

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

**КВАЛІФІКАЦІЙНА РОБОТА**

Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання  
засобів індивідуального захисту на виробничих об'єктах

Назва теми

Рівень вищої освіти другий (магістерський)

Галузь знань 12 «Інформаційні технології»

Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»

Шифр, назва

Освітня програма «Комп'ютерна інженерія та програмування»

Назва

Шифр КвРКІ 240121.19.01.14 ПЗ

Виконав здобувач II курсу, група КІ2м-24-1

Підпис

Ростислав МАРЧУК

Ініціали, прізвище

Керівник

д. техн. наук, професор

Науковий ступінь, учене звання

Підпис

Олег САВЕНКО

Ініціали, прізвище

Нормоконтролер

д. техн. наук, професор

Науковий ступінь, учене звання

Підпис

Сергій ЛИСЕНКО

Ініціали, прізвище

До захисту допускаю:  
завідувач кафедри КІС  
«01» травня 2026 р.

дата

Ольга ПАВЛОВА

Ініціали, прізвище

# ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти ДРУГИЙ (МАГІСТЕРСЬКИЙ)

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Завідувачка кафедри КІІС

  
Ольга ПАВЛОВА

“ 12 ” 01 2026 р.

## ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Марчуку Ростиславу Едуардовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

Керівник проекту (роботи) Савенко Олег Станіславович, д.т.н., проф.

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

Затверджена наказом ректора університету від 12.01.2026 р. № 6

2. Термін подання здобувачем роботи на кафедру 01.05.2026 р.

3. Вихідні дані до роботи Завдання на кваліфікаційну роботу

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

Метод автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

Проектування інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

Програмно-апаратна реалізація інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

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

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання « 12 » 01 2026 р.

**КАЛЕНДАРНИЙ ПЛАН**

№з/п	Назва етапів (розділів) дипломного проєкту (роботи)	Термін виконання етапів проєкту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	12.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	15.01.2026	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.02.2026	виконано
4	Робота над розділом 2 – розробка методу автоматичного розпізнавання ЗІЗ на виробничих об'єктах	01.03.2026	виконано
5	Робота над розділом 3 – проєктування інтелектуальної системи автоматичного розпізнавання ЗІЗ на виробничих об'єктах	29.03.2026	виконано
6	Робота над розділом 4 та оформлення пояснювальної записки згідно вимог	25.04.2026	виконано
7	Попередній захист ВКР	27.04.2026	виконано
8	Захист ВКР на засіданні ЕК	травень 2026 року	

Здобувач

  
Підпис

Ростислав МАРЧУК

Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи

  
Підпис

Олег САВЕНКО

Ім'я, ПРІЗВИЩЕ

## РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах.

Автор роботи: Марчук Ростислав Едуардович

Керівник роботи: Савенко Олег Станіславович

Пояснювальна записка: 80 с., 27 рис., 6 табл., 2 дод., 90 джерел.

*Комп'ютерна система, комп'ютерний зір, глибоке навчання, розпізнавання об'єктів, засоби індивідуального захисту, нейронні мережі, YOLO.*

Об'єктом дослідження є процеси автоматизованого відеомоніторингу та контролю використання засобів індивідуального захисту на виробничих об'єктах.

Предметом дослідження є методи, алгоритми та програмно-апаратні засоби розпізнавання об'єктів на зображеннях і відео, зокрема засобів індивідуального захисту, із використанням технологій комп'ютерного зору та глибокого навчання.

Метою кваліфікаційної роботи магістра є розроблення методу та інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах на основі методів комп'ютерного зору та глибокого навчання, що забезпечує підвищення рівня безпеки праці шляхом автоматизованого контролю дотримання вимог охорони праці в режимі реального часу.

Для розв'язання поставлених задач використовувалися методи порівняльного аналізу, методи комп'ютерного зору, глибокого навчання, метод попередньої обробки зображень та статистичні методи оцінювання ефективності.

Наукова новизна отриманих результатів:

– набув подальшого розвитку метод розпізнавання засобів індивідуального захисту на виробничих об'єктах;

– набула подальшого розвитку інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах, в якій на відміну від відомих використано комбінований підхід до

обробки відеопотоку на основі сучасних нейронних мереж типу YOLO та механізмів попередньої обробки зображень, що дозволяє підвищити точність детекції об'єктів в умовах складного освітлення, часткових перекриттів та різноманітних ракурсів;

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах.

Практична значимість отриманих результатів полягає у можливості впровадження розробленої системи на підприємствах, зокрема у сфері обробки та оздоблення меблевих фасадів, для автоматизованого контролю дотримання вимог охорони праці. Запропоноване рішення дозволяє зменшити ризик травматизму, підвищити виробничу дисципліну та оптимізувати роботу служб безпеки.

У ході роботи проведено аналіз предметної області, нормативних вимог та існуючих рішень у сфері відеомоніторингу й комп'ютерного зору. Встановлено, що традиційні підходи до контролю використання засобів індивідуального захисту мають обмеження, пов'язані з людським фактором, що зумовлює необхідність застосування інтелектуальних систем.

У другому розділі розроблено метод автоматичного розпізнавання засобів індивідуального захисту, який базується на використанні нейронних мереж для детекції об'єктів. Виконано формалізацію задачі, обґрунтовано вибір архітектури YOLO, описано процедури підготовки даних, навчання та оцінювання моделі. Запропоновано підхід до оптимізації моделі для роботи в режимі реального часу.

У третьому розділі розроблено архітектуру інтелектуальної системи, що включає підсистеми збору відеоданих, обробки та розпізнавання, а також візуалізації та сповіщення. Реалізовано програмно-апаратний комплекс, який забезпечує безперервний моніторинг виробничих процесів і автоматичне виявлення порушень вимог безпеки.

У четвертому розділі проведено експериментальне дослідження ефективності розробленої системи з використанням хмарного середовища та відкритого датасету. Отримані результати показали високі значення основних

метрик якості (Precision  $\approx 0.94$ , Recall  $\approx 0.92$ , mAP@0.5  $\approx 0.95$ ), що підтверджує ефективність запропонованого підходу. Візуальний аналіз і додаткові метрики також підтвердили здатність системи працювати в умовах, наближених до реального виробництва.

За темою роботи взято участь у Всеукраїнській науково-практичній WEB конференції аспірантів, студентів та молодих вчених та опубліковано тези доповіді: Марчук Р.Е., Лигун О.О. КОНЦЕПЦІЯ МЕТОДУ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ЗАСОБІВ ІНДИВІДУАЛЬНОГО ЗАХИСТУ НА ВИРОБНИЧИХ ОБ'ЄКТАХ. Матеріали ХІХ Всеукраїнської науково практичної WEB конференції аспірантів, студентів та молодих вчених (25-27 березня 2026 р.). – Кривий Ріг: Криворізький національний університет, 2026. с. 262-264 [90].

## ЗМІСТ

Скорочення та умовні позначки.....	5
Вступ.....	6
1 Аналіз проблеми та огляд існуючих рішень.....	9
1.1 Проблема контролю використання засобів індивідуального захисту (ЗІЗ) на виробничих.....	9
1.2 Нормативні вимоги до використання зіз у промисловості.....	13
1.3 Аналіз існуючих систем відеомоніторингу та комп'ютерного зору.....	16
1.4 Постановка задачі дослідження.....	24
1.5 Висновки до першого розділу.....	25
2 Метод автоматичного розпізнавання ЗІЗ.....	27
2.1 Загальна структура запропонованого методу.....	27
2.2 Формалізація задачі детекції засобів індивідуального захисту.....	29
2.3 Вибір архітектури нейронної мережі для вирішення задачі.....	34
2.4 Формування та підготовка датасету.....	36
2.5 Процедура навчання та валідації моделі.....	39
2.6 Метрики оцінювання ефективності.....	40
2.7 Висновки до другого розділу.....	43
3 Проектування та реалізація інтелектуальної комп'ютерної системи.....	45
3.1 Метод роботи та архітектура інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту на виробничих об'єктах.....	45
3.2 Апаратна складова інтелектуальної системи автоматизованого розпізнавання зіз на виробничих об'єктах.....	49
3.3 Програмна архітектура системи.....	54
3.4 Реалізація підсистеми збору відеоданих.....	55
3.5 Реалізація модуля розпізнавання ЗІЗ.....	57
3.6 Розроблення підсистеми сповіщень та логування порушень.....	58
3.7 Інтерфейс користувача та візуалізація результатів роботи інтелектуальної комп'ютерної системи автоматичного розпізнавання зіз на виробничих об'єктах.....	59
3.8 Висновки до третього розділу.....	62

4 Експериментальне дослідження та оцінювання ефективності інтелектуальної комп'ютерної системи автоматичного розпізнавання ЗІЗ на виробничих об'єктах .....	64
4.1 Організація експериментального дослідження.....	64
4.2 Опис середовища для проведення експерименту.....	65
4.3 Результати експериментів з розпізнавання зіз на виробничих об'єктах.....	69
4.4 Висновки до четвертого розділу .....	82
Висновки.....	84
Перелік джерел посилань.....	85
Додаток А .....	94
Додаток Б.....	

## СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ЗІЗ – засоби індивідуального захисту

ІІІ – штучний інтелект

НМ – нейронна мережа

CNN (Convolutional Neural Network) – згорткова нейронна мережа

DNN (Deep Neural Network) – глибока нейронна мережа

YOLO (You Only Look Once) – алгоритм детекції об'єктів у реальному часі

## ВСТУП

У сучасних умовах розвитку промисловості питання забезпечення безпеки праці набуває особливої актуальності. Незважаючи на наявність нормативно-правових вимог щодо використання засобів індивідуального захисту (ЗІЗ), на багатьох виробничих об'єктах спостерігаються порушення правил охорони праці, що призводить до підвищення рівня виробничого травматизму. Основною причиною таких порушень часто є людський фактор, недостатній контроль або неможливість постійного моніторингу великої кількості працівників.

Розвиток технологій комп'ютерного зору та глибокого навчання відкриває нові можливості для автоматизації контролю безпеки на виробництві. Інтелектуальні системи відеоаналізу дозволяють у режимі реального часу виявляти порушення використання засобів індивідуального захисту, зменшувати вплив людського фактора та підвищувати ефективність систем охорони праці.

У зв'язку з цим розроблення методів і систем автоматичного розпізнавання ЗІЗ є актуальним науково-практичним завданням, спрямованим на підвищення рівня безпеки працівників, зниження ризику травматизму та впровадження сучасних цифрових технологій у виробничі процеси.

Актуальність роботи полягає в розробці методу та інтелектуальної комп'ютерної системи для автоматичного розпізнавання ЗІЗ, спрямованих на підвищення рівня безпеки працівників, зниження ризику травматизму та впровадження сучасних цифрових технологій у виробничі процеси.

Метою кваліфікаційної роботи магістра є розроблення методу та інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах на основі методів комп'ютерного зору та глибокого навчання, що забезпечує підвищення рівня безпеки праці шляхом автоматизованого контролю дотримання вимог охорони праці в режимі реального часу.

Поставлена мета досягається розв'язанням таких основних завдань:

- провести огляд існуючих рішень та систем автоматизованого розпізнавання засобів індивідуального захисту на виробництві;
- виконати формалізацію задачі детекції засобів індивідуального захисту на зображеннях;
- обґрунтувати вибір методів і архітектури нейронної мережі для розпізнавання об'єктів;
- реалізувати процедуру навчання та валідації моделі з використанням сучасних методів глибокого навчання;
- провести експериментальне дослідження ефективності розробленої моделі з використанням відповідних метрик оцінювання;
- розробити архітектуру інтелектуальної системи, що включає підсистеми збору, обробки та візуалізації відеоданих;
- реалізувати програмно-апаратну систему автоматичного розпізнавання.

Об'єктом дослідження є процеси автоматизованого відеомоніторингу та контролю використання засобів індивідуального захисту на виробничих об'єктах.

Предметом дослідження є методи, алгоритми та програмно-апаратні засоби розпізнавання об'єктів на зображеннях і відео, зокрема засобів індивідуального захисту, із використанням технологій комп'ютерного зору та глибокого навчання.

Наукова новизна отриманих результатів:

- набув подальшого розвитку метод розпізнавання засобів індивідуального захисту на виробничих об'єктах;

- набула подальшого розвитку інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах, в якій на відміну від відомих використано комбінований підхід до обробки відеопотоку на основі сучасних нейронних мереж типу YOLO та механізмів попередньої обробки зображень, що дозволяє підвищити точність детекції об'єктів в умовах складного освітлення, часткових перекриттів та різноманітних ракурсів.

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

Практична значимість отриманих результатів полягає у можливості впровадження розробленої системи на підприємствах, зокрема у сфері обробки та оздоблення меблевих фасадів, для автоматизованого контролю дотримання вимог охорони праці. Запропоноване рішення дозволяє зменшити ризик травматизму, підвищити виробничу дисципліну та оптимізувати роботу служб безпеки.

Для розв'язання поставлених задач використовувалися методи порівняльного аналізу, методи комп'ютерного зору, глибокого навчання, метод попередньої обробки зображень та статистичні методи оцінювання ефективності.

За темою кваліфікаційної роботи опубліковано одну публікацію [90] у Збірнику наукових праць за матеріалами Всеукраїнської науково-практичної WEB конференції аспірантів, студентів та молодих вчених та опубліковано тези доповіді: Марчук Р.Е., Лигун О.О. Концепція методу автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах. Матеріали XIX Всеукраїнської науково-практичної WEB конференції аспірантів, студентів та молодих вчених (25-27 березня 2026 р.). – Кривий Ріг: Криворізький національний університет, 2026. с. 262-264.

## 1 АНАЛІЗ ПРОБЛЕМИ ТА ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

### 1.1 Проблема контролю використання засобів індивідуального захисту (ЗІЗ) на виробничих

Забезпечення безпеки працівників на виробничих об'єктах є одним із ключових завдань сучасних промислових підприємств. Незважаючи на впровадження систем управління охороною праці, значна частина виробничих травм пов'язана з неналежним використанням або повною відсутністю засобів індивідуального захисту (ЗІЗ). До таких засобів належать захисні каски, світловідбивні жилети, захисні окуляри, рукавиці, респіратори (рисунок 1.1) та інші елементи, які мінімізують ризики механічних, хімічних, термічних та інших небезпечних впливів [1].



а)



б)



в)



г)



д)

Рисунок 1.1 – Засоби індивідуального захисту, які використовуються на виробничих об'єктах: (а)захисна каска; б)світловідбивний жилет; в)захисні окуляри; г)захисні рукавиці; д)респіратори)

У реальних умовах виробництва контроль використання ЗІЗ переважно здійснюється вручну - відповідальними особами або службою охорони праці. Такий підхід має низку суттєвих недоліків: обмежене охоплення території, людський фактор, неможливість безперервного моніторингу, а також суб'єктивність оцінювання. На великих промислових об'єктах із значною кількістю працівників і складною інфраструктурою забезпечити постійний контроль фізично неможливо. Додатковою проблемою є динамічність виробничого середовища [2]. Працівники можуть тимчасово знімати каски або інші елементи захисту під час виконання певних операцій, переходів між зонами або через дискомфорт. Такі порушення часто залишаються непоміченими, що підвищує ризик травматизму. Особливо критичною є ситуація на будівельних майданчиках, у гірничодобувній промисловості, металургії та на об'єктах енергетики.

З розвитком технологій відеоспостереження підприємства масово впроваджують камери контролю доступу та моніторингу територій [3]. Проте в більшості випадків відеодані використовуються лише для ретроспективного аналізу інцидентів, а не для автоматичного виявлення порушень у реальному часі. Таким чином, наявна інфраструктура відеоспостереження не використовується

повною мірою для підвищення рівня промислової безпеки. Проблема полягає також у необхідності забезпечення високої точності розпізнавання ЗІЗ в умовах змінного освітлення, часткового перекриття об'єктів, різних ракурсів камери та великої кількості людей у кадрі. Система повинна працювати в режимі реального часу, мати низьку затримку обробки та бути придатною для інтеграції з існуючими інформаційними системами підприємства. На рисунку 1.2 (а, б, в) наведено приклади виробничих приміщень та складів, оснащених спеціалізованими камерами спостереження [4].



