ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

на тему: «Система інтелектуального відеоспостережання для забезпечення інформаційної безпеки»

на здобуття освітнього ступеня магістра
зі спеціальності __125 _Кібербезпека та захист інформації»_____
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____Володимир РАЗВАЛЯЄВ

Виконав: здобувач вищої освіти групи СЗДМ 61
РАЗВАЛЯЄВ Володимир_____

Керівник:_____КОТЕНКО Андрій_____
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент:_____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи кіберзахисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Розваляєву Володимиру Анатолійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система інтелектуального відеоспостереження для забезпечення інформаційної безпеки»
керівник кваліфікаційної роботи КОТЕНКО Андрій к.т.н., доцент
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
__Інформаційна безпека на підприємстві.
__Система відеоспостереження для підвіщення рівня інформаційної безпеки.
__Рівень захисту інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.__Дослідження систем відеоспостереження_____
2.__Аналіз складу та можливостей системи відеоспостереження._____
3.__Система відеоспостереження для забезпечення інформаційної безпеки_____

5. Перелік графічного матеріалу: ___Презентаційний матеріал на 14 слайдах_____
_____

6. Дата видачі завдання 20.10.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Володимир РАЗВАЛЯЄВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Андрій КОТЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина бакалаврської (магістерської) кваліфікаційної роботи: 81 стор., 30 рис., 3 табл., 30 джерел.

Об'єкт дослідження – Процес захисту інформації.

Предмет дослідження – Захист інформації на підприємстві

Мета роботи – Підвищити рівень захисту інформації за допомогою системи відеоспостереження.

Методи дослідження – системний аналіз, моделювання, опрацювання літератури за даною темою.

У роботі проаналізовано основні загрози інформаційній безпеці на підприємстві, зокрема через фізичний доступ та недоліки в існуючих системах відеоспостереження. Розглянуто можливість використання інтелектуальних алгоритмів комп'ютерного зору для виявлення, ідентифікації та відстеження потенційних загроз.

На основі проведеного дослідження змодельовано офісну систему відеоспостереження, яка включає в себе IP-камери з функцією розпізнавання облич та інтеграцію з іншими технічними засобами охорони.

Галузь використання – забезпечення інформаційної безпеки на підприємствах, об'єктах інформаційної діяльності, в офісних приміщеннях.

Апробація:

В.А. Развеляєв Захист даних відеоспостереження від несанкціонованого доступу *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.35 - 36.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

ІНФОРМАЦІЙНА БЕЗПЕКА, ВІДЕОСПОСТЕРЕЖЕННЯ, КОМП'ЮТЕРНИЙ ЗІР, IP-КАМЕРА, ФІЛЬТР КАЛМАНА, ІДЕНТИФІКАЦІЯ, ВІДСТЕЖЕННЯ ОБ'ЄКТІВ, АЛГОРИТМ DEEP SORT, ЗАХИСТ ДАНИХ.

ABSTRACT

The text part of the bachelor's (master's) qualification work: 81 pages, 30 figures, 3 tables, 30 sources.

The object of research is the process of information protection.

The subject of the research is information security at an enterprise.

The purpose of the work is to enhance the level of information security through the implementation of a video surveillance system.

Research methods – system analysis, modeling, and review of literature on the topic

The paper analyzes the main threats to information security at an enterprise, particularly those arising from physical access and shortcomings in existing video surveillance systems. The possibility of using intelligent computer vision algorithms for detecting, identifying, and tracking potential threats is considered.

Based on the conducted research, an office video surveillance system was modeled, which includes IP cameras with facial recognition capabilities and integration with other technical security measures.

Field of application – ensuring information security at enterprises, information activity facilities, and office premises.

Approbation:

V.A. Razvalyaev Protection of video surveillance data from unauthorized access All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 03, 2024, Kyiv: RVC DUIKT. – 024. P.35 - 36.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

INFORMATION SECURITY, VIDEO SURVEILLANCE, COMPUTER VISION, IP CAMERA, KALMAN FILTER, IDENTIFICATION, OBJECT TRACKING, DEEP SORT ALGORITHM, DATA PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8
ВСТУП 9
РОЗДІЛ 1. РОЛЬ ВІДЕОСПОСТЕРЕЖЕННЯ У КІБЕРБЕЗПЕЦІ 10
1.1. Інформаційна безпека: визначення, принципи та актуальність 10
1.2 Системи відеоспостереження: призначення, структура та класифікація 12
1.3 Забезпечення ІБ за допомогою відеоспостереження 14
1.4 Проблеми та виклики впровадження систем відеоспостереження 17
1.5 Висновок до першого розділу 19
РОЗДІЛ 2. КОМП'ЮТЕРНИЙ ЗІР ТА ЙОГО РОЛЬ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ 21
2.1 Штучні нейронні мережі та глибоке навчання 25
2.2 Багатошарові перцептрони 29
2.3 Згорткова нейронна мережа 30
2.3.1 Процес згортки 32
2.3.2 Згорткові шари 33
2.4 Алгоритми багатоцільового відстеження 35
2.5 Фільтр Калмана 38
2.6 Угорський алгоритм 44
2.7 Автоматизовані системи відеоспостереження 46
2.8 Модель взаємодії людини і об'єкта з точки зору ІБ 48
2.9 Використання ШІ у системах відеоспостереження 49
2.9.1 Побудова теплових карт 52
2.10 Висновок до другого розділу 54
Розділ 3 РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ З ВИКОРСИСТАННЯМ ШІ 56
3.1 Проектування системи комп'ютерного зору 56
3.2 Функціональні особливості 63
3.3 Результати роботи програми 65

3.4 Аналіз показників роботи алгоритму 67
3.5 Інтеграція комп’ютерного зору в систему відеоспостереження 69
3.6 Створення системи відеоспостереження на підприємстві 72
3.7 Оцінка ефективності системи відеоспостереження 74
3.8 Висновок до третього розділу 76
ВИСНОВОК 77
СПИСОК ДЖЕРЕЛ 79

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформацйна безпека

КСЗІ – комплексна система захисту інформації

СКУД – система контролю і управління доступом

ШІ – штучний інтелект

ШНМ – штучна нейронна мережа

API – Application Programming Interface – Інтерфейс програмування застосунків.

CCTV (Closed-circuit television) – система телебачення замкнутого контуру/

CNN – Convolutional Neural Networks – згорткова нейронна мережа

Deep SORT – Deep Simple Online and Realtime Tracking – глибоке просте онлайн відстежування у реальному часі

FRCNN – Faster Region-Based CNN – Більш швидка заснована на областях CNN

GPU – Graphics Processing Unit – графічний процесор, відеокарта

MOT – Multi Object Tracking – Відтсежування Багатьох Об’єктів

SSD – Single Shot MultiBox Detector – Система комп’ютерного зору Одиночного детектора MultiBox

YOLO – You Only Look Once – Система комп’ютерного зору «Дивишся лише раз»

ВСТУП

Основне призначення систем відеоспостереження полягає в підвищенні рівня безпеки. Головна функція таких систем — забезпечення нагляду за визначеними об'єктами чи суб'єктами, а також, за потреби, фіксація подій, що відбуваються в зоні спостереження. Візуальний контроль є більш ефективним методом для моніторингу території, оскільки дає можливість розглянути певну ситуацію детально і з різних ракурсів. На сьогодні охоронні системи відіграють значну роль у багатьох сферах діяльності. Важко уявити будь-яку організацію або підприємство без сучасної системи безпеки. Камери відеоспостереження не тільки додають впевненості власникам приватних будинків та магазинів, а й створюють ефект стримування для потенційних злочинців. Якщо ж правопорушення все ж було скоєно, записи з камер можуть сприяти пошуку та затриманню злочинців. Бажання захистити власність і родину спонукає до використання вдосконалених охоронних систем.

РОЗДІЛ 1. РОЛЬ ВІДЕОСПОСТЕРЕЖЕННЯ У КІБЕРБЕЗПЕЦІ

1.1. Інформаційна безпека: визначення, принципи та актуальність

Інформаційна безпека є однією з найважливіших складових загальної безпеки в умовах цифрової трансформації суспільства. Сучасні організації, незалежно від їхньої галузі, активно використовують інформаційні технології для обробки, передачі та зберігання даних. Це зумовлює необхідність забезпечення їхнього захисту від потенційних загроз.

Інформаційна безпека визначається як стан захищеності інформації та інформаційних систем від несанкціонованого доступу, використання, розголошення, модифікації або знищення. Основні характеристики, які вона забезпечує [1]:

Конфіденційність — гарантія того, що доступ до інформації мають лише уповноважені особи.

Цілісність — забезпечення достовірності та точності інформації.

Доступність — можливість доступу до інформації для уповноважених осіб у потрібний момент часу.

Рис. 1.1 – Властивості інформації

Інформаційна безпека має критичне значення для організацій, оскільки порушення захисту даних може призвести до фінансових втрат, репутаційних ризиків і порушення законодавства. Особливо це стосується сфер, пов’язаних із роботою з персональними, фінансовими чи державними даними.

Сучасний інформаційний простір стикається з численними загрозами, які можна поділити на:

- Технічні: атаки на мережі, впровадження шкідливого програмного забезпечення, використання вразливостей систем.
- Фізичні: крадіжка обладнання, порушення роботи серверних приміщень.
- Соціальні: інсайдерські загрози, соціальна інженерія, недбалість співробітників.

Для захисту інформаційних активів застосовуються різноманітні технічні та організаційні заходи. Одним із найважливіших інструментів є системи відеоспостереження, які дозволяють:

- Моніторити фізичний доступ до об’єктів.
- Виявляти аномальну поведінку персоналу чи відвідувачів.
- Запобігати вторгненням у захищені зони.
- Актуальність у сучасних умовах

Зростання обсягів цифрових даних, розвиток інтернету речей (IoT) та хмарних обчислень робить забезпечення інформаційної безпеки одним із ключових завдань для бізнесу та держави. У цьому контексті системи відеоспостереження відіграють важливу роль, інтегруючись із іншими технологіями для створення багаторівневого захисту інформації.

Таким чином, інформаційна безпека є основою функціонування сучасних організацій, а її забезпечення потребує комплексного підходу, у якому системи відеоспостереження займають важливе місце.

1.2 Системи відеоспостереження: призначення, структура та класифікація

Системи відеоспостереження є одним із ключових інструментів у забезпеченні безпеки об’єктів, інформації та людей. Їх застосування поширюється на широкий спектр галузей — від охорони громадських місць до корпоративних систем захисту даних [2].

Основна мета систем відеоспостереження — забезпечення візуального моніторингу та реєстрації подій у контрольованій зоні. Завдяки цим системам можна:

- Контролювати доступ до об’єктів.
- Виявляти підозрілі дії або поведінку.
- Фіксувати порушення для подальшого аналізу або використання як доказів.
- Здійснювати проактивний моніторинг, запобігаючи можливим загрозам.

Сучасна система відеоспостереження складається з кількох основних компонентів[3]:

Камери відеоспостереження:

- Відповідальні за зйомку відео. Камери можуть бути аналоговими, цифровими чи IP-камерами.
- Оснащуються функціями нічного бачення, панорамного огляду, автоматичного фокусування тощо.

Системи запису та зберігання даних:

- Сервери або відеореєстратори, які зберігають відеозаписи.
- Хмарні сховища для віддаленого доступу до даних.

Програмне забезпечення:

- Забезпечує обробку, аналіз і виведення відео.
- Містить функції для виявлення об’єктів, розпізнавання облич, аналізу руху тощо.

Моніторингові станції:

- Забезпечують відображення відео для операторів, які здійснюють контроль.
- Мережеве обладнання:

Використовується для передачі даних між камерами, серверами та іншими елементами системи.

Системи відеоспостереження поділяються за кількома критеріями [4]:

За типом передачі даних:

- Аналогові: передають відео у вигляді аналогового сигналу. Простота використання, але обмежена якість зображення.
- Цифрові: використовують цифровий сигнал, що забезпечує високу якість.
- IP-системи: передають дані через мережу, дозволяючи інтеграцію з іншими системами.

За способом зберігання даних:

- Локальні: використовують жорсткі диски або інші локальні сховища.
- Хмарні: дані зберігаються на віддалених серверах, що забезпечує доступність і надійність.

За режимом роботи:

- Реального часу: дозволяють здійснювати моніторинг подій у момент їхнього виникнення.
- Архівні: призначені для перегляду записаного матеріалу.

За рівнем автоматизації:

- Ручні: повністю залежать від дій оператора.
- Автоматизовані: використовують алгоритми для автоматичного виявлення загроз або аномалій.

Розвиток технологій привів до появи інноваційних рішень, таких як:

Штучний інтелект і машинне навчання: використовуються для аналізу відеопотоку, виявлення об’єктів та прогнозування загроз.

Розпізнавання облич і номерних знаків: застосовуються для ідентифікації людей та транспортних засобів.

Хмарні технології: забезпечують віддалений доступ до відео та високу надійність зберігання даних.

Інтеграція з іншими системами безпеки: дозволяє створювати комплексні рішення для захисту об’єктів.

Таким чином, системи відеоспостереження є важливим елементом сучасних технологій безпеки, забезпечуючи надійний контроль та моніторинг. Їх гнучкість, масштабованість і можливість інтеграції з іншими системами роблять їх незамінним інструментом у забезпеченні інформаційної безпеки

Рис. 1.2 – Система відеоспостереження

1.3 Забезпечення ІБ за допомогою відеоспостереження

Системи відеоспостереження (CCTV) займають важливе місце в забезпеченні інформаційної безпеки, оскільки вони поєднують можливості моніторингу фізичних об'єктів, виявлення загроз і створення архівів подій. Завдяки сучасним технологіям відеоспостереження дозволяє не лише відстежувати поточні події, але й здійснювати проактивне виявлення потенційних загроз. У цьому розділі

детально розглядаються основні механізми, за допомогою яких відеоспостереження сприяє зміцненню безпеки інформаційних систем.

Контроль фізичного доступу є важливою складовою інформаційної безпеки, оскільки багато ризиків виникають через несанкціоноване проникнення до зон із обмеженим доступом, таких як серверні кімнати, архіви або робочі станції. Відеоспостереження дозволяє:

- Візуально підтверджувати доступ: Камери, встановлені на входах до захищених зон, фіксують обличчя осіб, які входять чи виходять, дозволяючи перевіряти відповідність їхніх дій встановленим правилам.
- Реєструвати події: Відеозаписи створюють докладний архів усіх дій, який можна використовувати для розслідування інцидентів. Наприклад, якщо був зафіксований несанкціонований доступ, записи допоможуть ідентифікувати порушника.
- Інтегрувати з СКУД: Камери можуть працювати спільно з системами контролю та управління доступом (СКУД), наприклад, записуючи момент використання ідентифікаційної картки чи відбитка пальця.

Особливо важливим є використання камер із функцією розпізнавання облич, яка дозволяє автоматично ідентифікувати осіб і порівнювати їх із базою уповноважених користувачів.

Сучасні системи відеоспостереження оснащені алгоритмами штучного інтелекту та відеоаналітики, які здатні аналізувати поведінку людей і виявляти підозрілі дії. Приклади таких механізмів [5]:

- Виявлення аномальної поведінки: Якщо людина перебуває в зоні спостереження занадто довго або виконує незвичні дії (наприклад, оглядає приміщення, намагається щось приховати), система автоматично надсилає сигнал тривоги.
- Реагування на скупчення людей: У разі раптового зростання кількості людей у зоні спостереження система може сигналізувати про потенційну загрозу (наприклад, спробу несанкціонованого доступу групою).

- Моніторинг персоналу: Відеоспостереження дозволяє контролювати дотримання співробітниками правил безпеки, таких як використання ідентифікаційних карток чи обмеження доступу до певних зон.

Камери відеоспостереження оснащуються датчиками руху, тепловізорами та іншими інструментами, які підвищують ефективність системи. Завдяки цьому можливо [6]:

- Виявляти вторгнення: Якщо в зоні, яка має бути порожньою, з'являється рух, система спрацьовує та надсилає сповіщення відповідальним особам. Це особливо важливо для серверних кімнат або архівів, де присутність сторонніх осіб неприпустима.
- Попереджати крадіжки: У разі спроби несанкціонованого вилучення обладнання або документів відеоспостереження допомагає оперативно виявити та припинити порушення.
- Фіксувати аномалії: Наприклад, теплові камери можуть виявляти зміну температури, пов'язану з роботою обладнання або появою людей у зоні.

Системи відеоспостереження забезпечують довготривале зберігання відеоматеріалів, що є надзвичайно важливим для розслідування інцидентів. Основні можливості включають:

- Створення архіву: Відеозаписи зберігаються у високій якості, що дозволяє переглядати деталі, наприклад, обличчя порушників чи документи, які вони тримали в руках.
- Захист від маніпуляцій: Сучасні системи використовують шифрування та контроль доступу для захисту записів від несанкціонованого видалення чи модифікації.
- Аналітика після подій: Архівні матеріали можуть бути використані для аналізу причин інциденту та впровадження додаткових заходів безпеки.

