнт ще підключений. Якщо клієнт відключається або з'єднання з ним переривається, сервер припиняє передачу відео.

У разі успішного завершення трансляції або при виникненні помилки, сервер завершує процес, закриваючи з'єднання з клієнтом і зупиняючи захоплення відео з камери. Алгоритм завершується після того, як всі з'єднання закрито, і відеопотік більше не передається.

Алгоритм пошуку пожежі на відео представлено на рис.4.4 і починається з отримання послідовності зображень, що представляють відеокадри, які потрібно аналізувати. На першому етапі здійснюється сегментація рухомих областей шляхом різниці зображень. Цей процес дозволяє виділити області, що змінюються між послідовними кадрами, і визначити потенційно небезпечні зони руху.

Після цього виконується виділення пікселів вогню та диму за допомогою хроматичних ознак. Цей крок передбачає аналіз кольорів на зображеннях для визначення областей, які можуть відповідати вогню чи диму. Для цього використовуються специфічні характеристики кольорів, характерні для горіння та задимлення.

Наступним етапом є перевірка, чи є виявлена область справжнім вогнем. Для цього використовуються динамічні ознаки, які дозволяють оцінити рух і поведінку пікселів у відеопотоці. Якщо аналіз показує, що виявлені області не відповідають критеріям справжнього вогню, алгоритм повертається до обробки нових кадрів. Якщо ж область визначена як справжній вогонь, процес переходить до наступного етапу.

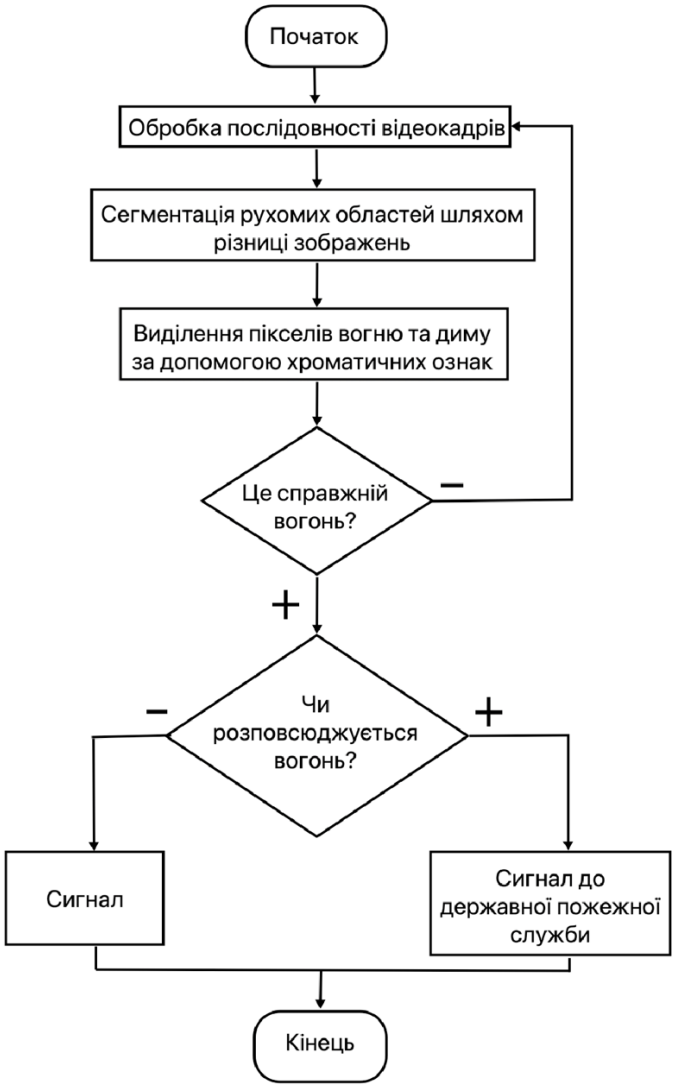

Рисунок 4.4 – Алгоритм пошуку пожежі на відео

Далі алгоритм аналізує, чи є ризик розповсюдження вогню. Це важливий крок для розуміння, чи буде ситуація ставати небезпечнішою. Якщо виявлено, що вогонь не розповсюджуватиметься, сигналізується про відсутність загрози, і процес знову переходить до аналізу наступних кадрів. Якщо ж є ознаки можливого поширення вогню, відправляється сигнал про пожежу, і пожежа вважається виявленою.