а)



б)



в)



г)

Рисунок 1.2 – Приклади оснащення виробничих об’єктів камерами спостереження [4]: (а)приклад встановлення камер ззовні; б)камери спостереження на виробничих ділянках; в)приклад оснащення камерами складських приміщень; г)приклади камер відеоспостереження, які можна використовувати на виробничих об’єктах)

Оснащення виробничих підприємств системами відеоспостереження є одним із ключових напрямів підвищення рівня промислової безпеки та контролю виробничих процесів. Встановлення камер відеоспостереження здійснюється як у внутрішніх приміщеннях (цехах, складах, технологічних зонах), так і на прилеглий території підприємства з метою забезпечення повного візуального покриття

критично важливих ділянок. Основним призначенням систем відеоспостереження є безперервний моніторинг виробничих процесів і дій персоналу, що дозволяє контролювати дотримання технологічних регламентів, правил охорони праці та внутрішніх інструкцій. Наявність відеофіксації сприяє своєчасному виявленню потенційно небезпечних ситуацій, аварійних випадків або порушень трудової дисципліни. Крім того, відеоархіви забезпечують можливість ретроспективного аналізу подій, розслідування інцидентів та формування доказової бази.

Сучасні системи відеоспостереження на підприємствах, як правило, інтегруються з відеореєстраторами, серверним обладнанням та програмним забезпеченням для централізованого управління відеопотоками. Такий підхід дозволяє здійснювати перегляд у режимі реального часу, зберігання відеоданих, налаштування параметрів доступу та інтеграцію з іншими підсистемами безпеки, зокрема системами контролю доступу та сигналізації.

Таким чином, оснащення виробництва камерами відеоспостереження створює технічну основу для підвищення рівня безпеки та ефективності управління підприємством. Разом із тим, у більшості випадків такі системи виконують переважно функцію пасивної фіксації подій, що зумовлює необхідність впровадження інтелектуальних методів автоматизованого аналізу відеоданих, зокрема для контролю використання засобів індивідуального захисту.

## 1.2 Нормативні вимоги до використання ЗІЗ у промисловості

Застосування засобів індивідуального захисту (ЗІЗ) у промисловості регламентується нормативно-правовими актами у сфері охорони праці, технічного регулювання та стандартизації. В Україні правові засади забезпечення безпечних умов праці визначаються Законом України «Про охорону праці» [5], відповідно до якого роботодавець зобов'язаний забезпечити працівників необхідними засобами індивідуального захисту та контролювати їх належне використання під час виконання виробничих завдань.

Вимоги до вибору, експлуатації та обліку ЗІЗ деталізуються у підзаконних нормативних актах, галузевих правилах охорони праці та державних стандартах [6-10]. Засоби індивідуального захисту повинні відповідати технічним регламентам та мати підтверджену відповідність вимогам безпеки. Зокрема, продукція цієї категорії підлягає оцінці відповідності відповідно до вимог технічних регламентів, гармонізованих із європейським законодавством.

На рівні міжнародного та європейського регулювання вимоги до ЗІЗ визначаються, зокрема, Регламентом (ЄС) 2016/425 про засоби індивідуального захисту [11], який встановлює вимоги до проектування, виробництва та введення в обіг такої продукції. Відповідність цим вимогам забезпечує належний рівень захисту від професійних ризиків та є підґрунтям для уніфікації стандартів безпеки. Окремими нормативними документами встановлюються мінімальні вимоги до забезпечення працівників конкретними видами ЗІЗ залежно від характеру небезпек: механічних, термічних, електричних, хімічних, біологічних тощо. Вибір засобів захисту здійснюється на основі оцінки професійних ризиків, яка повинна проводитися роботодавцем із урахуванням умов виробничого середовища, специфіки технологічних процесів та індивідуальних особливостей робіт.

Перелік діючих нормативних документів, які регулюють безпеку на виробничих об'єктах та використання ЗІЗ наведено у таблиці 1.1.

Таблиця 1.1 – Нормативно-правове регулювання використання засобів індивідуального захисту

№	Нормативний документ	Рівень регулювання	Основні положення щодо ЗІЗ
1	Закон України «Про охорону праці» № 2694-ХІІ від 14.10.1992 [5]	Національний	Встановлює обов'язок роботодавця забезпечувати працівників ЗІЗ та здійснювати контроль за їх використанням

Кінець таблиці 1.1

2	Кодекс законів про працю України [6]	Національний	Регламентує права працівників на безпечні умови праці
3	Технічний регламент засобів індивідуального захисту (Постанова КМУ № 761 від 27.08.2008, зі змінами) [7]	Національний	Визначає вимоги до відповідності, маркування та введення в обіг ЗІЗ
4	НПАОП 0.00-4.01-08 «Положення про порядок забезпечення працівників спеціальним одягом, спеціальним взуттям та іншими ЗІЗ» [8]	Галузевий	Встановлює порядок забезпечення, обліку та контролю використання ЗІЗ
5	ДСТУ EN 397:2017 (Захисні каски для промисловості) [9]	Національний стандарт	Визначає технічні вимоги до захисних касок
6	ДСТУ EN ISO 20471:2019 (Одяг сигнальний підвищеної видимості) [10]	Національний стандарт	Встановлює вимоги до сигнальних жилетів
7	Regulation (EU) 2016/425 on Personal Protective Equipment [11]	Європейський	Визначає вимоги до проектування, виробництва та сертифікації ЗІЗ у ЄС
8	ISO 45001:2018 Occupational health and safety management systems [12]	Міжнародний	Встановлює вимоги до систем управління охороною праці

Важливим аспектом є не лише забезпечення працівників необхідними засобами, а й організація контролю за їх використанням. Нормативні акти покладають на роботодавця обов'язок здійснювати нагляд за дотриманням працівниками вимог охорони праці, проводити інструктажі та навчання, а також застосовувати заходи реагування у разі порушень. Таким чином, відповідальність за використання ЗІЗ має як організаційний, так і технічний характер. У контексті сучасних виробничих систем актуалізується питання автоматизації контролю виконання нормативних вимог. Впровадження інтелектуальних комп'ютерних систем, здатних здійснювати автоматичне розпізнавання засобів індивідуального захисту на основі аналізу відеоданих, може розглядатися як інструмент підвищення ефективності виконання вимог чинного законодавства та зниження рівня виробничого травматизму.

### 1.3 Аналіз існуючих систем відеомоніторингу та комп'ютерного зору

Системи відеомоніторингу на сучасних промислових підприємствах є складовою комплексних рішень безпеки та управління виробничими процесами. Традиційні системи відеоспостереження включають мережеві або аналогові камери, відеореєстратори (NVR/DVR), серверне обладнання та програмне забезпечення для централізованого перегляду і зберігання відеоданих. Основною функцією таких систем є безперервна фіксація подій, архівування відеопотоків та забезпечення можливості ретроспективного аналізу інцидентів. Попри широке впровадження відеоспостереження, більшість традиційних систем працюють у пасивному режимі. Аналіз відео здійснюється оператором, що створює значне когнітивне навантаження та підвищує ризик пропуску порушень. Такий підхід є малоефективним у великих виробничих зонах із десятками камер і великою кількістю працівників. Приклад систем спостереження, де в основі є камери та оператор представлено на рисунку 1.3.

З розвитком інформаційних технологій сформувався напрям інтелектуального відеомоніторингу, що базується на методах комп'ютерного зору

та машинного навчання. Сучасні програмні комплекси здатні виконувати автоматичну детекцію руху, розпізнавання облич, підрахунок об'єктів, виявлення аномалій поведінки, а також класифікацію об'єктів у кадрі. Основою таких систем є алгоритми глибокого навчання, зокрема згорткові нейронні мережі (CNN), що демонструють високу точність у задачах детекції та сегментації об'єктів - рисунок 1.4.