Системи відеоспостереження з функціями штучного інтелекту дозволяють зменшити навантаження на операторів і підвищити ефективність моніторингу. Завдяки автоматизації:

- Розпізнаються об’єкти та особи: AI-алгоритми ідентифікують людей, транспортні засоби чи предмети, що з’являються в зоні спостереження.
- Фільтруються непотрібні події: Наприклад, система може ігнорувати тварин чи рух листя, зосереджуючись лише на людях або автомобілях.
- Пріоритизуються загрози: Події класифікуються за ступенем ризику, що дозволяє операторам швидше реагувати на серйозні інциденти.

Для досягнення максимальної ефективності системи відеоспостереження часто інтегрують із іншими елементами безпеки, такими як:

- Системи контролю доступу: Камери синхронізуються з електронними замками, які автоматично відкриваються чи блокуються.
- Сигналізація: У разі тривоги відеоспостереження дозволяє перевірити реальність загрози.
- Аналітичні системи: Наприклад, інтелектуальна аналітика може відстежувати ланцюги подій для прогнозування ризиків.

Таким чином, системи відеоспостереження є багатофункціональним інструментом, який забезпечує як превентивні, так і реактивні заходи захисту інформаційних ресурсів. Завдяки поєднанню аналітики, автоматизації та інтеграції з іншими технологіями вони здатні значно підвищити рівень інформаційної безпеки організації.

1.4 Проблеми та виклики впровадження систем відеоспостереження

Незважаючи на безліч переваг, які надають системи відеоспостереження, їх впровадження та ефективне використання стикаються з кількома проблемами та викликами. Зокрема, важливими аспектами є питання захисту даних, забезпечення приватності та обмеження систем, що виникають через специфіку середовища експлуатації [3].

Однією з основних проблем є захист даних, які передаються та зберігаються в системах відеоспостереження. Відео, що фіксує особисту інформацію або

діяльність у зоні спостереження, є чутливими даними, і їх збереження та передача повинні бути належним чином захищені від несанкціонованого доступу. Використання криптографії для шифрування даних є одним із способів мінімізації ризиків. Однак, зберігання великих обсягів відеозаписів також потребує ефективних механізмів зберігання та резервного копіювання, що може бути дорогим і технічно складним.

Інша проблема пов'язана з забезпеченням приватності. Відеоспостереження може суттєво порушити права людей на приватність, особливо в публічних місцях або при спостереженні за працівниками на робочих місцях. Законодавчі ініціативи та політики конфіденційності повинні враховувати баланс між безпекою та правами на конфіденційність. Наприклад, у багатьох країнах використання камер відеоспостереження у громадських місцях регулюється відповідними законами, які визначають межі їхнього використання та обробки даних.

Обмеження систем відеоспостереження виникають через вплив зовнішніх факторів на якість зображення та ефективність роботи системи. Погана освітленість, погана видимість через погодні умови або перешкоди можуть призвести до того, що камери не можуть забезпечити чітке зображення або зафіксувати важливі деталі. Це ставить під загрозу ефективність системи, особливо коли мова йде про захищені об'єкти, де кожен інцидент потребує ретельного аналізу

Крім того, проектування та встановлення систем відеоспостереження вимагає ретельного планування. Необхідно правильно розмістити камери для забезпечення максимального охоплення, але без надмірного перекриття зон. Неправильне розташування камер може призвести до "сліпих зон", де об'єкти залишатимуться непоміченими. Крім того, повинна бути врахована інфраструктура, що підтримує систему, зокрема, енергетичні ресурси та підключення до мережі.

Не менш важливим є питання обмеження людського фактору. Довіряючи системі відеоспостереження, важливо забезпечити належну підготовку персоналу, що працює з системою, а також налаштувати процеси моніторингу та реагування

на події. Оператори повинні бути готові до можливих інцидентів, щоб забезпечити належне реагування на загрози.

Таким чином, попри численні переваги систем відеоспостереження, їх впровадження та ефективне використання потребує вирішення низки технічних, правових та організаційних проблем. Для успішної інтеграції відеоспостереження в комплексну систему безпеки необхідно враховувати всі аспекти, що можуть впливати на ефективність і надійність роботи таких систем [4].

1.5 Висновок до першого розділу

У першому розділі було розглянуто ключові аспекти використання систем відеоспостереження в контексті забезпечення інформаційної безпеки. Було детально проаналізовано принципи інформаційної безпеки, включаючи конфіденційність, цілісність та доступність інформації, а також їх значення у сучасних умовах розвитку технологій.

Відеоспостереження відіграє важливу роль у захисті інформаційних систем, оскільки дозволяє здійснювати моніторинг фізичного доступу до захищених зон, реєструвати події та виявляти потенційні загрози. Особливу увагу приділено інтеграції відеоспостереження з іншими елементами безпеки, такими як системи контролю доступу, сигналізація та аналітичні системи.

Цифрові технології забезпечують високу якість зображення, автоматизацію процесів та гнучкість у використанні, що робить їх ефективним інструментом у забезпеченні кібербезпеки. Крім того, сучасні системи, оснащені штучним інтелектом і алгоритмами відеоаналітики, здатні ідентифікувати об'єкти, аналізувати поведінку людей і автоматично реагувати на загрози. Це значно підвищує ефективність роботи операторів та надійність охорони.

Розглянуто також проблеми, які виникають при впровадженні систем відеоспостереження, зокрема виклики, пов’язані з розташуванням камер, забезпеченням безперервності роботи системи та захистом даних. У зв’язку з цим

підкреслено важливість правильного проектування таких систем, врахування специфіки об’єкта та дотримання вимог щодо конфіденційності.

Таким чином, системи відеоспостереження є важливим інструментом у комплексному забезпеченні інформаційної безпеки. Вони не лише сприяють запобіганню загрозам, але й відіграють ключову роль у розслідуванні інцидентів, забезпечуючи докази для подальшого аналізу. Завдяки поєднанню інноваційних технологій, автоматизації та інтеграції з іншими елементами безпеки, вони мають значний потенціал для подальшого розвитку та застосування у різних сферах.

РОЗДІЛ 2. КОМП’ЮТЕРНИЙ ЗІР ТА ЙОГО РОЛЬ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

Зорова система людини здатна ефективно сприймати навколишній світ, демонструючи високу чутливість до деталей. Наприклад, вона легко відокремлює основний об’єкт від фону, розпізнаючи навіть найдрібніші особливості освітлення та тіні (Рис 2.1) [6].

Рис. 2.1 - Зорова система людини без проблем виділяє об'єкт з навколишнього фону

Розглядаючи фотографію групи людей (Рис. 2.2), людина легко може порахувати точну кількість осіб і навіть зробити висновки про їхній емоційний стан на основі виразів облич. Вчені, які досліджують механізми візуального сприйняття, протягом десятиліть намагаються розкрити принципи функціонування зорової системи. Хоча завдяки використанню оптичних ілюзій вдалося виявити деякі

фундаментальні закономірності, багато питань щодо її роботи залишаються без остаточної відповіді [7].

Рис. 2.2 - Приклад застосування комп'ютерного зору у розпізнаванні облич

Дослідники в галузі комп'ютерного зору паралельно розробляли математичні підходи для розпізнавання і реконструкції тривимірної форми об'єктів на зображеннях. Сьогодні існують високоефективні методи, що дозволяють точно відновлювати часткові 3D-моделі середовища, використовуючи тисячі фотографій із частковим перекриттям. Завдяки великому набору даних можливо створювати детальні та щільні моделі тривимірних поверхонь із застосуванням технології стереопідсилення (Рис. 2.3) [8].

Рис. 2.3 - Стереосистемні алгоритми зіставлення можуть створювати детальну 3D-модель фасаду будівлі

Сучасні алгоритми відстеження руху можуть ефективно фіксувати переміщення окремих людей або навіть цілих груп, забезпечуючи точність навіть за умов складного знімального середовища (Рис 2.4).

Рис 2.4 - Приклад роботи алгоритму відстеження людини, що рухається

Попри значні досягнення, рівень розпізнавання образів і виділення контексту із зображень залишається значно нижчим, ніж здатності дитини дошкільного віку. Основна причина цього полягає у зворотній природі задачі, яка передбачає відновлення відсутньої або прихованої інформації на основі обмежених даних. Для вирішення таких завдань необхідно використовувати фізичні та ймовірнісні моделі, щоб мінімізувати розбіжності між можливими рішеннями. Проте, створення повної моделі візуального світу в реальному часі, яка враховує всі його аспекти, залишається на сьогодні неможливим.

Задачі комп’ютерного зору спрямовані на відтворення прихованої інформації, тобто опис світу, представленого в одному або серії зображень, з метою відновлення таких властивостей, як форма, освітлення, текстура та переходи кольору. Часто ті, хто не працює в цій галузі, недооцінюють складність проблеми. Ця помилка бере свій початок у ранні роки розвитку штучного інтелекту, коли вважалося, що логічні аспекти інтелекту, як-от доведення теорем чи планування, є значно складнішими, ніж перцептивні задачі, такі як бачення. Насправді ж задачі сприйняття виявилися надзвичайно складними через їхню багатогранність і необхідність опрацювання величезного обсягу змінних [9].

Моделювання візуального світу залишається викликом для дослідників, оскільки потрібно врахувати безліч факторів, які впливають на відтворення зображення: фізичні характеристики об’єктів, умови освітлення, динамічні зміни середовища тощо. Навіть із використанням сучасних алгоритмів та технологій розпізнавання, реалізація повноцінної моделі зорового сприйняття є лише частково досяжною, особливо у складних і непередбачуваних умовах.

Комп'ютерне бачення сьогодні широко використовується у різноманітних сферах, забезпечуючи нові можливості автоматизації та підвищення ефективності процесів. До основних напрямів його застосування належать:

-Розпізнавання облич: Використовується для покращення фокусування камер, організації фотографій у галереях, а також для проведення релевантного пошуку за зображеннями.

- Візуальна аутентифікація: Технологія перевірки особистості на основі унікальних рис облич, що застосовується у безпечному доступі до пристроїв чи об’єктів.

- Відстеження руху транспорту: Застосовується для моніторингу дорожнього руху, автоматичного зчитування номерних знаків і оптимізації управління транспортним потоком.

- Оптичне розпізнавання символів (OCR): Використовується для автоматизації зчитування рукописних або друкованих текстів, таких як поштові коди чи реєстраційні знаки транспортних засобів.

- Технічна інспекція: Забезпечує контроль якості деталей, наприклад, шляхом аналізу деформацій крил літальних апаратів за допомогою стереоскопічного зору або пошуку дефектів сталевих деталей із використанням рентгенівського обладнання.

- 3D-моделювання: Використовується для автоматизованої побудови тривимірних моделей об’єктів або територій, наприклад, на основі аерофотознімків.

- Автомобільна безпека: Спрямоване на виявлення непередбачених перешкод, таких як пішоходи, у складних умовах, коли традиційні активні методи, наприклад, радар, можуть не працювати.

-Інтеграція комп’ютерних зображень з реальними відеозаписами (AR): Технологія, яка дозволяє поєднувати комп’ютерну графіку з реальними відеоданими, знаходить застосування у сфері розваг, освіти та промисловості.

Ці приклади демонструють, як комп'ютерне бачення стає невід'ємною частиною багатьох галузей, сприяючи розвитку технологій і підвищенню безпеки та зручності у повсякденному житті [10].

2.1 Штучні нейронні мережі та глибоке навчання

Штучні нейронні мережі (ШНМ), або нейромережі, — це обчислювальні системи, натхненні структурою і функціонуванням біологічних нейронних мереж,

які формують основу роботи мозку тварин. Вони моделюють принципи роботи біологічних нейронів, використовуючи взаємопов’язані вузли, відомі як штучні нейрони або просто нейрони.

Кожен нейрон приймає вхідні сигнали, обробляє їх і передає результат через свої з’єднання, які аналогічні синапсам у біологічному мозку. Вхідні сигнали представлені у вигляді числових значень, а вихід нейрона обчислюється шляхом застосування нелінійної функції до зваженої суми всіх вхідних сигналів. Кожне з'єднання між нейронами має вагу, яка визначає силу впливу сигналу. Ці ваги є ключовими параметрами, що налаштовуються під час навчання мережі, дозволяючи їй адаптуватися до поставлених задач.

Крім того, нейрони можуть мати поріг активації: сигнал передається далі тільки в тому випадку, якщо підсумкове значення вхідного сигналу перевищує цей поріг. Це забезпечує більш гнучке моделювання різноманітних взаємозв’язків [11].

Структурно нейрони організовані в шари:

- Вхідний шар отримує початкові дані.

- Приховані шари виконують проміжні обчислення, здійснюючи складні трансформації даних.

- Вихідний шар формує результат роботи мережі.

На рис. 2.5 можна побачити схему ШНМ

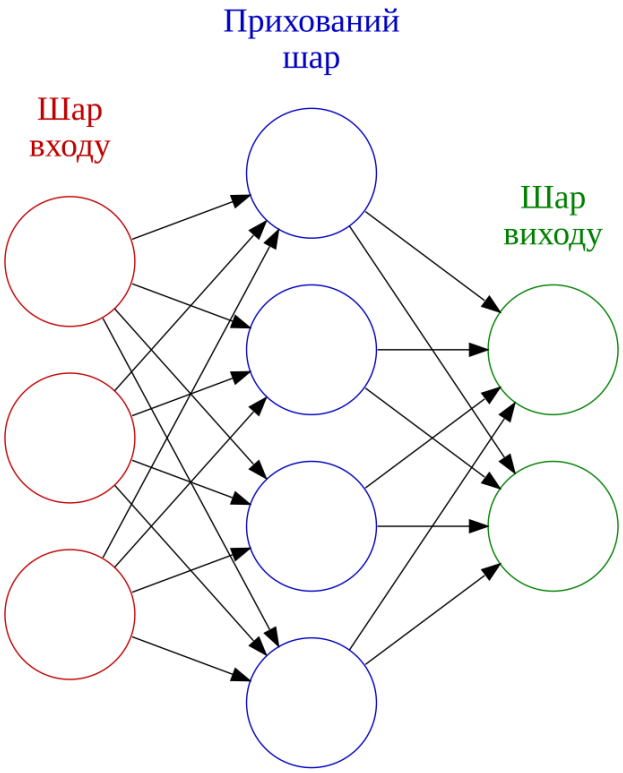


Рис 2.5 Схема нейронної мережі

Сигнали передаються через шари, зазвичай у напрямку від вхідного до вихідного, хоча в деяких архітектурах можливі зворотні зв'язки [12]. Кількість шарів і нейронів, а також спосіб їхньої організації визначають можливості нейронної мережі вирішувати різні завдання, від класифікації до прогнозування та генерації нових даних.

ШНМ стали фундаментом сучасного машинного навчання, особливо у сфері глибокого навчання, де мережі з багатьма шарами (глибинні мережі) використовуються для складних задач, таких як розпізнавання образів, аналіз мови, прогнозування і багато іншого.

Таким чином, кожен нейрон у штучній нейронній мережі є базовим блоком, що моделює обчислювальну функцію. Залежно від параметрів ваг і вибору передавальної функції, мережа може виконувати різноманітні завдання, включаючи класифікацію, розпізнавання образів, прогнозування та багато інших. Нейронні мережі навчаються шляхом обробки набору прикладів, кожен з яких має

відомі значення «входу» та «виходу» [13]. У процесі навчання мережа формує ймовірнісно зважені асоціації між цими входами та виходами, які зберігаються у її внутрішній структурі.

Процес навчання зазвичай відбувається через наступні етапи:

1. Обчислення похибки: Для кожного прикладу обчислюється різниця між реальним виходом мережі (передбаченням) та цільовим виходом (очікуваним результатом). Ця різниця називається похибкою.

2. Підлаштування ваг: На основі похибки мережа змінює значення своїх ваг згідно з певним правилом навчання, таким як алгоритм зворотного поширення помилки (backpropagation). Це дозволяє мережі поступово зменшувати похибку.

3. Повторення: Процес обчислення похибки та підлаштування ваг повторюється для великої кількості прикладів. З часом мережа починає генерувати результати, які дедалі більше відповідають цільовим [14].

4. Завершення навчання: Навчання завершується, коли похибка зменшується до прийнятного рівня або коли мережа досягає визначеного критерію зупинки.

Цей підхід відноситься до керованого навчання, коли мережа отримує доступ до навчального набору даних із заздалегідь позначеними результатами.

Одна з ключових особливостей нейронних мереж — здатність навчатися виконувати складні завдання без програмування чітких правил. Наприклад, у задачах розпізнавання зображень, мережі можуть навчитися ідентифікувати котів, аналізуючи велику кількість прикладів, позначених як «кіт» або «не кіт». Важливо, що нейромережа не отримує жодної інформації про фізичні характеристики котів (наприклад, наявність хутра чи вусів) [15]. Замість цього вона автоматично виявляє ознаки, що дозволяють відрізнити котів від інших об’єктів.

Цей процес дозволяє нейронним мережам створювати потужні моделі для вирішення задач у багатьох сферах, таких як розпізнавання мовлення, аналіз текстів, медична діагностика та автономне керування транспортними засобами [16].