4.5 Вхідні та вихідні дані

Вхідними даними для алгоритму є послідовність відеокадрів, яка представляє безперервний відео потік (рис.4.5). Цей потік може бути отриманий через API за наступними адресами:

– http://127.0.0.1:5000/user: використовується для підключення камер спостереження, що передають відеопотік для обробки. Це забезпечує моніторинг подій у реальному часі для звичайних користувачів.

– http://127.0.0.1:5000/admin: використовується адміністративними пристроями для доступу до додаткових функцій, таких як перегляд історії записів.

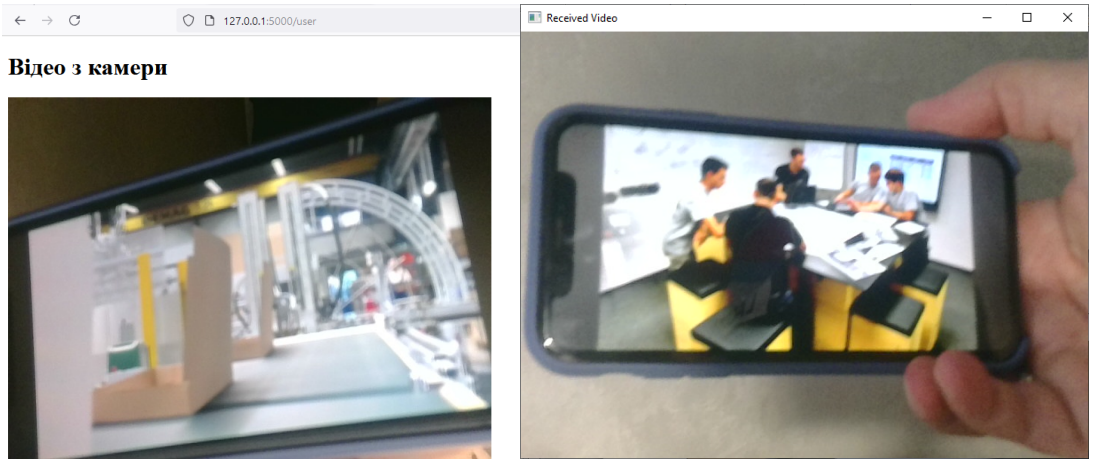

Рисунок 4.5 – Приклад роботи ПЗ з послідовністю відеокадрів

Вихідними даними є результат роботи алгоритму є визначення наявності чи відсутності пожежі, а також можливості її поширення. У разі підтвердження справжнього вогню та виявлення ризику його розповсюдження алгоритм видає сигнал тривоги про виявлену пожежу. Вихідні дані можуть включати повідомлення про пожежу, координати або зображення з маркованими областями, де було виявлено вогонь і дим. Також можливе виведення детальної інформації про характеристики вогню та його динаміку, що дозволяє приймати своєчасні заходи для боротьби з пожежею (рис.4.6).