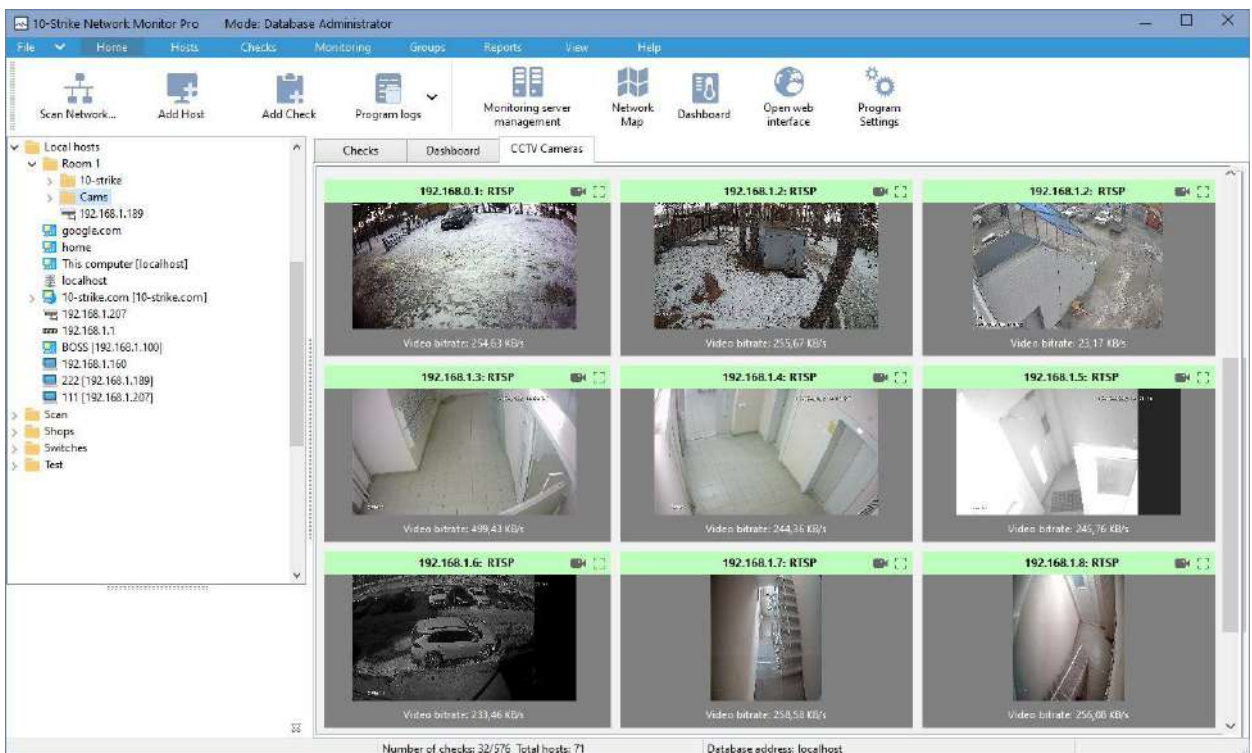


Рисунок 1.3 – Приклад роботи системи відеоспостереження на підприємстві (вікно оператора системи) [14]

У промисловому середовищі вже застосовуються рішення для контролю дотримання техніки безпеки, включаючи виявлення відсутності каски або сигнального жилета. Проте більшість наявних комерційних систем мають закриту архітектуру, високу вартість впровадження та обмежену гнучкість адаптації до специфіки конкретного підприємства. Крім того, їх ефективність може знижуватися в умовах складного освітлення, часткових перекриттів об'єктів та високої щільності персоналу в кадрі. Важливою тенденцією є використання edge-обчислень [19,20], коли обробка відеопотоку здійснюється безпосередньо на

периферійних пристроях, що дозволяє зменшити затримки передачі даних і навантаження на центральний сервер. Такий підхід є особливо актуальним для систем реального часу, орієнтованих на негайне реагування на порушення вимог безпеки.



Рисунок 1.4 – Приклад роботи згорткової мережі для задачі сегментації зображень

Доцільно зазначити, що інтелектуальні системи відеоаналітики для контролю промислової безпеки вже впроваджуються у практиці великих міжнародних компаній, які працюють у сферах енергетики, машинобудування, нафтогазової промисловості та логістики.

Одним із прикладів є діяльність компанії Siemens [13], яка у межах концепції цифрового підприємства впроваджує системи відеоаналітики для моніторингу виробничих процесів та підвищення рівня безпеки на промислових об'єктах.

Рішення компанії інтегрують відеоспостереження з аналітичними платформами та системами управління виробництвом.

Компанія Honeywell [14] реалізує комплексні системи промислової безпеки, які включають відеоаналітику для виявлення небезпечних ситуацій, контроль використання засобів індивідуального захисту та інтеграцію з системами реагування на інциденти. Подібні рішення застосовуються на об'єктах нафтохімічної та енергетичної галузей.

У сфері нафтогазовидобутку інтелектуальні системи відеомоніторингу впроваджуються компанією Shell [15], де відеоаналітика використовується для підвищення рівня промислової безпеки на виробничих майданчиках, включаючи контроль дотримання вимог щодо носіння касок, захисного одягу та іншого обладнання.

У виробничому секторі автомобілебудування подібні рішення застосовує BMW [16], де відеоаналітика використовується для оптимізації процесів та підвищення стандартів безпеки праці на заводах.

Також технологічні компанії, зокрема Hikvision [17] та Dahua Technology [18], розробляють спеціалізовані модулі відеоаналітики з використанням алгоритмів глибокого навчання для автоматичного виявлення відсутності засобів індивідуального захисту у кадрі.

Таким чином, практика провідних міжнародних компаній демонструє актуальність та ефективність застосування інтелектуальних систем комп'ютерного зору для забезпечення промислової безпеки. Разом із тим, більшість таких рішень є комерційними та закритими, що обумовлює доцільність розроблення власного методу та спеціалізованої інтелектуальної комп'ютерної системи, адаптованої до конкретних умов експлуатації.

У ході даного дослідження також було проаналізовано наукові публікації на предмет автоматичного розпізнавання засобів ЗІЗ на виробничих об'єктах.

Відтак, у [23] запропоновано інтелектуальну систему виявлення засобів індивідуального захисту в промислових середовищах із використанням глибоких нейронних мереж, реалізовану за концепцією edge computing. Обробка відеопотоку

здійснюється безпосередньо на периферійних пристроях, що дозволяє зменшити затримки, знизити навантаження на мережу та підвищити рівень захисту даних. Автори демонструють можливість роботи системи в реальному часі в умовах виробництва, що робить її практично придатною для інтеграції у промислову інфраструктуру.

Автори [24] розглядають концепцію «розумних» засобів індивідуального захисту, оснащених сенсорами та інтегрованих у систему інтелектуального моніторингу будівельної безпеки. У дослідженні акцент зроблено не лише на візуальному розпізнаванні, а й на зборі телеметричних даних (локація, фізіологічні показники, параметри середовища). Такий підхід розширює можливості контролю безпеки, однак виходить за межі виключно відеоаналітичних методів.

Автори [25] представили низьковартісну систему реального часу для перевірки використання ЗІЗ на промислових об'єктах, орієнтовану на застосування вбудованих edge-пристроїв. Система поєднує детекцію об'єктів і механізми трекінгу працівників, що дозволяє відслідковувати дотримання вимог безпеки протягом часу. Особлива увага приділяється зниженню вартості впровадження та забезпеченню стабільної роботи в умовах реального виробництва.

У магістерській роботі [26] досліджується застосування методів розпізнавання зображень для виявлення засобів безпеки в обробній промисловості. Окрім технічних аспектів, автори аналізують питання прийнятності систем відеомоніторингу персоналом і проблематику захисту приватності. Дослідження підкреслює важливість соціально-етичних аспектів впровадження інтелектуальних систем.

Автори [27] виконали систематичний огляд сучасних підходів до автоматичного контролю використання ЗІЗ на основі комп'ютерного зору. У роботі проаналізовано застосовані алгоритми (переважно архітектури сімейства YOLO та Faster R-CNN), використані датасети, рівень досягнутої точності, а також типові обмеження практичного впровадження, зокрема вплив освітлення, оклюзії та масштабованості систем. Автори окреслюють напрями подальших досліджень у цій галузі.