2.2 Багатошарові перцептрони

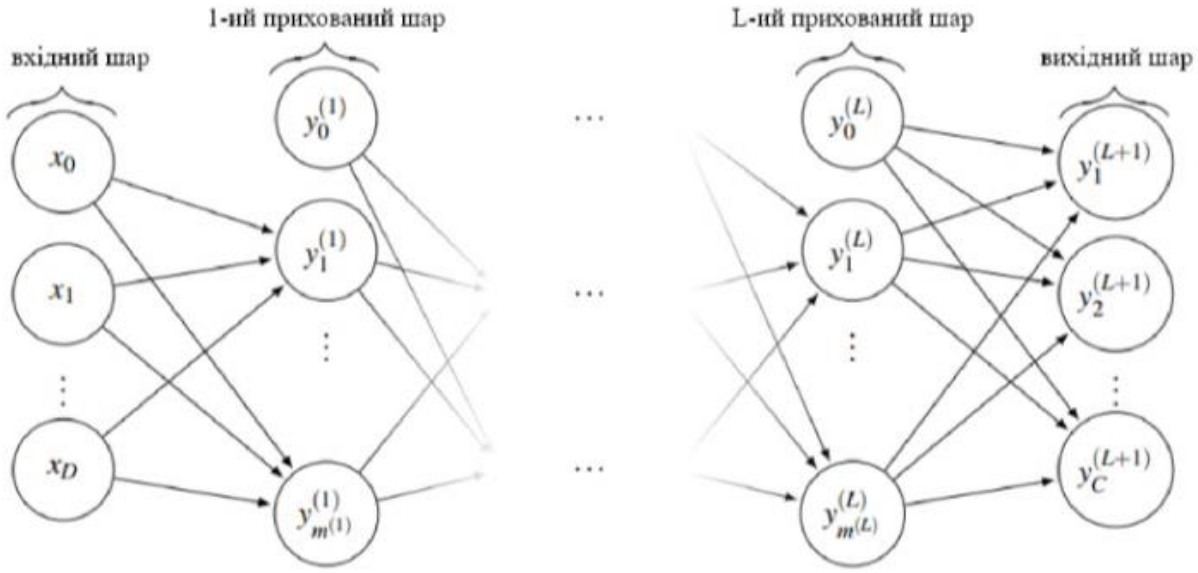


Рис. 2.6 - Мережевий граф перцептрона з L + 1 шарами, D входами та C виходами, що містить L прихованих шарів

Перцептрон, зображений на Рисунку 2.6, складається з \(L + 1\) шарів, включаючи \(D\) вхідних даних, \(C\) вихідних сигналів, а також \(L\) прихованих шарів. Кожен \(i\)-й елемент у шарі \(l\) розраховує свій вихід за визначеною формулою.

$$y_i^{(l)} = f\left(z_i^{(l)}\right), \text{де} \tag{2.1}$$

$$z_i^{(l)} = \sum_{k=0}^{m^{(l-1)}} w_{i,k}^{(l)}\, y_{i,k}^{(l-1)} + w_{i,0}^{(l)} \tag{2.2}$$

де $w_{i,k}^{(l)}$ – це вага з'єднання між k елементом у шарі l – 1 з i елементом і елементом шару l, а $w_{i,0}^{(l)}$ – це зовнішній вхід до пристрою і називається зміщенням. Тут $m^{(l)}$ показує кількість елементів у шарі l, так, що $D = m^{(0)}$ та $C = m^{(L+1)}$.Для

того, шоб було простіше, можна розглядати зміщення як вагу при введенні фіктивного блоку $y_0^{(l)} := 1$ у кожен із шарів.

$$z_i^{(l)} = \sum_{k=0}^{m^{(l-1)}} w_{i,k}^{(l)} \, y_{i,k}^{(l-1)} \tag{2.3}$$

Або

$$z_i^{(l)} = w^{(l)} y^{(l-1)} \tag{2.4}$$

де $z^{(l)}, w^{(l)}$ та $y^{(l-1)}$ позначають відповідні векторні та матричні вигляди про фактичні входи $z_i^{(l)}$, ваги $w_{i,k}^{(l)}$ та виходи $y_{i,k}^{(l-1)}$ відповідно

У загальному випадку багатошаровий перцептрон можна функціонально описати наступним чином.:

$$y(\cdot, w): \mathbb{R}^D \to \mathbb{R}^C, x \mapsto y(x, w) \tag{2.5}$$

Де вихід вектору (x, w) має вихідні значення $y_i(x, w) := y_i^{(L-1)}$ та w є вектором усіх вагових коефіцієнтів в мережі

Нейронні мережі вважаються глибокими, якщо вони включають понад три приховані шари. Навчання таких мереж є досить складним завданням. [17].

2.3 Згорткова нейронна мережа

Згорткові нейронні мережі (Convolutional Neural Networks, CNN) є найпоширенішим типом ШНМ, який використовується для аналізу зображень і відео. Основна ідея CNN полягає у виявленні характерних ознак зображення за допомогою згорткових шарів.

CNN працюють за такими принципами:

- Згорткові шари виділяють локальні особливості зображення, такі як контури, кути та текстури.
- Шари підвибірки (Pooling layers) зменшують розмірність даних, що знижує обчислювальні витрати і підвищує стійкість до зсувів або змін масштабу.
- Повнозв’язні шари використовуються для класифікації отриманих ознак.

У відеоспостереженні CNN застосовуються для:

- Детектування об’єктів на відео.
- Розпізнавання осіб та ідентифікації людей.
- Виявлення залишених предметів або підозрілих дій.

Faster Region-Based CNN (Faster R-CNN) є вдосконаленням стандартної архітектури CNN, яке спеціалізується на швидкому і точному детектуванні об’єктів. Архітектура Faster R-CNN працює у два етапи:

1. Генерується набір регіонів за допомогою спеціального модуля Region Proposal Network (RPN). Це дозволяє визначити області на зображенні, які, ймовірно, містять об’єкти.
2. Згенеровані регіони передаються у згорткову мережу, яка класифікує об’єкти та уточнює їх межі.

Завдяки своїй високій точності Faster R-CNN широко використовується у задачах розпізнавання та відстеження об’єктів у відеоспостереженні [18].

Окрім Faster R-CNN, у задачах відеоаналізу використовуються інші підходи:

- YOLO (You Only Look Once): забезпечує високошвидкісне детектування об’єктів у реальному часі.
- SSD (Single Shot MultiBox Detector): поєднує швидкість роботи з високою точністю.
- Recurrent Neural Networks (RNN) та Long Short-Term Memory (LSTM): застосовуються для аналізу послідовностей відеокадрів, дозволяючи враховувати часовий контекст.

Штучні нейронні мережі стали невід'ємною частиною систем відеоспостереження завдяки їх здатності працювати з великомасштабними даними, забезпечуючи високу точність і швидкість обробки. Вони дозволяють автоматизувати процеси виявлення об'єктів, аналізу поведінки та прогнозування загроз.

Таким чином, ШНМ, зокрема CNN, є важливим інструментом у задачах аналізу відеопотоку. Вони забезпечують ефективність і точність роботи сучасних систем відеоспостереження, сприяючи підвищенню рівня безпеки та автоматизації процесів моніторингу [19].

2.3.1 Згортка

Для простоти представимо зображення, як градації сірого, яке визначається функцією:

$$I: \{1, \dots, n_1\} \times \{1, \dots, n_2\} \to W \subseteq \mathbb{R}, (i, j) \mapsto I_{i,j} \tag{2.6}$$

таким чином зображення I може бути представлено за допомогою матриці розміром $n_1 \times n_2$. У більшості випадків W, який представлено набором {0, …, 255}, що є 8-бітним каналом. Тоді кольорове зображення можна представити масивом розміром $n_1 \times n_2 \times 3$, якщо взяти, наприклад, кольорову схему RGB. Виходячи з того, що $K \in \mathbb{R}^{2h_1+1 \times 2h_2+1}$, дискретна згортка зображення I та фільтр K можна представити формулою:

$$(I * K)_{r,s} := \sum_{u=-h_1}^{h_1} \sum_{u=-h_2}^{h_2} K_{u,v} I_{r+u,s+v} \tag{2.7}$$

де фільтр виглядає так:

$$K = \begin{pmatrix} K_{-h1,-h2} & \cdots & K_{-h1,h2} \\ \vdots & K_{0,0} & \vdots \\ K_{h1,-h2} & \cdots & K_{h1,h2} \end{pmatrix} \tag{2.8}$$

Слід звернути увагу на виконання цієї операції на краях зображення. Один із підходів до вирішення цієї проблеми полягає в тому, щоб застосовувати фільтр лише до тих ділянок зображення, де його використання є коректним. Це призводить до того, що розмір вихідного масиву буде меншим, ніж розмір початкового зображення. [20].

Розповсюдженим фільтром для згладжування є дискретний фільтр Гауса:

$$\left(K_{G(\sigma)}\right)_{r,s} = \frac{1}{\sqrt{2\pi}\sigma^2} \exp\left(\frac{r^2 + s^2}{2\sigma^2}\right) \tag{2.9}$$

де σ є середньо квадратичним відхиленням розподілу Гауса.

2.3.2 Згорткові шари

Якщо позначити згортковий шар як *l*, тоді вхід на шар *l* складається з $m_1^{(l-1)}$ відображень. У випадку, якщо l = 1, на вхід подається власне необроблене зображення *I*, яке складається з 1 чи більше складових каналів. Вихід згорткового шару *l* складається з $m_1^{(l)}$ відображень ознак, що має вигляд матриці розмірності $m_2^{(l)} \times m_3^{(l)}$. Кожна *i* матриця віображення ознак $Y_i^{(l)}$ з шару *l* має наступний вигляд

$$Y_i^{(l)} = B_i^{(l)} + \sum_{j=1}^{m_1^{(l-1)}} K_{i,j}^{(l)} * Y_j^{(l-1)} \tag{2.10}$$

де $B_i^{(l)}$ – це матриця зсуву (bias matrix), а $K_{i,j}^{(l)}$ є фільтром розміру $2h_1^{(l)} + 1 \times 2h_2^{(l)} + 1$, який поєднує *j* зображення ознак у шарі (l – 1) з *i* відображенням з шару

l (рис. 1.10). При цьому $m_1^{(l)}$ і $m_2^{(l)}$ знаходяться під впливом ефекту границі, що значить, що при використанні дискретної згортки у так званій коректній області, розмір вихідного відображення буде виглядати наступним чином:

$$m_2^{(l)} = m_2^{(l-1)} - 2h_1^{(l)} \text{ та } m_3^{(l)} = m_3^{(l-1)} - 2h_1^{(l)} \tag{2.11}$$

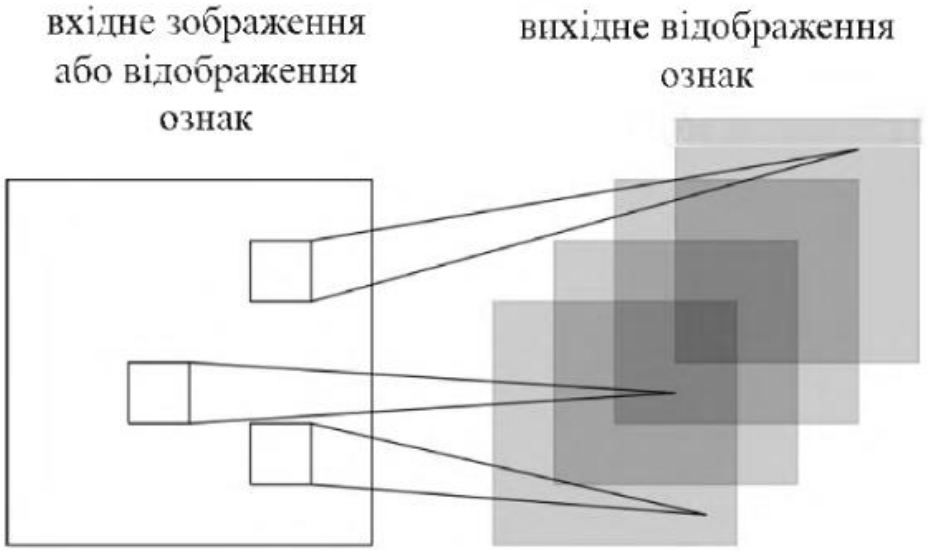


Рис. 1.10 - Ілюстрація одного зі згорткових шарів.

Ці фільтри, які використовують, щоб обчислити певне відображення ознак $Y_i^{(l)}$, часто є однаковими, тобто $K_{i,j}^{(l)} = K_{j,k}^{(l)}$, для $j \neq k$. Окрім цього, сума $\sum_{j=1}^{m_1^{(l-1)}} K_{i,j}^{(l)} * Y_j^{(l-1)}$ може вийти за межі підмножини вхідних відображень ознак.

Щоб пов'язати згортковий шар і його операції з багатошаровим перцептроном, необхідно переформулювати рівняння:

$$Y_i^{(l)} = B_i^{(l)} + \sum_{j=1}^{m_1^{(l-1)}} K_{i,j}^{(l)} * Y_j^{(l-1)} \tag{2.12}$$

Кожне відображення ознак $Y_i^{(l)}$ у шарі l містить $m_2^{(l)} \cdot m_3^{(l)}$ елементів, що організовані у вигляді двовимірного масиву. Елемент, розташований у позиції (r,s), обчислює свій вихід за наступним правилом.

$$\left(Y_i^{(l)}\right)_{r,s} = \left(B_i^{(l)}\right)_{r,s} + \sum_{j=1}^{m_1^{(l-1)}} \sum_{u=-h_1^{(l)}}^{h_1^{(l)}} \sum_{u=-h_2^{(l)}}^{h_2^{(l)}} \left(K_{i,j}^{(l)}\right)_{u,v} \left(Y_j^{(l-1)}\right)_{r+u,s+v} \quad (2.13)$$

Тренувальні вагові коефіцієнти розташовані у фільтрах $K_{i,j}^{(l)}$ та матриці зміщень $B_i^{(l)}$

Також слід зазначити, як використовується процес відбору виробку (subsampling) для зменшення рівню шумів та спотворень. Це досягається за рахунок використання факторів пропуску (skipping factors) $s_1^{(l)}$ і $s_2^{(l)}$. Для цього треба пропустити певну кількість пікселів зображення у горизонтальному і вертикальному напрямках перед тим, як повторно використовувати фільтр. У результаті розміри вихідного відображення ознак визначатимуться за такою формулою:

$$m_2^{(l)} = \frac{m_2^{(l-1)} - 2h_1^{(l)}}{s_1^{(l)} + 1} \text{ та } m_2^{(l)} = \frac{m_3^{(l-1)} - 2h_2^{(l)}}{s_2^{(l)} + 1} \quad (2.14)$$

2.4 Алгоритми багатоцільового відстеження

Багатоцільове відстеження (Multiple Object Tracking, MOT) є однією з основних задач у комп’ютерному зорі, яка полягає у виявленні та відстеженні кількох об’єктів, що рухаються одночасно, в умовах реального часу. Ця задача є складною через багато факторів, таких як часткове перекриття об’єктів, зміни їхнього вигляду, помилки виявлення та необхідність прогнозування їхнього

подальшого руху. У системах відеоспостереження багатоцільове відстеження використовується для ефективного моніторингу кількох об'єктів, таких як люди, транспортні засоби або інші об’єкти, що рухаються в межах зони спостереження.

Основною метою багатоцільового відстеження є зв’язування виявлених об’єктів на різних кадрах відео в єдиний відслідковуваний об’єкт. Задача складається з двох основних етапів:

1. Детектування об’єктів — на кожному кадрі необхідно виявити об’єкти, що знаходяться в полі зору камери. Для цього використовуються алгоритми детектування об’єктів, такі як Faster R-CNN або YOLO.

2. Відстеження об’єктів — після того як об’єкти виявлені, наступним кроком є їх ідентифікація та відстеження через кадри відео, щоб уникнути сплутування з іншими об’єктами. Для цього використовуються методи, що враховують попередній стан об’єкта, його рух і позицію.

Фільтр Калмана є математичним методом, який широко використовується для прогнозування траєкторій об’єктів, що рухаються. У контексті багатоцільового відстеження фільтр Калмана дозволяє оцінити майбутнє місцезнаходження об’єкта на основі його попереднього стану (позиції та швидкості).

Фільтр Калмана працює за принципом комбінування вимірювань (наприклад, координат об’єкта з кадрів відео) та прогнозу, ґрунтуючись на попередніх даних. Це дозволяє коригувати похибки у вимірюваннях та забезпечує більш точні прогнози траєкторії. У системах відеоспостереження фільтр Калмана використовується для відстеження рухомих об’єктів, забезпечуючи плавний перехід між кадрами, навіть якщо об’єкти тимчасово зникають із поля зору камери.

Однією з проблем багатоцільового відстеження є необхідність оптимального зіставлення об’єктів між кадрами відео. Оскільки об’єкти можуть переміщатися з кадру в кадр, і навіть змінювати форму або частково перекриватися, важливо правильно визначити, який об’єкт на поточному кадрі є тим самим, що на попередньому.

Для цього використовується Угорський алгоритм, який є класичним методом для вирішення задачі оптимального зіставлення. Алгоритм визначає, який

об’єкт на поточному кадрі найкраще відповідає об’єкту на попередньому, мінімізуючи різницю між їх позиціями та характеристиками. Застосування Угорського алгоритму дозволяє мінімізувати помилки при відстеженні, забезпечуючи точність та стійкість системи [21].