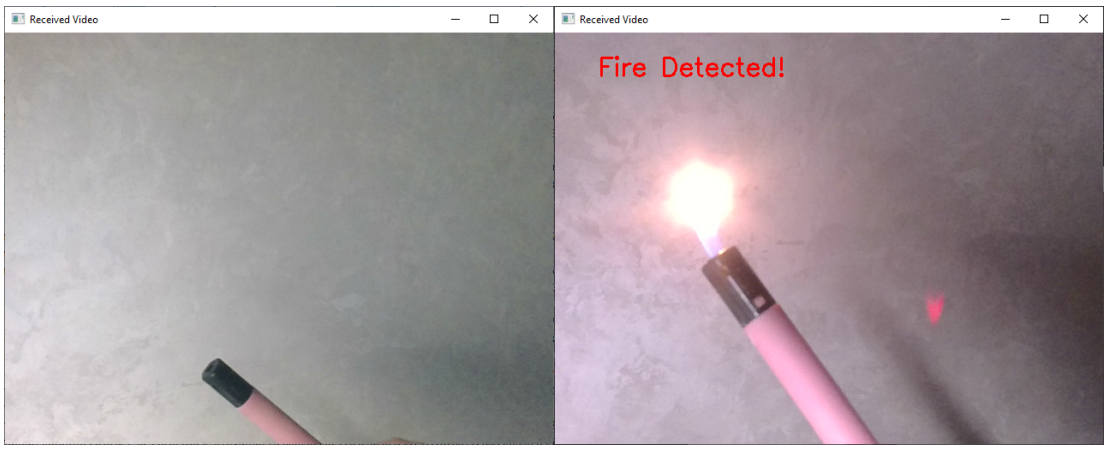

Рисунок 4.6 – Результат пошуку пожежі на відео

Лог клієнтської частини ілюструє основні дії системи (рис.4.7) – обробка запитів GET і POST для доступу до функцій моніторингу (/user) або адміністративних функцій (/admin). Відповіді з відеопотоком (/video_feed), який обробляється в реальному часі. Режим налагодження (debug), що дозволяє відстежувати процеси в роботі системи.

```
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with watchdog (windowsapi)
 * Debugger is active!
 * Debugger PIN: 114-655-412
127.0.0.1 - - [15/Nov/2024 20:03:54] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [15/Nov/2024 20:04:04] "POST /login HTTP/1.1" 302 -
127.0.0.1 - - [15/Nov/2024 20:04:04] "GET /user HTTP/1.1" 200 -
127.0.0.1 - - [15/Nov/2024 20:04:14] "GET /video_feed HTTP/1.1" 200 -
127.0.0.1 - - [15/Nov/2024 20:04:35] "POST /login HTTP/1.1" 302 -
127.0.0.1 - - [15/Nov/2024 20:04:35] "GET /admin HTTP/1.1" 200 -
```

Рисунок 4.5 – Лог клієнтської частини

4.6 Висновки до розділу

Розроблене програмне забезпечення забезпечує автоматичний аналіз відеопотоку для виявлення пожеж у реальному часі. Реалізовано клієнтський і адміністративний інтерфейси, які забезпечують зручність використання та управління системою. Серверна частина відповідає за обробку відеопотоку, виконання алгоритмів класифікації та передачу результатів. Вхідні дані — це відеопотік і запити користувачів, вихідні — марковані зображення,

координати зон пожежі та оповіщення про небезпеку. Розробка інтегрує сучасні методи аналізу відео, забезпечуючи ефективність і надійність системи.

РОЗДІЛ 5
ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

5.1 Формування вимог до експерименту для розроблення алгоритму виявлення пожежі

Для впевненості в ефективності та адекватності розробленого алгоритму виявлення пожежі, необхідно провести систематичний експеримент, спрямований на перевірку заданих вимог і функціональності системи. Основна мета експерименту полягає в оцінці точності, швидкодії та стійкості алгоритму до різних умов експлуатації.

Експеримент спрямований на перевірку кількох ключових аспектів роботи системи. Перш за все, необхідно оцінити точність виявлення пожежі (Accuracy). Алгоритм повинен правильно класифікувати кадри як "пожежа" або "без пожежі" з точністю не меншою за 90%. Це є критичним показником, який гарантує надійність системи та її ефективність у реальних умовах.

Другим важливим параметром є швидкість обробки одного кадру. Для забезпечення роботи в реальному часі час обробки одного кадру відеопотоку має бути меншим за 200 мс. Це дозволить алгоритму швидко реагувати на зміну ситуації та оперативно передавати сигнал тривоги у разі виявлення пожежі.

Окремо необхідно перевірити стійкість алгоритму до змін умов експлуатації. Система повинна демонструвати коректну роботу при зміні освітлення (денне світло, сутінки, нічні умови), у випадках задимленості, що може ускладнювати розпізнавання полум'я, а також при різних ракурсах камер, які можуть впливати на вигляд пожежі в кадрі.

Таким чином, проведення експерименту дозволить перевірити відповідність системи її призначенню та оцінити її ефективність в умовах, наближених до реального використання.

5.2 Метрики для оцінки алгоритму експерименту

Експеримент проводився на тестовому наборі відеоданих, що включає два основні типи відео:

– відео із симуляцією пожежі, що містять такі елементи, як полум’я та дим. Це відео відображає реалістичні умови, при яких алгоритм має виявляти ознаки пожежі;

– відео без ознак пожежі, що складає контрольний набір даних. Це відео служить для перевірки точності алгоритму в умовах відсутності пожежі, дозволяючи оцінити рівень помилкових спрацьовувань алгоритму.

Для оцінки роботи алгоритму було використано такі метрики: Accuracy, Precision, Recall та F1-міра [21, 22].

Точність (Accuracy) – загальна ефективність алгоритму, що визначається як співвідношення правильних прогнозів до загальної кількості тестових прикладів. Це дає загальне уявлення про те, як часто алгоритм правильно класифікує відео.

Прецизійність (Precision) – метрика, яка оцінює, скільки з виявлених алгоритмом випадків пожежі є насправді пожежами. Висока прецизійність означає, що алгоритм рідко помилково виявляє пожежу в тих відео, де її немає.