У [28] запропоновано гібридний підхід, що поєднує глибоку нейронну мережу для детекції об'єктів із модулем нечіткої логіки для прийняття остаточного рішення щодо відповідності вимогам безпеки. Такий підхід дозволяє зменшити кількість хибних спрацювань та адаптувати систему до невеликого обсягу навчальних даних. Особливістю роботи є орієнтація на реалізацію алгоритму на вбудованих пристроях. Додатково підкреслюється можливість гнучкого налаштування правил нечіткої логіки під конкретні умови експлуатації. Це забезпечує підвищення надійності системи в умовах змінного середовища та обмежених обчислювальних ресурсів.

Автори [29] запропонували фреймворк на основі YOLOv3 для автоматичної перевірки дотримання вимог щодо носіння касок і сигнальних жилетів на будівельних майданчиках. Система забезпечує класифікацію станів «безпечний» та «небезпечний» і може бути інтегрована з підсистемами оповіщення. Робота є одним із ранніх прикладів впровадження глибокого навчання для задач PPE compliance.

У [30] розроблено систему реального часу для контролю безпеки на будівельних майданчиках із використанням моделей глибокого навчання на базі YOLO-архітектури. Автори запропонували підхід, у якому детекція людини та елементів захисту доповнюється логікою перевірки відповідності кожного працівника вимогам безпеки. Робота демонструє високу швидкість і точність обробки відеопотоку. Додатково відзначається ефективність системи при роботі в умовах складного освітлення та часткових перекриттів об'єктів. Це підтверджує можливість її практичного застосування для автоматизованого моніторингу безпеки на реальних об'єктах.

Автори [31] розглядають застосування технологій комп'ютерного зору в інтелектуальних робототехнічних системах керування. Хоча дослідження не зосереджене безпосередньо на засобах індивідуального захисту, воно демонструє можливості інтеграції алгоритмів розпізнавання об'єктів у складні системи керування, що може бути використано при побудові кіберфізичних систем промислової безпеки.

Результати запропонованого вище аналізу у зведеному вигляді наведено у таблиці 1.2.

Таблиця 1.2 – Результати аналізу наукових публікацій на предмет автоматичного розпізнавання засобів ЗІЗ на виробничих об'єктах

№	Джерело	Що запропоновано
1	Gallo et al., 2022 (IEEE Access)	Edge-орієнтована система реального часу: відеопотік аналізується глибокою нейронною мережею без постійної передачі в хмару; акцент на економії трафіку, надійності та приватності; обробка здійснюється безпосередньо на вбудованому пристрої.
2	Rashidi et al., 2025 (Smart and Sustainable Built Environment)	Концепція «smart PPE»: використання сенсорів, інтегрованих у засоби захисту, для збору телеметричних даних (локація, висота, параметри середовища) у системі інтелектуального моніторингу безпеки.
3	Lema et al., 2023 (Journal of Real-Time Image Processing)	Низьковартісна система на embedded/edge-пристроях: поєднання детекції та трекінгу працівників, формування автоматичних тривог у разі відсутності ЗІЗ, орієнтація на промислові умови реального часу.
4	Hallonqvist & Cromsjö, 2021 (Thesis, Linköping University)	Дослідження застосування image recognition для виявлення засобів безпеки у виробництві з аналізом сприйняття персоналом та аспектів приватності.

Кінець таблиці 1.2

5	Vukicevic et al., 2024 (Artificial Intelligence Review)	Систематичний огляд методів комп'ютерного зору для PPE compliance: аналіз архітектур, датасетів, рівня точності та практичних обмежень впровадження.
6	Iannizzotto et al., 2021 (Expert Systems with Applications)	Гібридний підхід: поєднання глибокої нейронної мережі для розпізнавання та модуля нечіткої логіки для прийняття рішення щодо відповідності вимогам безпеки; орієнтація на embedded-пристрої.
7	Delhi et al., 2020 (Frontiers in Built Environment)	Фреймворк на базі YOLOv3 для автоматичної перевірки носіння касок і жилетів; класифікація станів SAFE/NOT SAFE та інтеграція з системою оповіщення.
8	Nath et al., 2020 (Automation in Construction)	Система реального часу на основі YOLO-архітектури: розпізнавання людини та елементів ЗІЗ із подальшою логікою перевірки відповідності кожного працівника вимогам безпеки.
9	Che et al., 2024 (arXiv)	Дослідження застосування комп'ютерного зору в інтелектуальних робототехнічних системах керування; розгляд загальних підходів до розпізнавання об'єктів.

З наведеного вище аналізу літератури можна побачити, що домінуючим підходом до автоматичного розпізнавання ЗІЗ є використання моделей глибокого навчання сімейства YOLO із реалізацією на edge-пристроях для забезпечення роботи в режимі реального часу. Водночас актуальними залишаються питання підвищення стійкості до складних умов експлуатації, зменшення хибних спрацювань та інтеграції систем у промислові інформаційні середовища.

#### 1.4 Постановка задачі дослідження

Аналіз сучасних наукових підходів і практичних рішень у сфері автоматичного розпізнавання засобів індивідуального захисту показав, що існуючі системи переважно базуються на моделях глибокого навчання сімейства YOLO та реалізуються у вигляді програмних модулів відеоаналітики. Водночас залишаються відкритими питання адаптації таких рішень до реальних умов виробничого середовища, забезпечення стабільної роботи в режимі реального часу, зменшення кількості хибних спрацювань та інтеграції з існуючою інфраструктурою підприємства. У зв'язку з цим виникає науково-прикладна задача розроблення методу та інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах, яка забезпечить надійний контроль дотримання вимог охорони праці в умовах реальної експлуатації.

Метою дослідження є підвищення ефективності контролю використання засобів індивідуального захисту шляхом створення методу автоматичної детекції та програмно-апаратної системи, здатної здійснювати обробку відеопотоку в режимі реального часу.

Для досягнення поставленої мети необхідно розв'язати такі задачі:

- 1) проаналізувати сучасні алгоритми комп'ютерного зору для задач детекції об'єктів та обґрунтувати вибір архітектури нейронної мережі;
- 2) сформулювати та підготувати навчальний набір даних, адаптований до умов виробничого середовища;
- 3) розробити метод автоматичного визначення наявності або відсутності засобів індивідуального захисту у працівників;
- 4) реалізувати програмну складову інтелектуальної системи з можливістю роботи на серверному або edge-обладнанні;
- 5) забезпечити інтеграцію системи з підсистемою сповіщення та журналювання подій;

б) провести експериментальне дослідження ефективності запропонованого методу за показниками точності, повноти, швидкодії та стійкості до змін умов зйомки.

Очікуваним результатом роботи є створення масштабованої інтелектуальної комп'ютерної системи, що забезпечує автоматичне виявлення порушень вимог безпеки в реальному часі та може бути інтегрована у кіберфізичну інфраструктуру сучасного виробництва.

## 1.5 Висновки до першого розділу

У першому розділі магістерської роботи було проаналізовано проблему контролю використання засобів індивідуального захисту на виробничих об'єктах та обґрунтовано її актуальність у контексті забезпечення промислової безпеки. Встановлено, що значна частина виробничих ризиків пов'язана з неналежним використанням або відсутністю ЗІЗ, а традиційні методи контролю, що базуються на людському факторі, не забезпечують достатньої оперативності та об'єктивності.

Проведений аналіз нормативно-правової бази показав, що законодавство України та міжнародні стандарти покладають на роботодавця обов'язок забезпечувати працівників засобами індивідуального захисту та здійснювати контроль за їх використанням. Це створює передумови для впровадження автоматизованих інтелектуальних систем, здатних підвищити ефективність нагляду за дотриманням вимог охорони праці.

Огляд існуючих систем відеомоніторингу засвідчив, що більшість промислових підприємств уже оснащені камерами спостереження, однак ці системи здебільшого виконують функцію пасивної фіксації подій. Сучасні дослідження у сфері комп'ютерного зору демонструють високу ефективність застосування моделей глибокого навчання, зокрема архітектур сімейства YOLO, для автоматичного розпізнавання засобів індивідуального захисту в режимі реального часу. Водночас залишаються актуальними питання адаптації таких

рішень до складних виробничих умов, зниження хибних спрацювань, забезпечення масштабованості та інтеграції з існуючою інфраструктурою.