Deep SORT (Deep Simple Online and Realtime Tracking) є одним з популярних алгоритмів для багатоцільового відстеження, який поєднує детектування об’єктів з алгоритмами відстеження. Основні компоненти цього алгоритму включають:

- Deep Association Metric (DAM) — нейронну мережу, яка генерує вектор ознак для кожного об’єкта, що дозволяє точно ідентифікувати об’єкти на різних кадрах, навіть якщо вони частково перекриваються.
- *Фільтр Калмана* — використовується для прогнозування руху об’єктів між кадрами.
- *Угорський алгоритм* — для оптимального зіставлення об’єктів, що дозволяє мінімізувати кількість помилок при відстеженні.

Deep SORT значно покращує точність відстеження об’єктів, оскільки використовує не лише прості координати об’єкта, але й його особливості, отримані через нейронну мережу, що дозволяє відстежувати об’єкти навіть у складних умовах, таких як перекриття чи часткова втрата зображення.

Алгоритми багатоцільового відстеження є основою для побудови сучасних систем відеоспостереження, які здатні ефективно відстежувати та ідентифікувати об’єкти в реальному часі. Застосування таких алгоритмів, як фільтр Калмана, Угорський алгоритм і Deep SORT, дозволяє забезпечити точність і стабільність відстеження, що є критично важливим для безпеки та моніторингу в реальному світі. Водночас, вирішення складних задач, таких як перекриття об’єктів і часткова втрата зображення, є значущими досягненнями для подальшого розвитку технологій відеоспостереження [22].

2.5 Фільтр Калмана

Фільтр Калмана вважається оптимальним рішенням для багатьох задач прогнозування даних та відстеження [13].

Більшість сигналів можна описати наступним чином:

$$y_k = a_k x_k + n_k \tag{2.15}$$

де y_k – залежний від часу сигнал, a_k – коефіцієнт посилення, x_k – сигнал, який переносить інформацію, а n_k – адаптивний шум.

Потрібно оцінити x_k. Похибка – різниця між очікуванним $\hat{x}_k$ та реальним x_k:

$$f(e_k) = f(x_k - x_k) \tag{2.16}$$

Особлива форма $f(e_k)$ залежить від конкретного застосування, однак відомо, що ця функція має бути позитивною і монотонно зростати [23]. Одним із прикладів функції помилки з такими властивостями є квадрат функції помилки.

Крім того, необхідно враховувати здатність фільтра прогнозувати великий обсяг даних протягом тривалого часу. Для цього вводиться більш інформативна метрика – очікуване значення функції помилки;

$$f_{\text{втрати}} = E\big(f(e_k)\big) \tag{2.17}$$

З цього виходить функція середнього квадратичного відхилення

$$\epsilon(t) = E(e_k^2) \tag{2.18}$$

Більш точне виведення може бути здійснене за допомогою статистики максимальної вірогідності [24]. Це досягається шляхом переоцінки цілі фільтра для знаходження значення x̂, яке максимізує ймовірність у.,

$$\max[P(y|\hat{x})] \tag{2.19}$$

Якщо припустити, що адаптивний випадковий шум має гауссовий розподіл зі стандартним відхиленням k, то.

$$P(y|\hat{x}) = K_k exp - \frac{(y_k - a_k x_k)^2}{2\sigma_k^2} \tag{2.20}$$

де K_k – константа нормалізації. Тоді максимальна функція правдоподібності є наступною:

$$P(y|\hat{x}) \prod_k K_k \, exp - \left(\frac{(y_k - a_k x_k)^2}{2\sigma_k^2} \right) \tag{2.21}$$

З цього виходить, що

$$\log P(y|\hat{x}) = -\frac{1}{2} \sum_{л} \left(\frac{(y_k - a_k x_k)^2}{2\sigma_k^2} \right) + C \tag{2.22}$$

Керуюча функція являє собою середньоквадратичне відхилення і може бути максимізована через зміну x_k. Таким чином, вона може бути застосована, коли маємо відхилення y_k, що відповідає гауссовому розподілу. У такому випадку середньоквадратичне відхилення використовується для знаходження значення x_k, яке максимізує ймовірність сигналу y_k [25].

У цьому контексті оптимальний фільтр визначається як той, який з усіх можливих мінімізує середньоквадратичне відхилення.

Припустимо, ми хочемо визначити значення змінної в процесі з певною формою.

$$x_{k+1} = \Phi x_k + \omega_k \tag{2.23}$$

де x_k – вектор станів процесу в момент часу k (розмірність – $n \times 1$); Ф – це матриця (розмірність – $n \times m$) переходу станів в процесі від стану у момент часу k до стану у момент часу $k + 1$, що вважається стаціонарною з плином часу; ω_k – це білий шум з відомою коваріацією, який пов'язаний з процесом ($n \times 1$)

За цією змінною можна показати спостереження у формі

$$z_k = Hx_k + v_k \tag{2.24}$$

де z_k – це фактичне вимірювання x у момент часу k (розмірніість - $m \times 1$); H – зв'язок, без шуму, між вектором вимірювання та вектором стану, припускається стаціонарним з плином часу (розмірність $m \times n$); v_k – помилка вимірювання, тобто білий шум, пов'язаний з вимірюванням, який має відому коваріацію та нульову перехресну кореляцію з власне шумом процесу (розмірність $m \times 1$).

Як показано, для зменшення середньоквадратичного відхилення оптимальний фільтр можна побудувати, правильно моделюючи системні похибки через гауссові розподіли. При цьому припускається, що коваріації двох шумових моделей є стаціонарними в часі та описуються таким чином:.

$$Q = E[\omega_k \omega_k^T] \tag{2.25}$$

$$R = E[v_k v_k^T] \tag{2.26}$$

З функції середнього квадратичного відхилення, випливає:

$$E[e_k e_k^T] = P_k \tag{2.27}$$

де P_k – матриця коваріації похибки в момент часу k (розмірність $n \times n$)

Можна розширити рівняння наступним чином:

$$P_k = E[e_k e_k^T] = E[(x_k - \hat{x}_k)(x_k - \hat{x}_k)^T] \quad (2.28)$$

Приймаючи попередню оцінку $\hat{x}_k$ за $\hat{x}'_k$, отриману на основі знань про систему, ми отримуємо рівняння для нової оцінки, комбінуючи попередню оцінку з даними вимірювань.

$$\hat{x}_k = \hat{x}'_k + K_k(z_k - H\hat{x}'_k) \quad (2.29)$$

де K_k – передавальний коефіцієнт Калмана. Тоді як, $z_k - H\hat{x}'_k$ – нововведення (відхилення) вимірювання

$$i_k = z_k - H\hat{x}'_k \quad (2.30)$$

Використовуючи підстановки, отримаємо

$$\hat{x}_k = \hat{x}'_k + K_k(H\hat{x}_k + v_k - H\hat{x}'_k) \quad (2.31)$$

$$P_k = E\left[[(I - K_k H)(x_k - \hat{x}'_k) - K_k v_k][(I - K_k H)(x_k - \hat{x}'_k) - K_k v_k]^T\right] \quad (2.32)$$

Треба зазначити, що $x_k - \hat{x}'_k$ - це похибка попередньої оцінки. Вона не корелює з похибкою вимірювання, тобто рівняння можна переписати наступним чином

$$P_k = (I - K_k H)P'_k(I - K_k H)^T + K_k R K_k^T \quad (2.33)$$

де P'_k - це попередня оцінка P_k

Отримане рівняння є коваріацією оновленої оцінки. Діагональ матриці коваріації містить середні квадратичні відхилення.

$$P_{kk} = \begin{bmatrix} E[e_{k-1}e_{k-1}^T] & E[e_{k1}e_{k-1}^T] & E[e_{k+1}e_{k-1}^T] \\ E[e_{k-1}e_k^T] & E[e_{k1}e_k^T] & E[e_{k+1}e_{k1}^T] \\ E[e_{k-1}e_{k+1}^T] & E[e_{k1}e_{k+1}^T] & E[e_{k+1}e_{k+1}^T] \end{bmatrix} \quad (2.34)$$

Сума елементів діагоналі матриці – це слід матриці. У випадку матриці коваріації похибок, слід – це сума середньо квадратичних відхилень. Це значить, що дане відхилення можна мінімізувати за допомогою мінімізації сліду P_k, через що зменшиться слід P_{kk}.

Слід P_k – це перша похідна по K_k, результат прирівнюється до нуля для знаходження умови мінімуму.

$$P_k = P_k' - K_k H P_k' - P_k' H^T K_k^T + K_k (H P_k' H^T + R) K_k^T \quad (2.35)$$

Слід зазначити, що слід матриці дорівнює сліду її транспозиції, тобто можемо записати рівняння як

$$T[P_k] = T[P_k'] - 2T[K_k H P_k'] + T[K_k (H P_k' H^T + R) K_k^T] \quad (2.36)$$

де $T[P_k]$ – це слід матриці P_k.

Після диференціювання по K_k отримуємо

$$\frac{dT[P_k]}{dK_k} = -2(HP_k')^T + 2K_k(HP_k'H^T + R) \quad (2.37)$$

Після прирівнювання з нулем та перестановки доданків

$$(HP_k')^T = K_k(HP_k'H^T + R) \quad (2.38)$$

Знаходимо коефіцієнт Калмана K_k

$$K_k = HP'_kH^T + R \tag{2.39}$$

Після остаточної підстановки отримуємо

$$P_k = P'_k - P'_k\, H^T(HP'_kH^T + R)^{-1}HP'_k \tag{2.40}$$

$$P_k = P'_k - K_kHP'_k \tag{2.41}$$

$$P_k = (I - K_kH)P'_k \tag{2.42}$$

Це рівняння, яке ми отримали – це оновлена матриця коваріації похибок з оптимальним передавальним коефіцієнтом (формула коваріації апостеріорної похибки). Отримані рівняння використовують для оцінки значення x_k. Проекція стану досягається за рахунок

$$\hat{x}'_{k+1} = \Phi\hat{x}_k \tag{2.43}$$

Для того, щоб завершити рекурсію, необхідно знайти рівняння, яке проектує матрицю коваріації похибок у наступний інтервал часу $k + 1$. Спочатку сформуємо вираз без попередньої похибки

$$e'_{k+1} = x_{k+1} - \hat{x}'_{k+1} \tag{2.44}$$

$$e'_{k+1} = (\Phi e_k + \omega_k) - \Phi\hat{x}'_k \tag{2.45}$$

$$e'_{k+1} = \Phi e_k + \omega_k \tag{2.46}$$

Продовжуючи рівняння для k+1

$$P'_{k+1} = E[e'_{k+1}e^{T\prime}_{k+1}] = E[(\Phi e_k + \omega_k)(\Phi e_k + \omega_k)^T] \tag{2.47}$$

Слід зазначити, що e_k і ω_k мають нульову перехресну кореляцію, оскільки шум ω_k накопичується у момент часу $\overline{k, k+1}$, а e_k – похибка до моменту k

$$P'_{k+1} = E\left[e'_{k+1} e^{T'}_{k+1}\right] \quad (2.48)$$

$$P'_{k+1} = [\Phi e_k (\Phi e_k)^T] + E[\omega_k \omega_k^T] \quad (2.49)$$

$$P'_{k+1} = \Phi P_k \Phi^T + Q \quad (2.50)$$

Остаточний алгоритм фільтру Калмана наведено нижче (рис. 2.11)

Рис. 2.11 - Діаграма фільтру Калмана

2.6 Угорський алгоритм

Угорський алгоритм — це алгоритм комбінаторної оптимізації, який розв'язує задачу про призначення за час, пропорційний поліному. $O(n^4)$

Формулювання задачі: Є n ресурсів і n завдань, які потрібно розподілити так, щоб кожен ресурс виконував лише одне завдання. Відомі витрати на виконання кожного завдання кожним ресурсом. Потрібно знайти оптимальний спосіб

призначення завдань ресурсам. У матричному поданні це виглядає як матриця розміром n × n , де елемент у і -му рядку та j -му стовпці визначає вартість виконання j -го завдання і -м ресурсом.

$$c = \begin{bmatrix} c_{1,1} & \cdots & c_{1,1} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{n,n} \end{bmatrix} \tag{2.51}$$

Алгоритм:

1. Організувати дані в матриці так, щоб рядки відповідали "ресурсам", а стовпці — "завданням", причому кожен елемент матриці відображає витрати ресурсу на виконання конкретного завдання.

2. Перевірити, чи матриця квадратна. Якщо ні, додати фіктивний рядок (ресурс) або стовпець (завдання), заповнивши їх значеннями, рівними найбільшому елементу початкової матриці.

3. У кожному рядку відняти найменше значення з усіх елементів цього рядка.

4. У кожному стовпці виконати аналогічну операцію, віднімаючи мінімальне значення з усіх елементів стовпця.

5. Викреслити всі нульові елементи матриці мінімальною кількістю ліній. Якщо кількість ліній дорівнює розміру матриці, перейти до кроку 9.

6. Додати найменший з не викреслених елементів матриці до кожного елемента, що перетинається з лініями. Якщо елемент перетинається двома лініями, додавання виконується двічі.

7. Від кожного елемента, що не перекреслений жодною лінією, відняти цей мінімальний елемент.

8. Повторно викреслити всі нульові елементи, використовуючи мінімальну кількість ліній. Якщо кількість ліній усе ще менша за розмірність матриці, повернутися до кроку 6.

9. Обрати оптимальний розподіл «завдань» серед «ресурсів», забезпечуючи, щоб у кожному рядку і стовпці був вибраний лише один нуль.

10. Перенести знайдений розподіл на початкову матрицю, виключивши фіктивні рядки та стовпці. В результаті цей розподіл покаже, якому ресурсу призначене яке завдання, а сума вибраних елементів визначить загальну вартість виконання завдань.

2.7 Автоматизовані системи відеоспостереження

Автоматизовані системи відеоспостереження включають мережу відеодатчиків, які здійснюють моніторинг людей, аналізуючи їх поведінкові особливості та визначаючи тих, хто може становити потенційну загрозу. Такий підхід ефективно використовується в системах, де застосовуються універсальні та очевидні візуальні показники, що дають змогу оцінювати рівень безпеки або наявність небезпеки [12].

Прикладом таких метрик є виявлення специфічних об’єктів, які можуть вказувати на потенційну загрозу, наприклад, зброї.

Рис. 2.12 - Розпізнавання збройного нападу

Ще одним показником, який може свідчити про незвичайність подій, є положення тіла людини та швидкість її пересування.

Рис. 2.13 - Розпізнавання незвичної поведінки

Системи комп’ютерного зору, що натреновані на розпізнавання людського руху, будуть вважати рух інших транспортних засобів, наприклад велосипеду (Рис. 2.14), аномальним, та сповіщати про це оператора.

Рис. 2.14 - Аномальний рухаючийся об'єкт (велосипедист)

У сфері інформаційної безпеки виникає проблема складності визначення критеріїв безпеки. Наприклад, фізичний доступ до певного об’єкта однією особою може бути допустимим, тоді як ті самі дії іншої особи можуть порушувати встановлений рівень доступу. До того ж, навіть відносно точне виявлення факту фізичного доступу до певного інформаційного ресурсу є доволі складним завданням [26].

2.8 Модель взаємодії людини і об’єкта з точки зору ІБ

Одним із можливих способів вирішення цієї проблеми є модель взаємодії людини з об'єктами (human-object interaction). Ця модель застосовує контекстуальний підхід і навчається визначати інформативні області зображення, використовуючи зовнішній вигляд людини або об'єкта. Контекст допомагає визначити, на які частини зображення варто звернути увагу. Наприклад, для визначення того, чи тримає людина предмет у руці, система аналізує область навколо її рук [27]. У випадку з велосипедом на зображенні акцент зміщується на позу людини поблизу нього, що дозволяє розрізняти такі дії, як їзда на велосипеді або його ведення. Крім того, система аналізує напрямок погляду людини, що дає змогу зрозуміти, на що вона звертає свою увагу, і тим самим зменшити ймовірність помилок.

Однак існує низка недоліків, які наразі ускладнюють впровадження цього підходу в системах відеоспостереження:

1. Швидкодія. Системи відеоспостереження, що використовують алгоритми розпізнавання образів, повинні бути здатними одночасно відстежувати десятки осіб за допомогою кожної камери. Незважаючи на те, що сучасні алгоритми комп’ютерного зору дозволяють здійснювати моніторинг взаємодії людини з об’єктами в реальному часі зі задовільною частотою кадрів, їх масштабованість все ще залишається недостатньою.

2. Ракурс. Для максимально ефективної роботи системі потрібен прямий ракурс. Проте камери відеоспостереження зазвичай розташовані вище рівня очей,

що ускладнює відстеження зорового центру уваги людини. А це є важливим аспектом фізичного захисту інформаційних систем.

3. Аналіз дій людини. Хоча комп’ютерний зір демонструє вражаючу точність у описі певних ситуацій, він здебільшого зосереджується на процесах (наприклад, людина тримає документ), а не на їх наслідках (людина сховала документ у валізу) [27]. Це обмеження не дозволяє ефективно аналізувати дії, які потенційно можуть призводити до витоку інформації.