Повнота (Recall) – визначає, яку частину всіх відео з реальною пожежою алгоритм зміг правильно виявити. Висока повнота свідчить про здатність алгоритму не пропускати випадки пожежі.

F1-міра – комбінована метрика, що поєднує прецизійність і повноту, надаючи баланс між ними. Вона особливо корисна в умовах, коли потрібно знайти оптимальний компроміс між кількістю пропущених випадків та кількістю помилкових спрацьовувань.

Час виконання – час, необхідний для обробки кожного відеофрагмента, що є важливим аспектом для оцінки ефективності алгоритму в реальному часі, особливо для застосувань, де швидкість є критично важливою.

Ці метрики були використані для комплексної оцінки точності та ефективності алгоритму в реальних умовах, де необхідно вчасно і точно виявляти пожежі на відео.

5.3 Проведення експерименту за допомогою тестового набору відеоданих

В даному експерименті використовувалось 90 відеокадрів. Алгоритм показав непогані результати на тестовому наборі відеоданих (табл. 5.1). Точність (Accuracy) склала 92.5%, що перевищує заданий поріг для ефективного виявлення пожежі. Це означає, що алгоритм здатен правильно класифікувати більшість відеофрагментів, що свідчить про його високу загальну ефективність.

Таблиця 5.1 – Результати експерименту

Метрика	**Значення**
Accuracy	82.5%
Recall	80.3%
Precision	84.1%
F1-міра	82.1%
False Positive Rate	23.8%
Середній час обробки	285 мс

Прецизійність на рівні 84.1% вказує на те, що з усіх випадків, де алгоритм визначав пожежу, більшість з них є справжніми. Це означає, що алгоритм рідко помилково визначає пожежу, коли її немає, що є важливим аспектом для зменшення числа хибних тривог.

Повнота на рівні 80.3% означає, що алгоритм виявляє лише 80% справжніх випадків пожеж, пропускаючи близько 20%. Це може бути проблемою в реальних умовах, де кожен пропущений випадок може мати серйозні наслідки. Алгоритм не охоплює всі пожежі, що знижує його ефективність в критичних ситуаціях.

F1-міра, яка становить 82.1%, є хорошим індикатором загальної ефективності алгоритму, оскільки вона поєднує точність і повноту в одну метрику. Високе значення цієї метрики вказує на те, що алгоритм вміє знаходити баланс між точністю та повнотою, хоча є деякі недоліки в обох аспектах.

False Positive Rate (FPR) на рівні 23.8% є значним показником, що вказує на високу кількість хибних спрацьовувань. Це означає, що алгоритм помилково виявляє пожежу в 23.8% випадків, де її немає. Такий високий рівень хибних спрацьовувань може бути проблемою в умовах реального застосування, оскільки постійні помилкові сповіщення можуть призвести до зниження довіри до системи і витрат на необґрунтовані перевірки.

Середній час обробки кожного кадру становить 285 мс. Це значення дещо вище за оптимальне для систем реального часу, де швидкість обробки критична. Хоча час обробки ще в межах прийнятних значень для більшості задач, у ситуаціях, де потрібна обробка відео в реальному часі (наприклад, в автоматичних системах моніторингу пожеж), це може бути занадто повільно, особливо якщо потрібно обробляти відео з високою частотою кадрів.

На рис.5.1 наведено гістограми розподілу часу обробки кадрів та помилок.