На основі проведеного аналізу сформульовано постановку задачі дослідження, визначено мету, об'єкт і предмет роботи, а також окреслено основні наукові та прикладні завдання. Отже, подальші дослідження будуть спрямовані на розроблення методу та інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту, здатної забезпечити надійний контроль дотримання вимог безпеки на виробничих об'єктах у реальному часі.

## 2 МЕТОД АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ЗІЗ

### 2.1 Загальна структура запропонованого методу

Запропонований метод автоматичного розпізнавання засобів індивідуального захисту (ЗІЗ) призначений для виявлення фактів порушення вимог охорони праці на виробничих об'єктах шляхом аналізу відеопотоку в режимі реального часу. Метод базується на використанні алгоритмів комп'ютерного зору та глибокого навчання для детекції працівників і відповідних елементів індивідуального захисту. Метод автоматичного розпізнавання засобів індивідуального захисту (ЗІЗ) реалізується як послідовність взаємопов'язаних етапів обробки відеоданих, починаючи з отримання зображення та завершуючи формуванням рішення щодо відповідності вимогам безпеки.

Крок 1. Захоплення відеопотоку. На першому етапі здійснюється отримання відеопотоку з IP-камер, встановлених на виробничому об'єкті. Відеодані надходять у вигляді послідовності кадрів  $I_k$ , які передаються до обчислювального модуля для подальшої обробки. Якість цього етапу визначає точність усіх наступних процедур.

Крок 2. Попередня обробка зображення. Для забезпечення стабільної роботи алгоритмів комп'ютерного зору виконується попередня обробка кожного кадру. Вона включає нормалізацію освітлення для зменшення впливу змінних умов освітлення, масштабування зображення до розміру, оптимального для нейронної мережі, а також шумозаглушення для усунення артефактів відеосигналу. Метою цього етапу є підвищення якості вхідних даних та зменшення похибок детекції.

Крок 3. Детекція об'єкта «Працівник». На третьому етапі застосовується модель глибокого навчання для локалізації людей у кадрі. Зазвичай використовується архітектура типу YOLO або інша модель детекції об'єктів, яка визначає координати обмежувальних прямокутників для кожного виявленого працівника. Результатом є множина об'єктів  $P=\{p_1, p_2, \dots, p_n\}$ , що представляють працівників у кадрі.

Крок 4. Детекція елементів засобів індивідуального захисту. Після виявлення працівників у межах кожної області інтересу виконується пошук окремих

елементів ЗІЗ. Система визначає наявність або відсутність каски, сигнального жилета, а за потреби – інших засобів захисту (окуляри, рукавиці тощо). Детекція може здійснюватися або окремою моделлю, або багатокласовою моделлю, здатною одночасно розпізнавати людей і відповідні елементи ЗІЗ. Додатково застосовується перевірка просторової відповідності елементів ЗІЗ до конкретної особи для уникнення хибних спрацювань. Це дозволяє підвищити точність ідентифікації навіть у випадках часткового перекриття об'єктів або складного фону. У разі використання багатокласової моделі забезпечується оптимізація обчислювальних ресурсів і підвищення швидкодії системи.

Крок 5. Логічна перевірка відповідності. Для кожного працівника формується вектор відповідності  $Worker_i = \{Helmet, Vest, Gloves, Glasses\}$ , де кожен елемент набуває значення 1 (виявлено) або 0 (не виявлено). Далі виконується перевірка відповідності нормативним вимогам. Якщо набір виявлених засобів задовольняє визначений перелік обов'язкових елементів, працівник вважається таким, що дотримується вимог безпеки.

Крок 6. Формування рішення. На основі результатів логічної перевірки система формує підсумкове рішення для кожного працівника. Можливі два стани:

- 1) SAFE – вимоги дотримано;
- 2) VIOLATION – зафіксовано відсутність одного або кількох обов'язкових елементів захисту.

Крок 7. Генерація події та реагування. У разі виявлення порушення система автоматично генерує подію. Вона включає створення сигналу тривоги, збереження відповідного фрагмента відео та журналювання інформації про інцидент у базі даних. Це забезпечує можливість подальшого аналізу та оперативного реагування відповідальних осіб. Додатково система може надсилати сповіщення відповідальним особам через різні канали зв'язку (мобільні додатки, електронну пошту або месенджери). Передбачена також можливість інтеграції з іншими системами безпеки для централізованого моніторингу та управління інцидентами.

Графічне представлення методу зображено на рисунку 2.1.



Рисунок 2.1 – Графічне представлення методу автоматичного розпізнавання засобів індивідуального захисту (ЗІЗ)

## 2.2 Формалізація задачі детекції засобів індивідуального захисту

Для формалізації представлено у попередньому підрозділі методу автоматичного розпізнавання засобів індивідуального захисту (ЗІЗ) введемо наступні позначення:

Нехай:

$V(t)$  – відеопотік з камери спостереження на виробничому об'єкті.

$I_k$  -  $k$ -тий вхідний кадр відеопотоку з камери відеоспостереження,

$I_k \in R^{H \times W \times 3}$  (для RGB  $C=3$ ).

$P=\{p_1, p_2, \dots, p_n\}$  – множина виявлених працівників у кадрі.

$E=\{e_1, e_2, \dots, e_m\}$  - множина елементів ЗІЗ (захисний шолом, жилет, перчатки тощо.)

Загальна функціональна схема методу може бути представлена як композиція операторів (формула 2.1):

$$F = f_{decision} \cdot f_{logic} \cdot f_{detect} \cdot f_{pre} \cdot f_{input}, \quad (2.1)$$

де  $f_{input}$  – оператор отримання кадру;

$f_{pre}$  – оператор попередньої обробки;

$f_{detect}$  – оператор детекції працівників та ЗІЗ;

$f_{logic}$  – оператор перевірки відповідності;

$f_{decision}$  – формування кінцевого рішення.

Метод передбачає обробку кожного кадру відеопотоку окремо, з можливістю подальшої інтеграції механізмів трекінгу для підвищення стабільності розпізнавання. Далі кожен крок методу, запропонованого у розділі 2.1, представимо у формалізованому вигляді.

Крок 1. Захоплення відеопотоку.  $I_k \in R^{H \times W \times 3}$  -  $k$ -й кадр відеопотоку з камери відеоспостереження. Задача розпізнавання формулюється як задача багатокласової локалізації об'єктів (формула 2.2):

$$f_{detect}: I_k \rightarrow \{(b_i, c_i, s_i)\}, \quad (2.2)$$

де  $b_i$  - координати обмежувальної рамки;

$c_i \in person, helmet, vest, gloves$ ;

$s_i \in [0,1]$  - ймовірність належності до класу.

Крок 2. Попередня обробка зображення. Нехай  $I_k \in R^{H \times W \times C}$  - вхідний кадр відеопотоку (для RGB  $C=3$ ). Попередня обробка полягає у застосуванні послідовності перетворень, спрямованих на нормалізацію вхідних даних та підвищення стійкості детектора до змін освітлення, шумів та масштабу. Визначимо оператор попередньої обробки (формула 2.3):

$$I_k = f_{pre}(I_k), \quad (2.3)$$

де  $I_k$  - кадр після попередньої обробки.

Оператор  $f_{pre}$  подамо як композицію підоператорів (формула 2.4):

$$f_{pre} = f_{norm} f_{resize} f_{denoise} f_{clr}, \quad (2.4)$$

де  $f_{clr}$ - приведення до уніфікованого колірному простору (за потреби);

$f_{denoise}$  - фільтрація шумів;

$f_{resize}$  - масштабування до розміру, потрібного моделі;

$f_{norm}$ - нормалізація інтенсивностей/освітлення.

Також опційно (за потреби) можна виконати перетворення з RGB у інший простір (наприклад, HSV або YCbCr) для зменшення впливу освітлення:  $I_k^{(c)} = f_{clr}(I_k)$ . На практиці часто достатньо залишати RGB, якщо модель була попередньо навчена у RGB. Ще однією процедурою попередньої обробки (підготовки до навчання) є шумозаглушення. Для цього може виконуватись фільтрація кадру  $I_k^{(d)} = f_{denoise}(I_k^{(c)})$  або Гаусове згладжування (формула 2.5):

$$I_k^{(d)} = I_k^{(c)} * G_\sigma, \quad (2.5)$$

де  $G_\sigma$ - Гаусове ядро;

\* - операція згортки.