2.9 Використання ШІ у системах відеоспостереження

Хоча системи розпізнавання образів наразі не можуть точно визначати факти фізичної загрози інформаційній безпеці, вони можуть виконувати роль допоміжного інструменту, доповнюючи існуючі рішення у сфері інформаційного захисту.

Основною функцією камер відеоспостереження є надання візуальної інформації персоналу, який контролює безпеку, про ситуацію в зоні спостереження. Оскільки об'єкти, що потребують захисту, зазвичай ізольовані, основними динамічними елементами у таких зонах зазвичай є люди, які там перебувають. Тому основним завданням обробки зображень у цьому контексті є виявлення присутності та визначення розташування людей у межах видимого поля камери.

Для підвищення рівня інформаційної безпеки запропоновано застосування систем комп'ютерного зору, які здійснюють моніторинг переміщення людей і відповідають таким вимогам [28]:

1. Кожен відстежуваний об'єкт отримує унікальний ідентифікатор під час його виявлення.

2. Система здатна коректно працювати навіть у випадках тимчасового зникнення об'єкта з поля зору камери, причому тривалість цього часу може налаштовуватися.

3. Ймовірність втрати об'єкта, що вимагає його повторної ідентифікації, зведена до мінімуму.

4. Обчислення виконуються у режимі реального часу з належною масштабованістю.

5. Система дотримується усіх вимог щодо безпеки та конфіденційності даних на всіх етапах роботи.

6. Результати обробки надаються у візуалізованому вигляді для покращення ефективності роботи оператора.

У запропонованій системі можна виділити такі ключові завдання:

1. Присвоєння ідентифікатора особі під час її реєстрації камерами відеоспостереження:

Ця задача є критичною, оскільки точність і унікальність ідентифікатора значно впливають на ефективність роботи системи. Найкращим рішенням є створення контрольного пункту з використанням аутентифікаторів, таких як зчитувачі смарт-карток. Альтернативою може бути застосування біометричних технологій, хоча такі рішення зазвичай є дорожчими.

2. Виділення сторонніх осіб на моніторі оператора: На об'єктах, де сторонні особи (наприклад, гості) присутні за гостьовими посвідченнями, а впровадження комплексних заходів захисту периметру є економічно необґрунтованим, доцільно позначати таких осіб на екранах операторів. Для підвищення ефективності роботи операторів система повинна акцентувати увагу на подіях, що мають значення для інформаційної безпеки. Завдяки надійним алгоритмам розпізнавання та відстеження пересувань, оператори можуть зосереджуватись на меншій кількості об'єктів. Особливу увагу слід приділяти довготривалій відсутності таких об'єктів у полі зору камер [29].

3. Обмеження доступу до даних аутентифікації: Задля захисту конфіденційної інформації та через використання сторонніх програм-аутентифікаторів, доступ до даних аутентифікації повинен бути обмеженим. Це можна вирішити шляхом впровадження API, яке дозволяє інтегрувати функціонал

системи з даними інших джерел через спеціально розроблені конектори для поширених систем.

4. Використання даних про переміщення осіб для поліпшення інформаційної захищеності об'єкта: Пропонується використовувати дані, отримані від алгоритмів відстеження переміщення осіб, як статистичні метрики для оцінки потенційних вразливостей захищених зон. Це передбачає застосування показників, які допомагають виявити наявність осіб з недостатнім рівнем доступу в критичних зонах. Дані про переміщення, що складаються з координат, ідентифікаторів осіб і камер на кожен момент часу, займають менше місця на носіях і можуть бути накопичені на тривалий період [30].

5. Можливість ручного контролю системи відслідковування переміщень: У разі втрати об'єкта спостереження оператор повинен мати можливість вручну вказати пропажу, що дозволить підвищити увагу оператора в майбутньому та компенсувати можливі помилки автоматичної системи. Це також покращує контроль і забезпечує додатковий рівень надійності в системі.

Таблиця 2.1

Чинники і фактори впливу комп’ютерного зору

Чинник	*Фактор впливу*
1) Використання ідентифікатора, отриманого під час допуску особи натериторію захищеного об’єкта длявідстеження її подальших переміщень.	Підвищення рівня безпеки за рахуноквикористання додаткових засобіваутентифікації. Рівень впливувизначається ефективністю алгоритмувідстеження та власне системиаутентифікації.
2) Виокремлення осіб з фону на відеозаписі, підсвічення з урахуванням певної встановленої легенди, наприклад рівня допуску.	Підвищення рівня контрольованості переміщень осіб, що становлять потенційну загрозу для витоку інформації, проте наявність яких на території об’єкту є неминучою (наприклад, особи, що знаходяться за гостьовим посвідченням).

Продовження таблиці 2.1

3) Сповіщення оператора про тимчасову втрату сліду певної особи, що може становити потенційну загрозу (наприклад, особи з низьким рівнем доступу).	Покращення спостереження на території об'єкта шляхом акцентування уваги оператора на конкретному секторі відеоспостереження. Рівень впливу залежить від здатності алгоритму здійснювати довгострокове відслідковування особи з мінімальним ризиком її втрати з поля зору.
4) Сповіщення оператора про остаточну втрату сліду певної особи з можливістю вручну відновити відсутній слід.	Покращення контролю за ситуацією на території об'єкта шляхом фокусування уваги оператора на конкретному секторі відеоспостереження. Рівень ефективності визначається здатністю алгоритму забезпечувати довгострокове відслідковування особи з мінімальним ризиком її втрати з поля зору.
5) Збереження даних про переміщення осіб на території об'єкта у форматі вихідних даних системи комп'ютерного зору для подальшого використання в статистичних цілях та при розслідуванні інцидентів.	Підвищення рівня захисту за рахунок додаткових записів про стан об'єкта. Використання статистичних даних для виявлення аномалій та закономірностей переміщень, що дозволяє обґрунтовано вносити зміни до вже існуючої системи контролю та захисту інформації (КСЗІ).

2.9.1 Побудова теплових карт

Зібрані дані можна застосовувати для статистичних цілей. Одним з таких методів є створення теплових карт (англ. - Heatmap). Теплова карта — це графічне представлення даних, де окремі значення з матриці відображаються через різні кольорові градієнти. У цьому випадку використовується інформація з камер відеоспостереження, що фіксує переміщення осіб на території захищеного об'єкта. На рис. 2.17 продемонстровано приклад використання цієї технології. Інтенсивність переміщень відображається більш яскравим кольором (або світлішими відтінками для чорно-білих зображень). Як видно на тепловій карті, алгоритм не розрізняє переміщення окремих осіб, оскільки його завданням не є відслідковування переміщення кожної людини [5].

Рисунок 2.16 - Приклад теплової карти переміщень людей (відтінки сірого позначають частоту проходження)

Якщо цю технологію впроваджувати як додаткову в систему комплексного захисту інформації (КСЗІ), доцільно буде виокремлювати переміщення кожної окремої особи. В такому випадку можна запропонувати шляхи використання отриманих даних для підвищення рівня інформаційної безпеки.

Таблиця 2.2 Вплив на КСЗІ

Шлях використання	*Вплив на КСЗІ*
Виявлення закономірностей переміщень	- Можливість реорганізації системи відеоспостереження для підвищення її ефективності. - Оцінка ефективності використання компонентів системи контролю доступу, з якими безпосередньо взаємодіють особи. - Можливість реорганізації персоналу для мінімізації переміщень і взаємодії осіб з різними рівнями доступу. - Оптимізація розподілу витрат на КСЗІ з урахуванням різниць у рівні та джерелах загроз залежно від часу.
Виявлення аномалій переміщень (окремих осіб відповідно до їх ріння доступу)	- Можливість своєчасно реагувати на потенційно несанкціонований доступ

2.10 Висновок до другого розділу

Другий розділ роботи був присвячений аналізу технологій та алгоритмів, що використовуються в сучасних системах відеоспостереження для автоматичного відстеження та ідентифікації об’єктів. Було розглянуто принципи роботи штучних нейронних мереж, а також їх роль у вирішенні задач комп’ютерного зору. Особливу увагу приділено застосуванню згорткових нейронних мереж (CNN) та їх модифікацій, таких як Faster R-CNN, для виявлення та класифікації об’єктів на зображеннях.

Окремо проаналізовано алгоритм Deep SORT, який поєднує методи детектування об’єктів із процедурами їхнього відстеження. Алгоритм демонструє високу ефективність завдяки використанню фільтра Калмана для прогнозування траєкторії об’єктів та угорського алгоритму для оптимального зіставлення об’єктів між кадрами. У роботі підкреслено переваги Deep SORT, зокрема його здатність працювати у режимі реального часу, масштабованість та точність навіть у складних умовах, таких як перекриття об’єктів або рух камери.

Розглянуто виклики, які постають перед системами багатоцільового відстеження, зокрема:

- Труднощі роботи з об’єктами, що частково перекриваються або знаходяться на межі поля зору камери.

- Обмеженість тренувальних наборів даних і відсутність універсальних стандартів оцінки ефективності алгоритмів.

- Чутливість алгоритмів до налаштувань параметрів, таких як коефіцієнти перекриття та часу втрати сліду.

Значну увагу було приділено тестуванню алгоритмів на реальних та згенерованих наборах даних. Проведені експерименти підтвердили, що сучасні методи, такі як Deep SORT, здатні забезпечити точне відстеження та ідентифікацію об’єктів за умов різної складності, включаючи великі скупчення людей або рух камери.

Таким чином, другий розділ демонструє важливість використання сучасних алгоритмів глибокого навчання та інструментів комп’ютерного зору у системах відеоспостереження. Висвітлені переваги цих підходів підтверджують їхню актуальність для вирішення задач багатоцільового відстеження в умовах реального світу. Крім того, результати експериментів засвідчують можливість адаптації цих методів до конкретних умов експлуатації, що підкреслює їхній потенціал для подальшого розвитку у сфері інформаційної безпеки.

Розділ 3 РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ З ВИКОРСИСТАННЯМ ШІ

Для розв’язання поставленої задачі було застосовано алгоритм Deep SORT (Deep Simple Online and Realtime Tracking), який використовує бібліотеку машинного навчання TensorFlow. В якості вхідних даних для нейронної мережі використовувалася інформація, зібрана F. Yu та співавторами у їхньому дослідженні [9].

Завдяки стрімкому розвитку технологій розпізнавання зображень на основі згорткових нейронних мереж (CNN), алгоритм інтегрує модифікацію CNN, відому як Faster Region CNN (FrRCNN). FrRCNN є повноцінним фреймворком, що працює у два етапи.

1. На першому етапі виділяються ключові особливості зображення та визначаються регіони, які можуть містити об’єкти.

2. На другому етапі ці регіони аналізуються для класифікації об’єктів, що в них розташовані.

Застосування такого підходу підвищує гнучкість і модульність системи, що дозволяє створювати більш ефективні рішення для задач розпізнавання зображень.

3.1 Проектування системи комп’ютерного зору

У цьому розділі детально описано структуру системи. Система складається з кількох основних модулів: модуля детектування нових об’єктів, модуля відслідковування раніше виявлених об’єктів, модуля візуалізації результатів роботи та головного модуля управління, який координує роботу всієї системи.

Діаграма класів надає статичне уявлення про структуру системи, відображаючи класи, що входять до її складу, їх атрибути, методи (операції) та зв’язки між об’єктами. Це дозволяє зрозуміти логічні зв’язки між компонентами та їх функціональність.

Діаграма пакетів, у свою чергу, демонструє залежності між різними пакетами, що формують модель системи. Вона слугує інструментом для аналізу загальної організації системи та взаємодії її частин.

На Рисунок 3.1 представлений клас, що відповідає за зберігання даних про виявлений об’єкт. Він містить наступні атрибути:

- Коефіцієнт впевненості детектування об’єкту
- Вектор ознак, що описує об'єкт
- Координати прямокутника, що описують виявлений об’єкт.

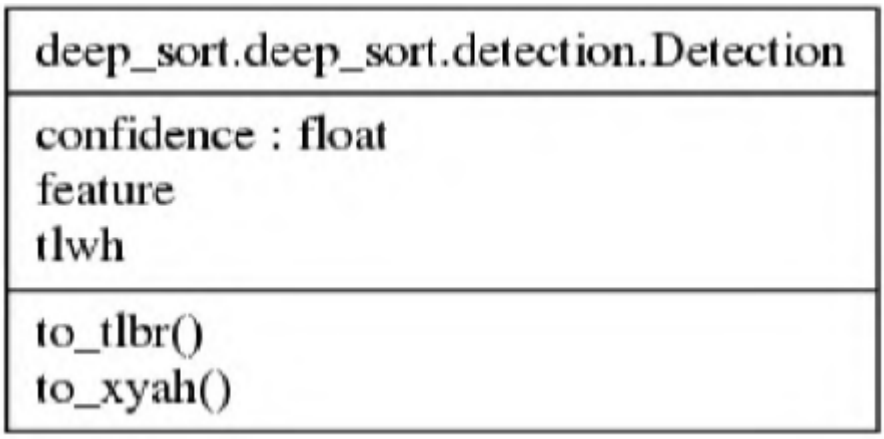


Рисунок 3.1 - Діаграма класів модуля виявлених об'єктів

На рисунку 3.2 зображено клас, який описує поточний стан об’єкта. На початковому етапі новостворені сліди мають статус «гіпотетичних», оскільки для їх підтвердження ще немає достатніх доказів. Після отримання достатньої кількості доказів стан сліду змінюється на «підтверджений», що свідчить про його достовірність. Якщо слід більше не відстежується або стає недійсним, його стан змінюється на «видалений», після чого він стає кандидатом на остаточне видалення з системи.

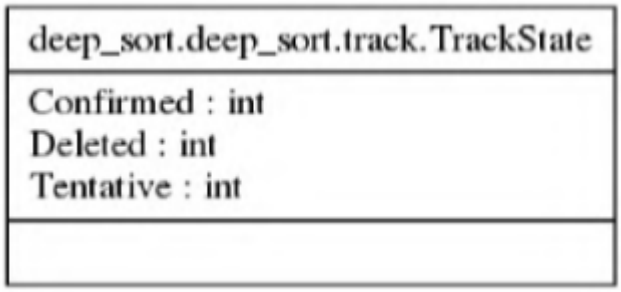


Рисунок 3.2 - Діаграма класів модуля контролю стану сліду цілі

На рисунку 3.3 представлено клас, який відповідає за збереження даних про слід об’єкта спостереження. Він містить такі ключові атрибути:

- Загальна кількість кадрів з моменту, коли об’єкт вперше потрапив у поле зору.

- Матриця коваріації початкового розподілу стану, що відображає початкову невизначеність моделі.

- Набір ознак об’єкта, який оновлюється під час кожного нового обчислення, що дозволяє уточнювати характеристику об’єкта.

- Загальна кількість оновлень вимірювань, що відображає частоту оновлення даних про слід.

- Вектор середніх величин розподілу поточного стану, який описує найбільш ймовірний стан об’єкта на даний момент.

- Поточний стан сліду, що може вказувати на актуальність даних (наприклад, «активний», «видалений» тощо).

- Загальна кількість кадрів після останнього оновлення вимірювань, що використовується для аналізу активності сліду.

- Унікальний ідентифікатор сліду, який забезпечує унікальність і дозволяє однозначно ідентифікувати об’єкт у системі.

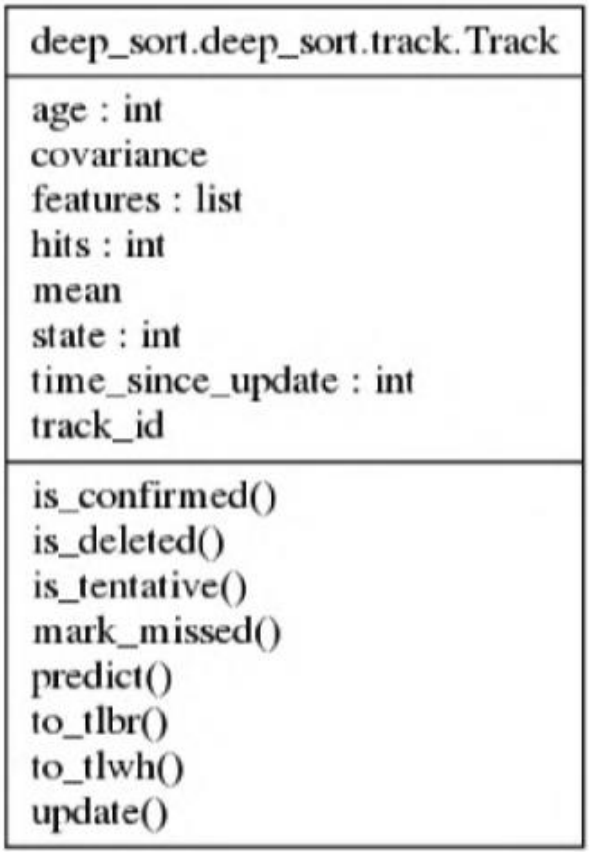


Рисунок 3.3 - Діаграма класів модуля по роботі зі слідами цілі

Модуль, представлений на рисунку 3.4, виконує функцію одночасного відслідковування кількох об’єктів. Він інтегрує механізм, що дозволяє ефективно оцінювати стан кожного об’єкта на поточний момент часу, використовуючи фільтр Калмана, описаний у розділі 2.