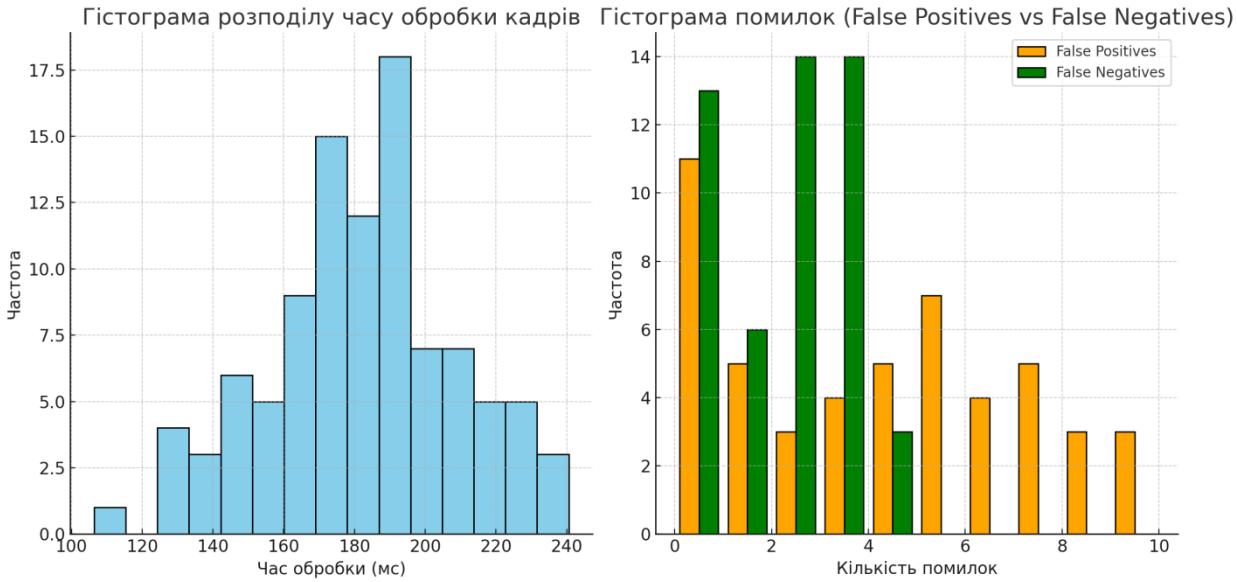

Рисунок 5.1 – Гістограми розподілу часу обробки кадрів та помилок.

Гістограма розподілу часу обробки кадрів показує, як розподіляється час обробки кадрів відеопотоку. Це дозволяє побачити, чи є певні кадри, які займають значно більше часу для обробки (наприклад, "довгі" кадри можуть вказувати на складність сцен або великий обсяг даних для обробки).

Гістограма помилок порівнює кількість хибних спрацьовувань (false positives) і хибних негативів (false negatives) на різних кадрах. Це дозволяє визначити, де алгоритм схильний до помилок і в яких ситуаціях його точність може бути знижена.

На рис.5.2 наведено графік, що показує кількість виявлених об'єктів (наприклад, полум'я або диму) на одиницю часу. Це дозволяє побачити, чи є якісь часи або періоди, коли виявлення стає більш чи менш точним. Дані мають чітку часову структуру, що показує регулярні інтервали між подіями. Між більшістю подій є інтервал у 15 хвилин, за винятком першої пари подій (08:00 і 08:05), що може свідчити про налаштування системи або тестування в першому випадку. Це вказує на те, що система працює з певною періодичністю, виконуючи сканування або перевірки через фіксований проміжок часу.

Події чергуються між двома типами: "дим" та "полум'я", що може свідчити про розпізнавання різних етапів однієї й тієї ж ситуації. Наприклад, спочатку система виявляє дим, а потім полум'я. Це може бути нормальною поведінкою системи, де кожен тип події зафіксований окремо, або ж результатом конфігурації датчиків, які фіксують різні аспекти однієї ситуації. Таке чергування дає підстави для виведення припущення, що кожна подія є частиною одного інциденту.