Також іноді досить корисним може стати масштабування, а саме переобчислення розміру кадру до  $H_0 \times W_0$ , які очікує нейромережева модель (наприклад,  $640 \times 640$ ) (формула 2.6):

$$I_k^{(r)} = f_{resize}(I_k^{(d)}), I_k^{(r)} \in R^{H_0 \times W_0 \times C}. \quad (2.6)$$

Нормалізація інтенсивностей пікселів є обов'язковим етапом попередньої обробки зображень перед подачею їх на вхід нейронної мережі. Вона забезпечує приведення значень яскравості до уніфікованого діапазону (наприклад,  $[0,1]$  або до нульового середнього та одиничної дисперсії), що сприяє стабільності процесу навчання та пришвидшує збіжність алгоритму оптимізації (формула 2.8). Крім того, нормалізація дозволяє узгодити розподіл вхідних даних із розподілом, на якому навчались попередньо натреновані моделі, що позитивно впливає на точність детекції. В умовах виробничого середовища, де можливі значні коливання освітлення, цей етап також зменшує чутливість моделі до змін яскравості та підвищує її узагальнювальну здатність. Побудову нормалізованого кадру виконуємо за формулою 2.7:

$$I_k = f_{norm}(I_k^{(r)}), \quad (2.7)$$

$$I_k = \frac{I_k^{(r)}}{255}. \quad (2.8)$$

Нормалізація за середнім та стандартним відхиленням (для кожного каналу) виконується за формулою 2.9:

$$I_k(x, y, c) = \frac{I_k^{(r)}(x, y, c) - \mu_c}{\sigma_c}, \quad (2.9)$$

де  $\mu_c$ ,  $\sigma_c$  - середнє та стандартне відхилення каналу  $c$  (обчислені на навчальному датасеті або прийняті стандартні для попередньо навчених моделей).

Таким чином, попередня обробка може бути описана наступним відношенням (формула 2.10):

$$f_{pre} : R^{H_x \times W_x \times C} \rightarrow R^{H_0 \times W_0 \times C}, \quad (2.10)$$

а результатом є кадр  $\tilde{I}_k$ , який подається на вхід модуля детекції  $P, E = f_{detect}(\tilde{I}_k)$ .

Крок 3. Детекція об'єкта «Працівник». Модель детекції можна описати за формулою 2.11:

$$P = f_d(I_k), \quad (2.11)$$

де:

$f_d$  - функція детекції об'єктів (у нашому випадку, ми будемо використовувати модель згорткової нейронної мережі YOLO);

$P \subset R^4$  - множина обмежувальних рамок для детекції працівників.

Крок 4. Детекція елементів засобів індивідуального захисту. Для кожного працівника  $p_i$  визначаємо функцію детекції елементів ЗІЗ (формула 2.12):

$$E_i = f_{pre}(I_k, p_i), \quad (2.12)$$

де:

$f_{pre}$  - функція детекції елементів ЗІЗ у межах області працівника.

Крок 5. Логічна перевірка відповідності. Для кожного працівника формується бінарний вектор відповідності (формула 2.13):

$$C_i = (c_{i1}, c_{i2}, \dots, c_{im}), \quad (2.13)$$

де  $c_{ij} = \begin{cases} 1, \text{ якщо } e_j \text{ виявлено} \\ 0, \text{ якщо } e_j \text{ не виявлено} \end{cases}$

Крок 6. Формування рішення.

Нехай  $R$  - множина обов'язкових елементів ЗІЗ  $R = \{Helmet, Vest, Gloves, Glasses\}$ .

Тоді рішення щодо наявності ЗІЗ у кожного окремого працівника можна визначити за формулою 2.14:

$$D_i = \begin{cases} SAFE, \text{ якщо } C_i \subseteq R \\ VIOLATION, \text{ якщо } C_i \text{ не виявлено} \end{cases} \quad (2.14)$$

Таким чином, загальну математичну модель системи виявлення ЗІЗ можна визначити за формулою 2.15:

$$Y_k = F(I_k) = D_1, D_2, \dots, D_n, \quad (2.15)$$

де  $F$  - композиція операторів, визначена за формулою 2.1.

### 2.3 Вибір архітектури нейронної мережі для вирішення задачі

Одним із ключових етапів розроблення методу автоматичного розпізнавання засобів індивідуального захисту є вибір архітектури нейронної мережі для задачі детекції об'єктів. Враховуючи специфіку задачі, а саме необхідність одночасного виявлення працівників та кількох елементів ЗІЗ у режимі реального часу, архітектура повинна забезпечувати баланс між точністю локалізації, швидкодією та можливістю оптимізації під обмежені обчислювальні ресурси. Сучасні підходи до детекції об'єктів поділяються на дві основні групи: двохетапні детектори та одноетапні детектори.

До двохетапних архітектур належать R-CNN, Fast R-CNN, Faster R-CNN. Їх принцип роботи полягає у генерації регіонів-кандидатів та подальшій класифікації та уточненні координат. Перевагами двохетапних архітектур є висока точність локалізації та добра робота з малими об'єктами. До недоліків можна віднести значну обчислювальну складність, меншу швидкість (зазвичай 5–10 FPS без

спеціальної оптимізації) та складність інтеграції у системи реального часу. Для промислових систем відеомоніторингу, де затримка прийняття рішення критична, такі моделі є менш доцільними [32].

Одноетапні детектори (SSD, YOLO, EfficientDet) виконують локалізацію та класифікацію об'єктів в межах одного проходу нейронної мережі. Вони характеризуються високою швидкістю, меншою затримкою, простотою інтеграції. У ході даної магістерської роботи було розглянуто такі архітектури: SSD (Single Shot Detector), EfficientDet, YOLOv5, YOLOv8. Результати порівняльного аналізу розглянутих архітектур наведено у таблиці 2.1:

Таблиця 2.1 – Результати порівняльного аналізу архітектур нейронних мереж

Архітектура	Тип	Швидкодія	Точність	Складність інтеграції
Faster R-CNN	Two-stage	Низька	Висока	Середня
SSD	Single-stage	Висока	Середня	Невисока
EfficientDet	Single-stage	Середня	Висока	Вища
YOLOv5 та v8	Single-stage	Дуже висока	Висока	Низька

Для задачі розпізнавання ЗІЗ у виробничих умовах визначальними є такі критерії, як швидкість обробки не менше 20 кадрів за секунду ( $FPS \geq 20$ ), можливість обробки декількох відеопотоків, підтримка оптимізації (квантизація, TensorRT), стійкість до часткових перекриттів об'єктів, здатність до багатокласової детекції.

З урахуванням вимог до системи автоматичного розпізнавання засобів індивідуального захисту як базову архітектуру детекції було обрано модель

сімейства YOLO. Такий вибір зумовлений необхідністю забезпечення високої швидкодії, мінімальної затримки обробки відеопотоку та можливості роботи в умовах обмежених обчислювальних ресурсів. YOLO належить до одноетапних детекторів об'єктів, що дозволяє виконувати локалізацію та класифікацію об'єктів за один прохід нейронної мережі. На відміну від двохетапних моделей, це значно зменшує обчислювальну складність і забезпечує стабільну роботу при обробці кількох відеопотоків.

Архітектура моделі складається з трьох основних частин: backbone (екстракція ознак), neck (багатомасштабна агрегація) та head (регресія координат і класифікація). Така структура дозволяє ефективно виявляти як працівників, так і окремі елементи ЗІЗ, зокрема каски та сигнальні жилети, навіть за умов часткових перекриттів.

Важливою перевагою YOLO є підтримка апаратного прискорення (CUDA, TensorRT), можливість квантизації моделі та масштабованість під різні обчислювальні платформи - від edge-пристроїв до серверів із GPU.

Таким чином, вибір архітектури YOLO обґрунтований її здатністю забезпечувати необхідний баланс між точністю детекції, швидкістю та можливістю оптимізації під промислові обчислювальні платформи, що робить її доцільною для реалізації інтелектуальної системи автоматичного контролю використання засобів індивідуального захисту [81].