Основний клас обробки слідів, що входить до складу цього модуля, містить такі ключові атрибути:

- Фільтр Калмана, який використовується для згладжування та прогнозування траєкторій цілей у просторі зображення.

- Максимальна кількість кадрів для втраченого об’єкта, після якої його слід автоматично видаляється із системи, якщо нові вимірювання відсутні.

- Максимальне значення коефіцієнта площі перетину двох прямокутників, які описують об’єкти, до їх об’єднання. Цей параметр важливий для коректного розв’язання ситуацій, коли один об’єкт перекриває інший.

- Кількість кадрів, необхідних для завершення етапу ініціалізації сліду, під час якого перевіряється стійкість об’єкта у полі зору.

- Список активних слідів, який містить інформацію про всі об’єкти, що наразі знаходяться у процесі відслідковування.

Цей модуль забезпечує надійне відслідковування кількох об’єктів одночасно, ефективно керуючи інформацією про їх стан та динаміку руху у просторі зображення.

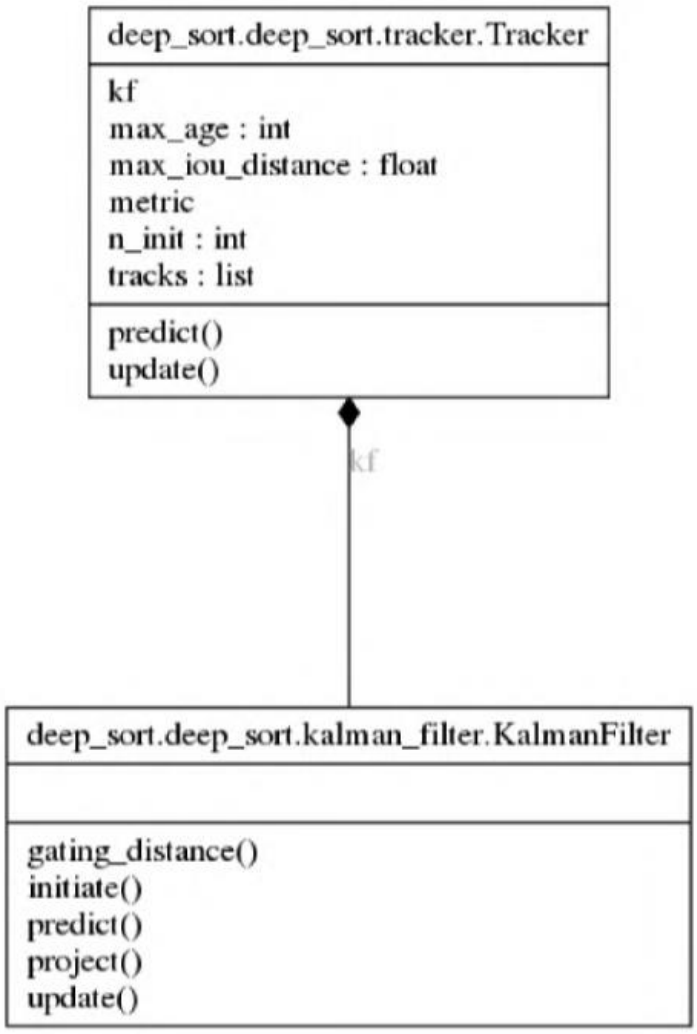


Рисунок 3.4 - Діаграма класів модуля відслідковування декількох об'єктів

Модуль візуалізації, зображений на рисунку 3.5, реалізовано через взаємодію двох класів. Його завданням є налаштування та відображення результатів роботи системи.

Основні характеристики, які виводяться поверх відеозапису, включають:

- Прямокутник, що обрамлює об’єкт: Він визначає межі об’єкта на кадрі та відображається у певному кольорі, який може змінюватися залежно від налаштувань системи або типу об’єкта.

- Унікальний ідентифікатор об’єкта: Відображається поряд із прямокутником, дозволяючи ідентифікувати конкретний об’єкт у процесі відстежування.

Модуль забезпечує зручну візуалізацію для аналізу результатів роботи системи, полегшуючи моніторинг і оцінку її ефективності.

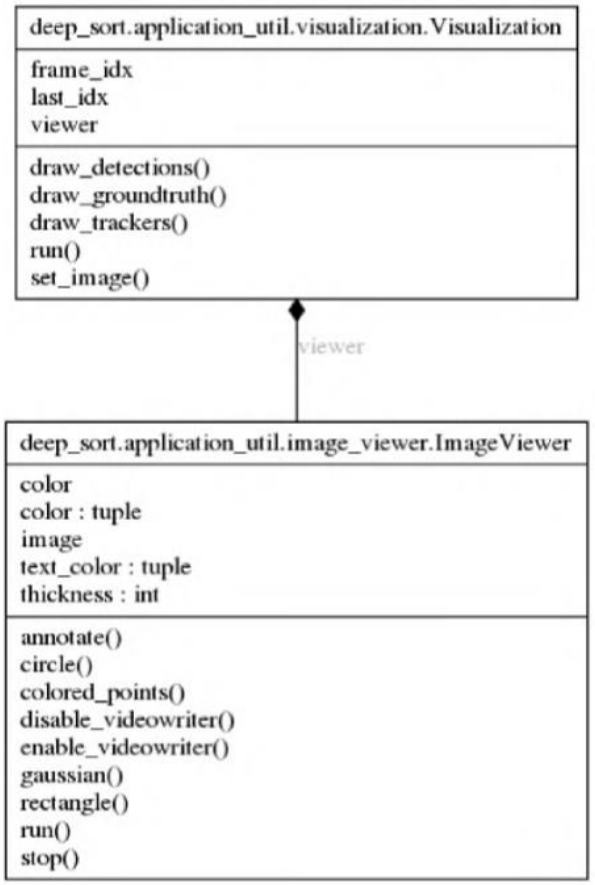


Рисунок 3.5 - Діаграма класів модуля візуалізації виявлення об'єктів

У разі, коли візуалізація результату роботи не є необхідною, існує модуль-заглушка, представлений на Рисунок 3.6

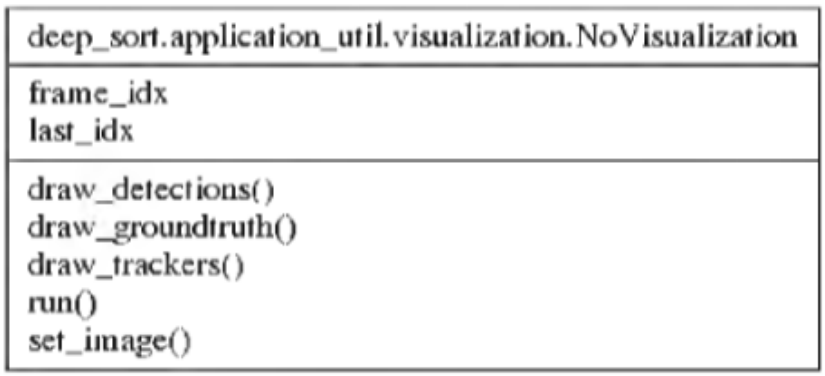


Рисунок 3.6 - Діаграма класів модуля-заглушки візуалізації виявлення об'єктів

Спроєктована діаграма пакетів, наведена на рисунку 3.7, демонструє взаємозв’язок між модулями системи. З діаграми видно, як основні компоненти інтегруються у головний виконавчий модуль, що координує роботу всієї системи.

Для головного виконавчого модуля створено консольний інтерфейс взаємодії, який надає такі можливості:

- Зчитування відеопослідовності з указаного місцезнаходження для подальшої обробки.

- Запис результатів роботи на вибраний носій для зберігання.

- Виведення результатів у режимі реального часу на монітор користувача.

- Налаштування порогового значення коефіцієнта впевненості, що визначає чутливість системи до виявлення нових об’єктів.

- Налаштування максимально допустимого часу відсутності об’єкта, після якого його слід вважається видаленим.

- Встановлення максимального коефіцієнта перекриття об’єктів, при перевищенні якого подальше визначення місцеположення об’єкта здійснюється виключно за допомогою фільтра Калмана.

- Задання мінімальної висоти об’єкта, що дозволяє зменшити кількість хибних спрацьовувань під час детектування.

Цей інтерфейс забезпечує гнучке налаштування системи, дозволяючи адаптувати її під конкретні умови експлуатації. Завдяки цьому користувач має

змогу оптимізувати роботу системи залежно від поставлених завдань та особливостей середовища.

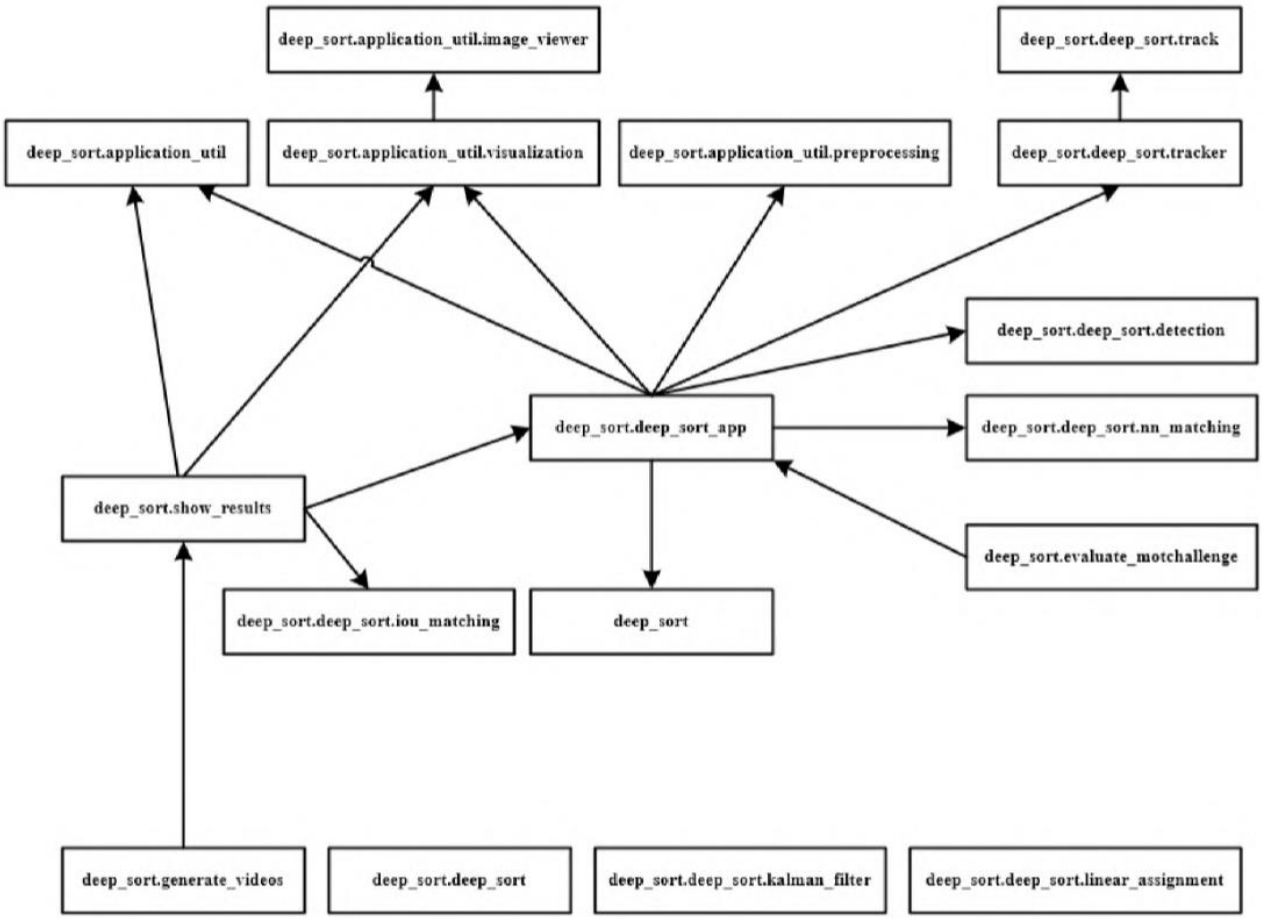


Рисунок 3.7 - Діаграма пакетів системи відслідковування переміщень з використанням алгоритма DeepSort

3.2 Функціональні особливості

У процесі детектування існуючих цілей розміри обмежувального прямокутника визначаються шляхом прогнозування його нового положення в наступному кадрі. Для цього будується матриця призначень, яка розраховується як значення відстані Жаккара між кожним виявленим і кожним прогнозованим обмежувальним прямокутником для поточних цілей. Завдання оптимального

зіставлення вирішується за допомогою Угорського алгоритму, описаного в розділі 2.

Крім того, мінімальне значення відстані Жаккара використовується для відхилення припущень, коли перекриття між об’єктами є меншим за встановлений поріг. Це дозволяє правильно обробляти ситуації, коли один об’єкт тимчасово перекриває інший. У таких випадках система відстежує лише перекриваючий об’єкт, а для перекритого об’єкта припущення не робляться.

При появі нового об’єкта або його остаточному зникненні з поля зору, унікальні ідентифікатори автоматично створюються чи видаляються. Якщо виявлено об’єкт із перекриттям, меншим за мінімальне значення, він розглядається як потенційно новий слід. Для створення нового сліду використовується розмір відповідного обмежувального прямокутника, а початкова швидкість встановлюється рівною нулю. Через те, що об’єкт раніше не спостерігався, коваріація його швидкості задається як високе значення, що відображає невизначеність.

Нові сліди повинні пройти випробувальний період, щоб зменшити кількість хибних спрацьовувань.

Сліди видаляються, якщо відповідний об’єкт не спостерігається протягом T кадрів. Це запобігає надмірному накопиченню слідів і помилкам, які можуть виникати при довгостроковому прогнозуванні місця об’єкта без підтвердження з боку детектора. Значення параметра T можна калібрувати залежно від умов експлуатації, таких як рівень охоплення відеоспостереження, важливість збереження слідів та вимоги до швидкодії системи.

Такий підхід забезпечує баланс між точністю відстежування і обчислювальною ефективністю, що є критично важливим для систем відеоспостереження.

3.3 Результати роботи програми

Була проведена перевірка швидкодії та ефективності системи за допомогою згенерованого масиву даних, який включав відеозаписи, зняті під різними кутами, з різною роздільною здатністю та масштабом. Додатково деякі відео були записані в русі, що ускладнювало роботу системи. Результати перевірки відображені на Рисунку 3.8. Алгоритм успішно виявив усіх людей та присвоїв їм унікальні ідентифікатори.

Рисунок 3.8 - Результат роботи програми. Помірна кількість людей, динамічна камера, наявність перекриття

У наборі даних були присутні моменти з великими скупченнями людей. Хоча такі ситуації не є типовими для реальних умов, коли йдеться про захищений об’єкт, ці уривки дозволяють перевірити масштабованість системи. На Рисунку 3.9 показано, як алгоритм намагається ідентифікувати кожну людину на платформі. Результати є задовільними, а швидкодія системи залишилася на необхідному рівні.

Рисунок 3.9 - Результат роботи програми. Велика кількість людей, динамічна камера, наявність перекриття

Алгоритм також було перевірено на даних, отриманих з вуличної камери, що найбільше відповідають сценарію спостереження за певним приміщенням (Рисунок 3.10). Результат виявився задовільним. Однак варто зазначити, що люди, які були частково в полі зору камери, не були виявлені. Це обмеження можна подолати за допомогою правильного проектування системи відеоспостереження, що забезпечить повне охоплення важливих ділянок з максимальною ефективністю.

3.4 Аналіз показників роботи алгоритму

Оцінка та порівняння методів багатоцільового відстеження є складною задачею з кількох причин. По-перше, на відміну від інших завдань, таких як зменшення рівня шуму в зображеннях, у цій області важко досягти ідеальних результатів. Частково видимі або перекриті об'єкти, відображення на дзеркальних поверхнях створюють труднощі при точному визначенні наявності цілі для спостереження. У деяких випадках, переглядаючи відеозаписи, навіть люди не можуть прийти до одностайного висновку, що ускладнює створення даних для порівняння. По-друге, велика кількість різних оціночних показників з вільними параметрами та неоднозначними визначеннями часто призводить до непослідовних кількісних результатів в науковій літературі. І нарешті, відсутність стандартизованих тестових даних і тренувальних наборів ускладнює неупереджене порівняння різних методів.

Одночасне відстеження великої кількості цілей є важливою проблемою в задачах опису та розуміння контексту сцени, де, на відміну від інших дослідницьких напрямів, до нещодавна не існувало стандартних бенчмарків і методів порівняння ефективності алгоритмів. Для вирішення цієї проблеми був розроблений тест MOTChallenge, який складається з трьох основних компонентів:

1. Публічно доступні набори даних, що дозволяють провести стандартизовану оцінку.

2. Загальноприйняті методи оцінки, які дають змогу порівнювати різні алгоритми.

3. Інфраструктура для додавання нових методів оцінки та наборів даних, що сприяє розвитку і покращенню технологій відстеження.

Результати роботи алгоритму Deep SORT у порівнянні з іншими алгоритмами, представленими в MOT Benchmark, наведені в Таблиці 3.1.