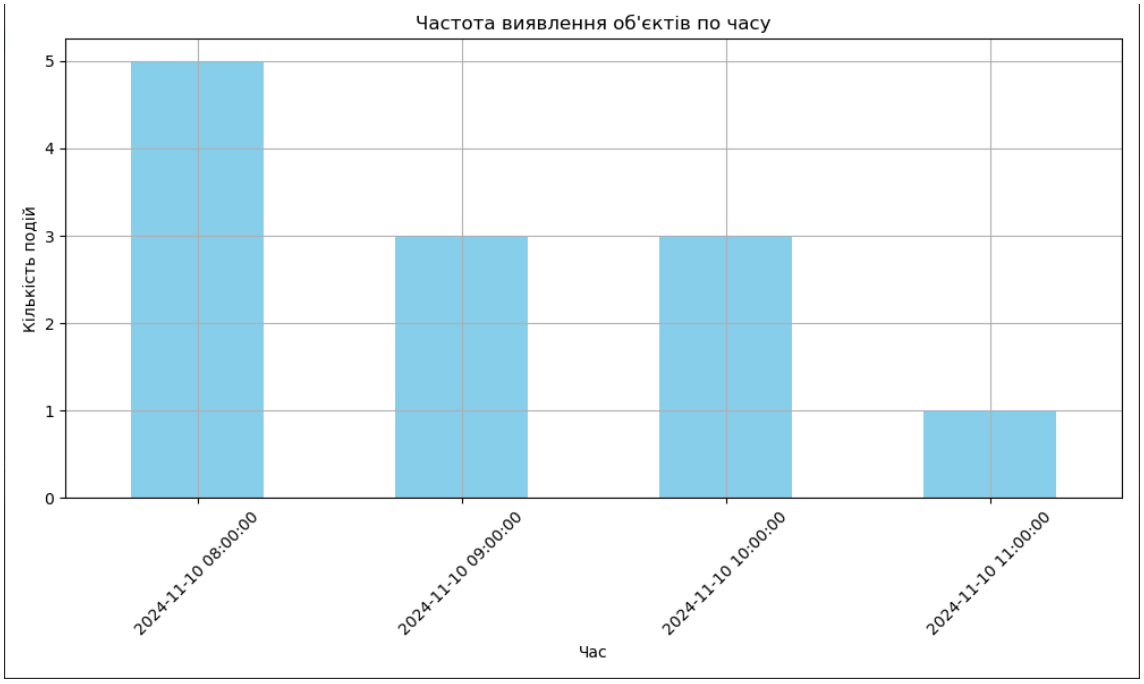

Рисунок 5.2 – Графік виявлення об’єктів по часу

5.4 Характеристика новизни результатів

Алгоритм пошуку пожежі на відео, розроблений в рамках цього дослідження, пропонує новий підхід до автоматичного виявлення та оцінки ризику поширення пожежі на основі відеозаписів. Зокрема, новизна результатів полягає в наступних ключових аспектах, які опишемо нижче.

Інтеграція сегментації рухомих областей та хроматичних ознак: Алгоритм поєднує дві основні методики для ефективного виявлення потенційних загроз — сегментацію рухомих областей через різницю між кадрами та аналіз кольорових ознак для виділення пікселів, що належать до вогню або диму. Це дозволяє не лише виявити зміни на відео, а й уточнити.

Динамічний підхід до визначення "реального" вогню: Замість того, щоб просто покладатися на стаціонарні ознаки (наприклад, колір чи форма), алгоритм включає додатковий крок — перевірку динамічних характеристик вогню. Цей підхід дозволяє відрізняти реальний вогонь від інших подібних явищ, таких як відблиски світла чи інші фальшиві спрацьовування, що можуть бути присутніми в середовищі.

Алгоритм передбачає перевірку на етапі виявлення вогню та диму, після чого проводиться перевірка на поширення. Це дозволяє економно використовувати обчислювальні ресурси, зменшуючи кількість непотрібних операцій та збільшуючи швидкість виявлення. Якщо вогонь не розповсюджується, система не надсилає сигнал тривоги, що дозволяє уникнути фальшивих спрацьовувань.

Оскільки процес пошуку вогню здійснюється через послідовність етапів (від обробки кадрів до визначення поширення вогню), алгоритм має можливість легко масштабуватися та інтегрувати додаткові модулі для поліпшення точності. Це дозволяє адаптувати систему до різних умов роботи, таких як різні типи відеокамер, освітлення або змінні фактори навколишнього середовища.

5.5 Висновки до розділу

У розділі було визначено основні вимоги до експерименту, що включають необхідність точності виявлення пожежних загроз за допомогою відеоаналізу, а також адаптивність алгоритму до різних умов навколишнього середовища. Було розглянуто вимоги до збору даних, якості відеоматеріалів, а також до обчислювальних ресурсів для забезпечення ефективної роботи алгоритму в реальному часі.

Експериментальне дослідження підтвердило працездатність запропонованого алгоритму, який здатний ефективно обробляти відео та виявляти потенційні загрози, такі як вогонь і дим. У ході експерименту було здійснено порівняння результатів роботи алгоритму в різних умовах освітлення.

За результатами експерименту було виявлено, що алгоритм демонструє хорошу точність у виявленні пожежних загроз навіть за умов різних факторів навколишнього середовища, таких як зміни освітлення чи рух об'єктів. Однак для досягнення максимальної ефективності алгоритм потребує певної

налаштування параметрів в залежності від конкретного застосування та характеристик відеопотоку.

ВИСНОВКИ

У кваліфікаційній роботі «Обґрунтування структури та параметрів комп'ютерної системи меблевої фабрики «Прогрес» з функціями відеонагляду та пожежної сигналізації» було розглянуто основні аспекти проектування та впровадження комплексної системи безпеки на підприємстві, що поєднує функції відеонагляду та пожежної сигналізації. Проведене дослідження дозволило досягти поставлених цілей та виконати основні завдання дослідження.

Проведено порівняльний аналіз існуючих систем відеонагляду та пожежної сигналізації, визначено їхні переваги та недоліки. Це дозволило обґрунтувати вибір оптимальних компонентів для розробки інтегрованої системи, враховуючи специфіку роботи меблевої фабрики «Прогрес».

Було визначено структуру та параметри системи, що забезпечують ефективну роботу відеонагляду та пожежної сигналізації. Функціональна схема системи включає зв'язок між відеокамерами, датчиками, серверами та користувацькими пристроями, що забезпечує надійний та швидкий обмін інформацією між усіма компонентами.

У системі використано сучасні методи аналізу відео та алгоритми виявлення пожежних загроз, що демонструють високу точність та адаптивність до різних умов середовища. Проведене моделювання та тестування підтвердили працездатність розробленої системи та її ефективність у виявленні загроз у реальному часі.

Розроблено програмний інструмент, що працює за клієнт-серверною архітектурою, забезпечуючи обробку відеопотоку, аналіз даних від пожежних датчиків та передачу сповіщень про небезпеку. Інтерфейс користувача надає зручний доступ до функцій перегляду відео в реальному часі та архівів, а також управління системою.

Випробування алгоритмів в умовах різних рівнів освітлення та змінних факторів навколишнього середовища показали їхню ефективність у виявленні

потенційних загроз. Система виявилася здатною до адаптації та налаштування для досягнення найвищих показників точності виявлення.

Розроблена система підвищує рівень безпеки меблевої фабрики, забезпечуючи своєчасне реагування на потенційні пожежні загрози та дозволяючи здійснювати комплексний моніторинг території. Це сприяє мінімізації ризиків для персоналу та майна, а також забезпечує безперервний контроль виробничих процесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Dang Ha the Hien. “The Modern History of Object Recognition – Infographic”. Medium, 2017. [Електронний ресурс]: https://medium.com/@nikasa1889/the-modern-history-of-object-recognition-infographicaea18517c318.

2. Imagery Library for Intelligent Detection Systems (i-LIDS) [Електронний ресурс]: https://assets.publishing.service.gov.uk/media/5a7af05040f0b66a2fc03e11/ilids-brochure.pdf

3. B. Cheng, J. Yang, S. Wang, and J. Chen, ‘‘Adaptive video transmission control system based on reinforcement learning approach over heterogeneous networks,’’ IEEE Trans. Autom. Sci. Eng., vol. 12, no. 3, pp. 1104–1113, Jul. 2017.

4. Ericsson AB. Adaptivity and control of resources in embedded systems. [Електронний ресурс]: https://cordis.europa.eu/project/id/216586

5. Cctv camera types: Ip camera vs analog camera. [Електронний ресурс]: http://www.annke.com/blog/2016/09/24/how-to-distinguish-analog-and-ip-security-cameras/.

6. MOBOTIX. Gide. [Електронний ресурс]: https://www.mobotix.com/sites/default/files/202206/mx_TB_en_220629_web_0.pdf

7. Video System Bosh. [Електронний ресурс]: https://software-bosch-video-client.software.informer.com/

8. Video System Hikvision Network Cameras. [Електронний ресурс]: https://www.hikvision.com/europe/products/IP-Products/Network-Cameras/

9. X. Wang, R. Habeeb, X. Ou, S. Amaravadi, J. Hatcliff, M. Mizuno, M. Neilsen, S. R. Rajagopalan, and S. Varadarajan. Enhanced security of building automation systems through microkernel-based controller platforms. In 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), pages 37–44, June 2017.

10. C. Ha, U. Hwang, G. Jeon, J. Cho, and J. Jeong, “Vision-based fire detection algorithm using optical flow”, 2012

11. Compact panel. [Електронний ресурс]: https://www.eaton.com/gb/en-gb/catalog/safety-security-and-emergency-communications/i-on-compact-panel.html

12. IQ8Control Panels IQ8Control C. [Електронний ресурс]: https://www.esser-systems.com/en/products/details/system-iq8control/iq8control-cintelligent-addressable/808003-facp-iq8control-c/

13. Меблева фабрика «Прогрес». [Електронний ресурс]: https://www.mebel-progress.com/uk/

14. R. Xu, Y. Guan, and Y. Huang, ‘‘Multiple human detection and tracking based on head detection for real-time video surveillance,’’ Multimedia Tools Appl., vol. 74, no. 3, pp. 729–742, Feb. 2015

15. Лазарєва І.І. Вулканологія: електронний навч. посібник / І.І. Лазарєва. – Київ, 2015. Електронний ресурс ННІ “Інститут геології”.