Таблиця 3.1

Результати роботи алгоритмів у MOT Benchmark

	MOTA↑	MOTP↑	MT↑	ML↓	ID↓	FM↓	FP↓	FN↓	Runtime↑
EAMTT	62.5	78.8	19.0%	34.9%	910	1321	4407	81223	12 Hz
POI	76.1	79.5	34.0%	20.8%	805	3093	5061	55914	10 Hz
SORT	79.8	79.6	25.4%	22.7%	1423	1835	8698	63245	60 Hz
Deep SORT	81.4	79.1	32.8%	18.2%	781	2008	12852	56668	40 Hz

Оцінювання проводиться по наступним критеріям:

Multi-object tracking accuracy, MOTA (↑): Загальна точність відстеження, що враховує FP, FN, ID

$$MOTA = 1 - \frac{\sum_t (m_t + fp_t + mme_t)}{\sum_t g_t} \tag{3.1}$$

де m_t – кількість пропущених об'єктів у кадрі t, fp_t – кількість хибнопозитивних (false positive) детекцій, mme_t – кількість помилок ідентифікації (mismatches), g_t – кількість об'єктів у кадрі t.

Multi-object tracking precision, MOTP (↑): Загальна точність визначення положення цілі

$$MOTP = \frac{\sum_{i,t} d_i^t}{\sum_i c_t} \tag{3.2}$$

де d_i^t – похибка в положенні для кожної відповідності між об'єктом і гіпотезою, c_t – кількість відповідностей у кадрі t.

Mostly tracked, MT (↑): кількість в більшості вистежених траєкторій. Тобто ціль має один і той же ідентифікатор принаймні протягом 80% її тривалості життя

Mostly lost, ML (↓) кількість в більшості втрачених траєкторій. Тобто ціль не відслідковується принаймні протягом 20% її тривалості життя.

Identity switches, ID (↓): кількість разів, коли ідентифікатор об’єкта помилково переходив іншому об’єкту.

Fragmentation, FM (↓): кількість разів, коли слід було прервано через відсутність виявлення.

False positive, FP (↓): Кількість помилкових виявлень.

False negative, FN (↓): Кількість пропущених виявлень.

Як видно з Таблиці 3.1, алгоритм Deep SORT відповідає сучасним критеріям ефективних систем розпізнавання образів, зберігаючи при цьому можливість використання у режимі реального часу. Це дозволяє алгоритму забезпечувати точне відстеження об'єктів без значних затримок, що є критично важливим для практичних застосувань, таких як відеоспостереження та автономне керування.

3.5 Інтеграція комп’ютерного зору в систему відеоспостереження

Для покращення системи відеоспостереження можна також інтегрувати базу даних співробітників для аутентифікації, де будуть зберігатися дані окремих співробітників компанії. Система буде розпізнавати людей, які заходять в приміщення, звіряти їх з базою даних, і, залежно від того, співробітник це чи ні, вона буде по різному реагувати.

Використання бази даних дає змогу централізовано зберігати інформацію про користувачів, їхні права доступу та логування дій. Якщо система побачить, що хтось знаходиться там, де не можуть знаходитися люди з таким рівнем доступу, то вона відразу сповіщає відповідну людину.

Важливо уточнити, що такі системи на даний момент є недосконалими і вони робитимуть помилки, тому повністю автоматизувати систему не вийде, концепт залишається такий самий, як і раніше. Є охоронець, який слідкує за тим, що відбувається на підприємстві, але система відеоспостереження, якщо знаходить

щось, на що треба звернути увагу, то вона сповіщає охоронця і він вживе необхідних заходів.

Також можна слідкувати за тим, хто мав доступ к яким робочим місцям, серверам або іншим важливим місцям та записувати це в базу даних. Це допоможе відокремити підозрюваних, якщо щось вийде з ладу, або якщо щось зникне.

На рис 3.10 можна побачити діаграму роботи такої системи.

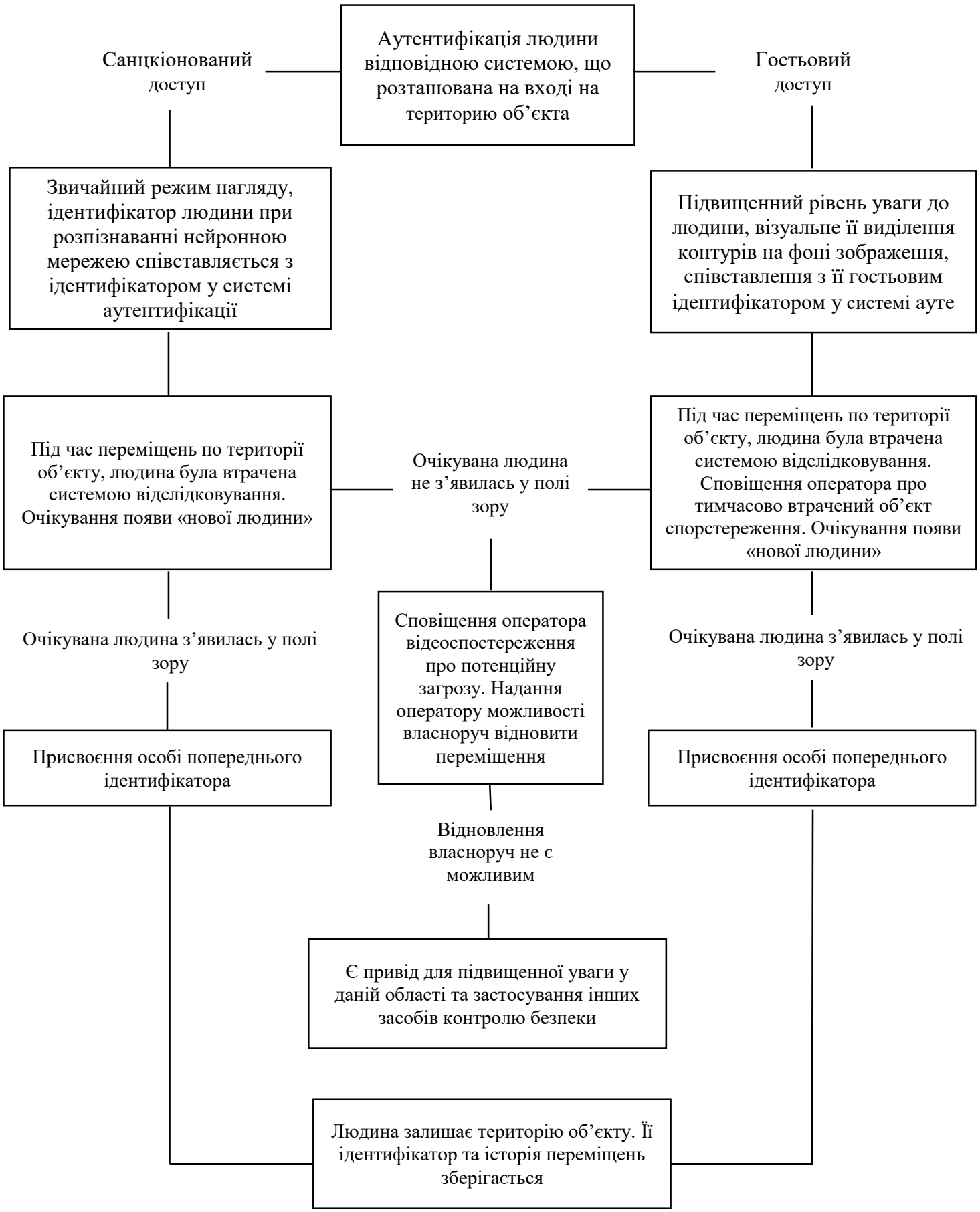


Рис 3.10 – діаграма функціонування системи відеоспостереження з ШІ

Також можна інтегрувати цю систему та систему контролю доступу. Це дозволяє поєднати моніторинг та контроль за вхідними/вихідними потоками людей. Наприклад, можна поєднувати відео з камери, що фіксує вхід людини, з її доступом до приміщення.

3.6 Створення системи відеоспостереження на підприємстві

Було створено систему відеоспостереження для офісу компанії (рис 3.11).

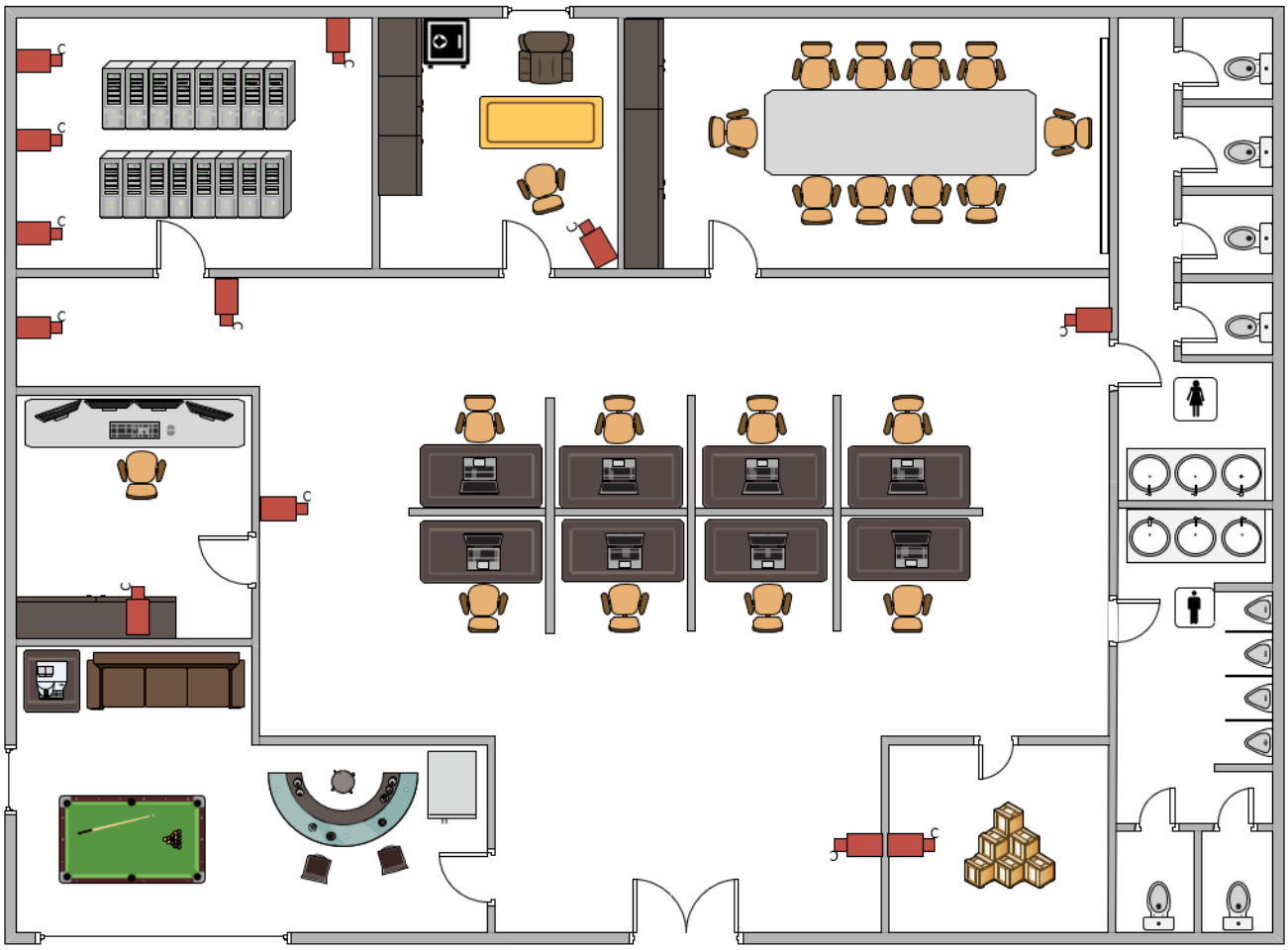


Рис 3.11 – офіс з системою відеоспостереження.

Архітектура системи відеоспостереження з комп'ютерним зором виглядає наступним чином:

- IP-камери: Камери високої роздільної здатності, що передають відеопотік у реальному часі.
- Сервер обробки даних: Обчислювальний сервер з GPU для роботи алгоритмів комп’ютерного зору.
- Програмне забезпечення відеоаналітики: Виконує обробку відео, детекцію та відстеження об'єктів.
- База даних: Зберігає дані про об’єкти, ідентифіковані обличчя, записи подій тощо.
- Інтерфейс користувача: Відображає результати аналізу для операторів системи безпеки.

Камери, які було виділено червоним кольором, розташовані в найважливіших місцях. Вони бачать усі двері, щоб бачити хто в які приміщення заходить. В технічному приміщенні треба спостерігати за обладнанням. У кабінках та у комнаті охоронця треба слідити за доступом к робочим місцям. В кабінеті начальника відділу важливі документу у сейфі. Особлива увага приділяється серверній кімнаті, окрім камери на вході, яка аутентифікує людину, всередені кімнати є 4 камери, які з усіх сторін бачать сервери, щоб кожна взаємодія була записана.

Система складається з 11 IP камер. Вони підключені до комп’ютера у кімнаті охорони. Доступ до кімнати охорони здійснюється за допомогою ключ карти, яка є тільки у уповноважених осіб. IP камери дозволяють легко масштабувати систему відеоспостереження, швидко інтегрувати її з іншими системами, вони мають більший функціонал. Вони більш вразливі для атак, тому треба пам’ятати про їх захист. Треба використовувати надійні паролі для доступу до системи, завжди використовувати шифрування, також можна зробити окрему локальну мережу із обмеженим доступом до інших сегментів мережі

Ця система забезпечує високий рівень захисту. Камери записують не тільки відео, але і хто куди заходив і мав доступ до робочого місця і коли. Вони розташовані ефективним чином, слідкуючи тільки за важливими місцями. Це,

разом з інтеграцію з базою даних дозволяє охоронцю ефективно слідкувати ситуацією в будинку, зменшує людський фактор, збільшує можливу територію спостереження та веде ретельне логування всіх важливих дій.

3.7 Оцінка ефективності системи відеоспостереження

Для визначення ефективності системи відеоспостереження можна використати цю формулу:

$$E = \sum_{i=1}^{N} W_i \cdot C_i \cdot A \cdot P \tag{3.3}$$

де E – ефективність системи

N – Кількість зон, на які поділено об’єкт

W_i –Вагомість і-ї зони (ймовірність того, що інцидент відбудеться в цій зоні). Сума всіх $W_i - 1$

C_i – Коефіцієнт покриття (частка покритої площі від загальної площи)

$$C_i = \frac{\text{Площа покриття камерами у зоні (м}^2\text{)}}{\text{Загальна площа зони (м}^2\text{)}} \tag{3.4}$$

A – доступність системи, тобто час, коли система працює.

$$A = \frac{\text{Час роботи системи (год)}}{\text{Загальний час спостереження (год)}} \tag{3.5}$$

P – відсоток успішної ідентифікації (однаковий для всіх камер, т.к. камери однакові і відеоряд аналізується однією програмою)

Розрахунок:

Загальна площа офісу: 181 м^2

Площа зон і покриття:

- Зона відпочинку: 18, покрито 0, вага: 0.025, $C_i = 0$
- Кімната охорони: 9, покрито 8, вага: 0.1, $C_i = 0.889$
- Серверна кімната: 14, покрито 13, вага: 0.35, $C_i = 0.929$
- Кабінет голови відділу 10, покрито 9, вага: 0.2, $C_i = 0.9$
- Конференц-зал: 20, покрито 0, вага 0.05, $C_i = 0$
- Туалети: 24, покрито 0, вага 0.025, $C_i = 0$
- Технічне приміщення: 7, покрито 6, вага: 0.1, $C_i = 0.857$
- Головне приміщення з кабінками: 79, покрито 69, вага: 0.15, $C_i = 0.873$

Доступність системи:

В ідеалі система повинна працювати 24 години на добу, але бувають збої, відключення електроенергії, при яких система простоює, поки вмикають генератори і т.д. Позначимо час роботи як 23 години 30 хвилин.

$$A = \frac{23.5}{24} = 0.979 \tag{3.6}$$

P візьмемо з таблиці 3.1, P = 0.81, кількість зон – 8, отримуємо:

$$E = \sum_{i=1}^{8} W_i \cdot C_i \cdot 0.979 \cdot 0.81 \tag{3.7}$$

$$0 + 0.0705 + 0.302 + 0.143 + 0 + 0 + 0.068 + 0.104 = 0.644 \tag{3.8}$$

Ефективність роботи системи відеоспостереження = 0.644, Але треба враховувати, що P – вірогідність ідентифікації порушника саме системою комп’ютерного зору, розрахувати ефективність за цією формулою, враховуючи охоронця може бути складною задачею, т.к. ця вірогідність залежить від людського фактору.

3.8 Висновок до третього розділу

У третьому розділі роботи було розглянуто процес моделювання та впровадження системи відеоспостереження для офісного приміщення з використанням сучасних технологій комп’ютерного зору. Основну увагу приділено архітектурі системи, її ключовим компонентам і можливостям інтеграції з іншими елементами безпеки.

Інтеграція технологій комп’ютерного зору, таких як алгоритм Deep SORT, дозволила реалізувати автоматичне виявлення, ідентифікацію та відстеження об’єктів у режимі реального часу. Важливим елементом стало використання фільтра Калмана, що підвищило стабільність і точність прогнозування траєкторії об'єктів.