16. Miller T.P., Casadevall T.J. Volcanic ash hazards to aviation II Encyclopedia of Volcanoes. Academic Press, San Diego, California. 2000. P. 915-930.

17. Lundgren, P, P. Berardino, M. Coltelli, G, Fornaro, R. Lanari, G. Puglisi, E. Sansosti, andM. Tesauro. Coupled magma chamber inflation and sector collapse slip observed with syntheic aperture radar interferometry on Mt. Etna volcano// J. Geophys. Res., 2003.108(B5), 2247, doi: 10.1029/2001JB000657.

18. Sparks, R.S. J., Aspinall, W.P., Crosweller, H.S., and Hincks, T.K. (2013). Risk and uncertainty assessment of volcanic hazards. Cambridge University Press. 364–397. DOI: 10.1017/CBO9781139047562.012..

19. Brown, S.K., Sparks, R.S.J., Mee, K., Vye-Brown, C., Ilyinskaya, E., Jenkins, S.F., and Loughlin, S.C. (2017). Country and regional profiles of volcanic hazard and risk. Global Volcanic Hazards and Risk. Cambridge University Press, Cambridge.

20. Bateni, S.; Wang, Z.; Zhu, Y.; Hu, Y.; Liu, C. Co-Optimizing Performance and Memory Footprint Via Integrated CPU/GPU Memory Management, an Implementation on Autonomous Driving Platform. In Proceedings of the 2020 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Sydney, Australia, 21–24 April 2020.

21. Zhao, Q.; Sheng, T.; Wang, Y.; Tang, Z.; Chen, Y.; Cai, L.; Ling, H. M2Det: A Single-Shot Object Detector Based on Multi-Level Feature Pyramid Network. In Proceedings of the AAAI Conference on Artificial Intelligence, Honolulu, HI, USA, 27 January–1 February 2019; pp. 9259–9266.

22. Liu, W.; Anguelov, D.; Erhan, D.; Szegedy, C.; Reed, S.; Fu, C.-Y.; Berg, A.C. SSD: Single Shot MultiBox Detector. In Computer Vision—Eccv 2016; Part I; Leibe, B., Matas, J., Sebe, N., Welling, M., Eds.; Springer: Cham, Switzerland, 2016; pp. 21–37.

23.Python. [Електронний ресурс]: https://www.w3schools.com/python/.

24. Flask. [Електронний ресурс]: https://flask.palletsprojects.com/en/stable/.

ДОДАТОК А. ТЕКСТ ПРОГРАМИ

```
import socket
import cv2
import pickle
import struct
from flask import Flask, Response, render_template

# Ініціалізація Flask
app = Flask(__name__)

# Параметри підключення до сервера
host_ip = '127.0.0.1'  # або IP-адреса вашого сервера
port = 9999
socket_address = (host_ip, port)

# Функція для отримання відеопотоку
def video_stream():
    client_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    client_sock.connect(socket_address)
    print(f"Connected to server at {host_ip}:{port}")

    data = b""
    payload_size = struct.calcsize("Q")

    try:
        while True:
            # Отримання даних із сокета
            while len(data) < payload_size:
                packet = client_sock.recv(4 * 1024)  # Отримання пакета
                if not packet:
                    break
                data += packet

            packed_msg_size = data[:payload_size]
            data = data[payload_size:]
            msg_size = struct.unpack("Q", packed_msg_size)[0]

            while len(data) < msg_size:
                data += client_sock.recv(4 * 1024)

            frame_data = data[:msg_size]
            data = data[msg_size:]

            # Десеріалізація відеофрейму
            frame = pickle.loads(frame_data)

            # Перетворення кадру на JPEG
            _, jpeg = cv2.imencode('.jpg', frame)
            frame_bytes = jpeg.tobytes()

            # Відправлення кадру клієнту
            yield (b'--frame\r\n'
                   b'Content-Type: image/jpeg\r\n\r\n' + frame_bytes +
b'\r\n')

    except Exception as e:
        print(f"Error: {e}")
    finally:
        client_sock.close()
```

```
# Головна сторінка
@app.route('/')
def index():
    return render_template('index.html')

# Маршрут для відеопотоку
@app.route('/video_feed')
def video_feed():
    return Response(video_stream(), mimetype='multipart/x-mixed-replace;
boundary=frame')

# Запуск сервера Flask
if __name__ == "__main__":
    app.run(host='0.0.0.0', port=5000, debug=True)
```