Результати дослідження підтвердили ефективність системи, яка демонструє високу точність у виявленні об'єктів, низький рівень хибних спрацьовувань та можливість роботи в реальному часі. Це дозволяє використовувати систему не лише для забезпечення інформаційної безпеки, а й для моніторингу доступу до приміщення, контролю поведінки персоналу та автоматичного виявлення потенційних загроз.

Загалом, розроблена система відеоспостереження має значний потенціал для впровадження на підприємствах. Її функціональність може бути розширена за рахунок інтеграції з іншими засобами безпеки, впровадження додаткових сенсорів або використання алгоритмів аналізу поведінки для виявлення аномалій. Такий підхід забезпечує високий рівень адаптивності та надійності системи.

ВИСНОВОК

У дипломній роботі було досліджено, спроєктовано та реалізовано систему відеоспостереження з використанням сучасних алгоритмів багатоцільового відстеження об’єктів, що базуються на технологіях штучного інтелекту та комп’ютерного зору. Основною метою дослідження було підвищення ефективності та автоматизації відеоспостереження для забезпечення безпеки на підприємствах.

Основні досягнення роботи:

1. Теоретична база та аналіз технологій: У першому розділі роботи було проведено глибокий аналіз сучасних технологій комп’ютерного зору, алгоритмів відстеження об’єктів та їх застосування у системах відеоспостереження. Виявлено переваги та недоліки існуючих рішень, що дозволило сформулювати вимоги до розроблюваної системи.

2. Вибір і реалізація алгоритмів: У другому розділі було досліджено сучасні алгоритми, такі як Deep SORT, фільтр Калмана та Угорський алгоритм, які забезпечують точність відстеження об’єктів навіть у складних умовах, таких як перекриття або втрата об’єкта з поля зору. Впровадження цих алгоритмів у систему дозволило досягти високої точності та продуктивності роботи в реальному часі.

3. Проєктування та тестування системи: У третьому розділі було розроблено архітектуру системи, що складається з модулів детектування, відстеження, візуалізації та управління даними. Проведено тестування системи на стандартних наборах даних і реальних відеопотоках, яке підтвердило ефективність реалізованого підходу.

4. Інтеграція з іншими системами: Система спроєктована з можливістю інтеграції з іншими технологіями безпеки, такими як системи контролю доступу та хмарне зберігання даних, що підвищує її функціональність та масштабованість.

Запропонована система є універсальною і може бути адаптована для використання в різних галузях, включаючи промислові підприємства, офісні приміщення, громадські простори та транспортну інфраструктуру. Її переваги включають автоматизацію моніторингу, зниження залежності від людського

фактору, можливість прогнозування потенційних загроз та швидке реагування на інциденти.

У майбутньому розвиток системи може включати:

- Інтеграцію технологій розпізнавання осіб та аналізу поведінки для забезпечення глибшого розуміння ситуацій.

- Оптимізацію обчислювальних ресурсів для роботи на пристроях із обмеженою потужністю.

- Використання більш складних моделей машинного навчання для підвищення точності роботи.

- Розширення функціоналу за рахунок додавання нових модулів, таких як аналітика потоку людей або транспортних засобів.

Розроблена система відеоспостереження демонструє ефективне використання сучасних технологій штучного інтелекту для автоматизації процесів моніторингу та підвищення рівня безпеки. Проведене дослідження підтверджує актуальність впровадження таких систем у різні сфери діяльності, що дозволяє суттєво покращити їхню продуктивність і функціональність.

СПИСОК ДЖЕРЕЛ

1. Коваленко Ю. Забезпечення інформаційної безпеки на підприємстві – Україна: Економіка промисловості, 2010, 129с.

2. Відеоспостереження і охоронні системи.[Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.install.in.ua

3. Kruegle H. CCTV Surveillance: Video Practices and Technology 2nd Edition — UK: Butterworth-Heinemann 2006, — 672 c.

4. Відеокамери види та різниця [Електронний ресурс]. – Режим доступу: World Wide Web. – URL. – URL:http://www.bezpekacity.com.ua

5. A. Bewley Simple online and realtime tracking / A. Bewley, Z Ge, L. Ott, F. Ramos, B. Upcroft – US: IEEE International Conference on Image Processing (ICIP) – 2016.

6. C. Gao iCAN: Instance-Centric Attention Network for Human-Object Interaction Detection / C. Gao, Y. Zou, J. Huang – UK: British Machine Vision Conference – 2018, 23 c.

7. D. Stutz Understanding Convolutional Neural Networks – US: Computer Science and Natural Sciences, 2014, 69c.

8. C. Dicle The way they move: Tracking multiple targets with similar appearance /C. Dicle, M. Sznaier, O. Camps – US: International Conference on Computer Vision – 2013, 12 c.

9. F. Yu Poi: Multiple object tracking with high performance detection and appearance feature / F. Yu, W. Li, Q. Li, Y. Liu, X. Shi, and J. Yan – UK: ECCV. Springer- 2016, 42 c.

10. L. Leal-Taix e MOTChallenge 2015: Towards a Benchmark for Multi-Target Tracking /L. Leal-Taix'e, A. Milan, I. Reid, S. Roth, and K. Schindler – US: arXiv preprint – 2015, 26 c.

11. S. Ren Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks / S. Ren, K. He, R. Girshick, J. Sun – US: Advances in Neural Information Processing Systems – 2015, 73 c.

12. T. Lacey Tutorial: the Kalman Filter [Електронний ресурс] Режим доступу: World Wide Web. – URL:http://web.mit.edu/kirtley/kirtley/binlustuff/literature/control/Kalman%20filter.pdf .

13. H. W. Kuhn The Hungarian method for the assignment problem [Електронний ресурс] Режим доступу: World Wide Web. – URL: http://www.math.harvard.edu/archive/20_spring_05/handouts/assignment_overheads.pdf - 1955.

14. Відеоспостереження і охоронні системи.[Електронний ресурс]. –Режим доступу: World Wide Web: https://secur.ua.

15. Технології для відеоспостереження [Електронний ресурс]. – Режим доступу: World Wide Web: https://viatec.ua

16. Відеоспостереження, спеціалізована відео техніка.- [Електронний ресурс. – Режим доступу до ресурсу: https://www.bezpeka-shop.com.

17. Алтуєв М. Перспективи розвитку цифрового CCTV. – Миколаїв: Думки фахівців. Алгоритм Безпеки. – 2004. – № 5. - 57с.

18. Система відеоспостереження // Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.elvis.com.ua/ua/cctv-ua.html

19. Системи відеоспостереження -[Електронный ресурс]. – Режим доступу: World Wide Web. – URL: https://bezpeka.club/

20. Відеокамери види та різниця – [Електронний ресурс]. – Режим доступу: World Wide Web. – URL:http://www.bezpekacity.com.ua

21. Види систем відеоспостереження - [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://ohrana.ua/uk/stati-i-obzory/vidi-sistem-videonablyudeniya.html

22. Все про відеокамери– [Електронний ресурс].– Режим доступу: World Wide Web. – URL: https://pipl.ua

23. Інтегровані системи безпеки відеоспостереження [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://видеокамеры.com.ua/integrovani_sustemu_bezpeku/

24. Проект відеоспостереження [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://www.vostok.dp.ua/ukr/infa1/sistemy_vidyeonablyudeniya/psv/

25. Проектування системи відео спостереження [Електронний ресурс] Режим доступу – World Wide Web. – URL: https://видеокамеры.com.ua/proektyvannya_videosposterejennya/

26. Системи відеоспостереження для безпеки будинку і офісу - [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://worldvision.com.ua/videonabludenie/

27. Bhadeshia H. Neural Networks in Materials Science. – US: ISIJ International. – 1999. – 979 с.

28. Egmont-Petersen M. Image processing with neural networks – a review. – US: UCL Press. – 2002. – №35. – 2301 с.

29. Kalman R. A new approach to linear filtering and prediction problems. – UK: Journal of Basic Engineering. – 1960. – 45 с.

30. Roweis S. A, Unifying Review of Linear Gaussian Models. Neural Computation / S. Roweis, Z. Ghahramani. – UK: Cambridge University Press. 1961. – 345 с.

ДОДАТКИ

ДОДАТОК А

Презентаційні матеріали до магістерської роботи

на тему: «Система інтелектуального відеоспостереження для забезпечення інформаційної безпеки»

Слайд 1

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

РАЗВАЛЯЄВ ВОЛОДИМИР АНАТОЛІЙОВИЧ

Кваліфікаційна робота
здобувача освітнього ступеня «МАГІСТР»

Тема:

СИСТЕМА ІНТЕЛЕКТУАЛЬНОГО ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Спеціальність: 125 – Кібербезпека та захист інформації
Керівник: канд. техн. наук, доц. Андрій КОТЕНКО

Київ – 2025

Слайд 2

АКТУАЛЬНІСТЬ РОБОТИ

2

• зростання ролі відеоспостереження у фізичному та інформаційному захисті підприємств
• ризики несанкціонованого фізичного доступу до зон обробки даних
• необхідність автоматизації виявлення загроз за допомогою комп'ютерного зору та ШІ

Об'єкт дослідження:
процес захисту інформації на підприємстві.

Предмет дослідження:
система відеоспостереження з алгоритмами комп'ютерного зору для виявлення, ідентифікації та відстеження об'єктів.

Мета кваліфікаційної роботи:
підвищення рівня захисту інформації за допомогою системи інтелектуального відеоспостереження.

Слайд 3

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

3

1. РОЗДІЛ 1. Розглянуто роль відеоспостереження у кібербезпеці та захисті інформації.

2. РОЗДІЛ 2. Проаналізовано комп'ютерний зір, нейронні мережі, CNN, фільтр Калмана, Угорський алгоритм та Deep SORT.

3. РОЗДІЛ 3. Спроєктовано модель системи відеоспостереження з використанням ШІ та проведено оцінювання її ефективності.

4. ВИСНОВКИ. Сформовано практичні рекомендації щодо інтеграції інтелектуального відеоспостереження в систему інформаційної безпеки підприємства.

Слайд 4

ПЕРШИЙ РЕЗУЛЬТАТ

4

РОЛЬ ВІДЕОСПОСТЕРЕЖЕННЯ У КІБЕРБЕЗПЕЦІ

• відеоспостереження підсилює контроль фізичного доступу до інформаційних активів
• відеоархіви є доказовою базою для розслідування інцидентів
• інтеграція CCTV зі СКУД та сигналізацією формує багаторівневий захист

Слайд 5

5

ПЕРШИЙ РЕЗУЛЬТАТ

СТРУКТУРА СУЧАСНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

IP-камери
відеопотік, нічне бачення, огляд зон

Сервер/NVR
зберігання, архів, резервування

Відеоаналітика
детекція об'єктів, тривожні події

СКУД і сигналізація
реакція на події та контроль доступу

Слайд 6

6

ДРУГИЙ РЕЗУЛЬТАТ

КОМП'ЮТЕРНИЙ ЗІР У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

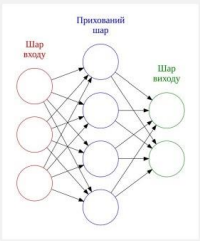
- виявлення та класифікація об'єктів у відеопотоці
- розпізнавання облич і контроль появи сторонніх осіб
- відстеження траєкторій руху у складних умовах

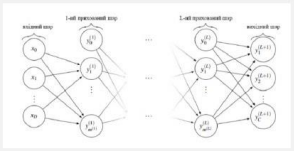
Слайд 7

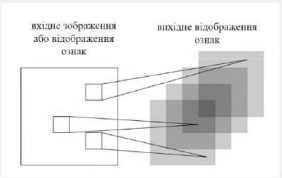
7

ДРУГИЙ РЕЗУЛЬТАТ

НЕЙРОННІ МЕРЕЖІ ТА CNN ДЛЯ АНАЛІЗУ ВІДЕО







- багатошарові перцептрони забезпечують формування ознак
- CNN виконує згортку, виділення локальних патернів і класифікацію
- глибоке навчання підвищує точність розпізнавання об’єктів

Слайд 8

8

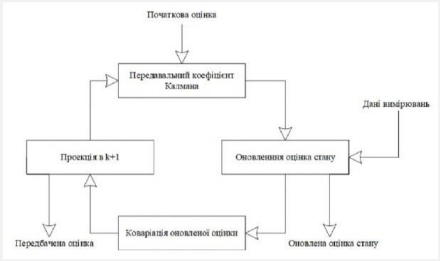
ДРУГИЙ РЕЗУЛЬТАТ

АЛГОРИТМИ БАГАТОЦІЛЬОВОГО ВІДСТЕЖЕННЯ

Deep SORT
- **поєднання детекції та повторної ідентифікації**
- **робота з кількома об’єктами у реальному часі**

Фільтр Калмана
- **прогноз координат**
- **уточнення стану цілі після нових вимірювань**

Угорський алгоритм
- **оптимальне зіставлення детекцій і треків**
- **зменшення помилок прив’язки**



Слайд 9

ДРУГИЙ РЕЗУЛЬТАТ

9

ВИЯВЛЕННЯ ЗАГРОЗ І ПОБУДОВА ТЕПЛОВИХ КАРТ

- автоматичне виявлення збройного нападу, нетипової поведінки та аномальних переміщень
- аналіз маршрутів і зон концентрації людей
- підтримка оперативних рішень служби безпеки

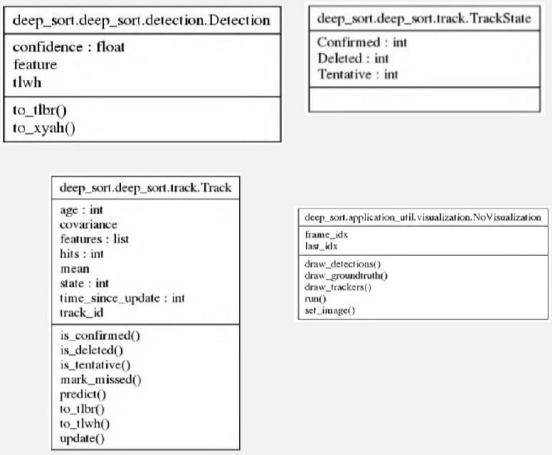
Слайд 10

ТРЕТІЙ РЕЗУЛЬТАТ

10

ПРОЄКТУВАННЯ СИСТЕМИ КОМП'ЮТЕРНОГО ЗОРУ

- **модуль виявлення об'єктів**
- **модуль контролю стану сліду цілі**
- **модуль роботи зі слідами**
- **модуль візуалізації та інтеграції з відеоспостереженням**

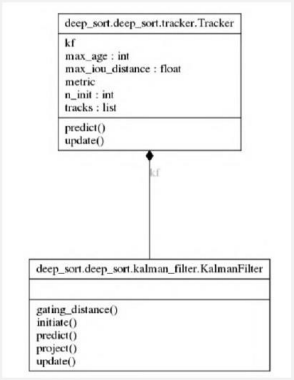


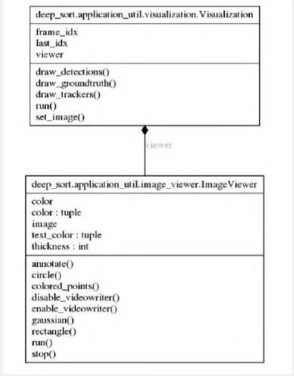
Слайд 11

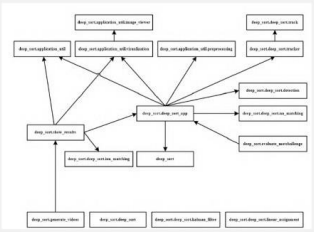
11

ТРЕТІЙ РЕЗУЛЬТАТ

АРХІТЕКТУРА МОДУЛІВ DEEP SORT







Пакетна структура забезпечує розподіл функцій між детекцією, трекінгом, асоціацією ознак та візуалізацією результатів.

Слайд 12

12

ТРЕТІЙ РЕЗУЛЬТАТ

РЕЗУЛЬТАТИ РОБОТИ ПРОГРАМИ

Програма демонструє здатність супроводжувати людей у відеопотоці за умов перекриття, динаміки сцени та значної кількості об’єктів.

Слайд 13

13

ТРЕТІЙ РЕЗУЛЬТАТ

ІНТЕГРАЦІЯ СИСТЕМИ НА ПІДПРИЄМСТВІ

- розміщення камер у зонах входу, коридорах, серверних і офісних приміщеннях
- об’єднання відеоспостереження зі СКУД та журналюванням подій
- підвищення оперативності реагування на інциденти

Оцінка ефективності: зниження ризику несанкціонованого доступу, розширення доказової бази та автоматизація моніторингу.

Слайд 14

14

ВИСНОВКИ

- проаналізовано роль відеоспостереження у забезпеченні інформаційної безпеки підприємства
- досліджено алгоритми комп’ютерного зору, Deep SORT, фільтр Калмана та Угорський алгоритм
- спроєктовано модель інтелектуальної системи відеоспостереження з функціями виявлення, ідентифікації та відстеження
- обґрунтовано доцільність інтеграції системи з технічними засобами охорони та СКУД

ДЯКУЮ ЗА УВАГУ!