## 2.4 Формування та підготовка датасету

Для навчання моделі детекції засобів індивідуального захисту використовується відкритий датасет Hard Hat Workers, розміщений на платформі Roboflow [82]. Даний набір даних призначений для задачі детекції працівників та захисних касок у виробничому середовищі. Він містить зображення реальних будівельних та промислових сцен із розміченими об'єктами класів "helmet" та "person". Розмітка виконана у форматі bounding boxes (обмежувальної рамки), що дозволяє

безпосередньо використовувати датасет для навчання моделей типу YOLO. Приклад тренувального зображення з датасету [82] наведено на рисунку 2.2:



Рисунок 2.2 – Приклад зображення для навчання нейронної мережі з датасету [82]

Загалом датасет налічує 7041 зображення, з яких 75% це зображення для навчання нейронної мережі, а 25% - для її тестування. Оскільки датасет має два класи – «helmet» та «person», це дасть можливість спростити нам задачу до бінарної класифікації об'єктів на зображенні, а саме людей, які одягнені в каску, і які ні.

Для попередньої підготовки датасету до навчання нейронної мережі, подамо його у формалізованому вигляді. Нехай навчальна вибірка подається як множина  $D$ , представлена формулою 2.16:

$$D = \{(I_i, Y_i)\}_{i=1}^N, \quad (2.16)$$

де:

$I_i$ -  $i$ -те зображення у датасеті;

$Y_i = (b_{ij}, c_{ij})$ - множина розмічених об'єктів на зображенні;

$b_{ij}$  - координати обмежувальної рамки на зображенні;

$c_{ij} \in \{person, helmet\}$ .

Для задачі даної магістерської роботи передбачено розширення класів шляхом подальшого додавання інших елементів ЗІЗ (наприклад, vest), однак базове навчання виконується на наявних класах датасету. Датасет [82] вже містить готову розмітку з обмежувальними рамками (bounding boxes). Однак перед використанням виконуються такі процедури:

- 1) Перевірка коректності координат (відсутність помилок та зміщень).
- 2) Візуальний контроль якості анотації.
- 3) Конвертація у формат, сумісний з обраною архітектурою (YOLO format).

Таким чином, анотація приводиться до вигляду:  $(X_{center}, Y_{center}, W, H)$ , нормалізованих відносно розмірів зображення. Для забезпечення стабільного навчання необхідно уникнути дисбалансу між класами. Нехай  $N_{person}$ ,  $N_{helmet}$  - кількість прикладів кожного класу.

У разі суттєвої різниці застосовуються: зважена функція втрат, штучне збільшення прикладів менш представленого класу, контроль частоти появи об'єктів. Балансування дозволяє зменшити ризик переорієнтації моделі на домінуючий клас.

Для підвищення узагальнювальної здатності моделі застосовується штучне розширення навчальної вибірки шляхом аугментації. Для покращення якості навчання моделі використовуються такі перетворення як горизонтальне віддзеркалення, масштабування, випадковий поворот ( $\pm 10-15^\circ$ ), зміна яскравості та контрасту, додавання гаусового шуму, зміна кольорового балансу тощо. Аугментація дозволяє моделі адаптуватися до різних умов освітлення, положення камери та часткових перекриттів.

## 2.5 Процедура навчання та валідації моделі

Процедура навчання моделі детекції засобів індивідуального захисту спрямована на формування стійкого та узагальнювального алгоритму, здатного коректно працювати в умовах реального виробничого середовища. Навчання здійснюється на підготовленому датасеті [82] із застосуванням архітектури YOLO, обраної у попередньому підрозділі. Перед запуском процесу навчання датасет поділяється на три підмножини: *train* - для оновлення ваг моделі, *validation* - для контролю перенавчання та *test* - для фінального оцінювання якості. Кожне зображення проходить етап попередньої обробки та аугментації відповідно до описаного раніше алгоритму.

Навчання моделі автоматичного розпізнавання засобів індивідуального захисту здійснюється з використанням підготовленого датасету та обраної архітектури YOLO. Метою навчання є формування параметрів нейронної мережі, які забезпечують мінімальну похибку детекції об'єктів і водночас високу узагальнювальну здатність моделі в умовах реального виробничого середовища.

Ініціалізація моделі здійснюється на основі попередньо натренованих ваг, отриманих у процесі навчання на великих відкритих датасетах. Нехай набір параметрів моделі позначається як  $\theta$ . Метою навчання є пошук таких параметрів  $\theta^*$ , які мінімізують функцію втрат. Для задачі детекції об'єктів використовується комбінована функція втрат (формула 2.17):

$$L = L_{box} + L_{cls} + L_{obj}, \quad (2.17)$$

де  $L_{box}$  - похибка локалізації (регресія координат обмежувальної рамки);

$L_{cls}$  - похибка класифікації;

$L_{obj}$  - похибка визначення наявності об'єкта (objectness score).

Використання *transfer learning* дозволяє скоротити час навчання, зменшити потребу у великому обсязі власних даних та підвищити точність розпізнавання. Процес навчання відбувається ітеративно протягом визначеної кількості епох. На

кожній ітерації модель отримує батч зображень, виконує пряме поширення для отримання прогнозів, після чого обчислюється функція втрат, яка враховує похибку локалізації об'єктів, похибку класифікації та достовірність визначення наявності об'єкта. На основі значення функції втрат виконується зворотне поширення помилки та оновлення ваг моделі за допомогою алгоритму оптимізації (наприклад, SGD або Adam).

Після завершення кожної епохи проводиться оцінювання моделі на валідаційній вибірці без оновлення параметрів. Це дозволяє відстежувати динаміку показників якості та своєчасно виявляти перенавчання. Якщо спостерігається зниження якості на валідаційних даних при покращенні результатів на навчальній вибірці, застосовуються методи регуляризації або ранньої зупинки навчання. Процедура навчання можна подати як задачу оптимізації (формула 2.18) з контролем узагальнювальної здатності:  $E_{val} = f(D_{val}, \theta)$ , де  $E_{val}$  - набір метрик якості (Precision, Recall, mAP):

$$\theta^* = \arg \min L(D_{train}, \theta), \quad (2.18)$$

Після завершення процесу навчання модель перевіряється на тестовій вибірці, що дозволяє отримати об'єктивні значення метрик ефективності та оцінити її готовність до впровадження в реальних умовах.

## 2.6 Метрики оцінювання ефективності

Оцінювання ефективності моделі детекції засобів індивідуального захисту є важливим етапом дослідження, оскільки дозволяє кількісно визначити якість розпізнавання об'єктів та обґрунтувати доцільність використання моделі в умовах реального виробництва. Для задачі детекції об'єктів застосовуються стандартні метрики: Precision, Recall, F1-score та mAP (mean Average Precision). Перед обчисленням метрик визначаються наступні величини [83]:

- True Positive (TP) - об'єкт коректно виявлено;

- False Positive (FP) - помилкове спрацювання;
- False Negative (FN) - пропущений об'єкт.

Коректність детекції визначається на основі показника IoU (Intersection over Union), який характеризує ступінь перекриття передбаченого та реального bounding box (обмежувальної рамки). Якщо значення IoU перевищує заданий поріг (наприклад, 0.5), детекція вважається правильною. Цей показник відіграє основну роль оцінці точності локалізації об'єктів.

Метрика Precision характеризує точність спрацювань моделі та визначається як відношення правильно виявлених об'єктів до загальної кількості виявлених об'єктів (формула 2.19). Високе значення Precision означає низьку кількість помилкових спрацювань, що є критично важливим для систем безпеки, оскільки зменшує кількість необґрунтованих тривог:

$$Precision = \frac{TP}{TP+FP}, \quad (2.19)$$

Метрика Recall характеризує повноту виявлення об'єктів та визначається за формулою 2.20. Високе значення Recall означає, що система рідко пропускає реальні порушення. У задачі контролю ЗІЗ ця метрика є особливо важливою, оскільки пропущене порушення може призвести до небезпечної ситуації:

$$Recall = \frac{TP}{TP+FN}, \quad (2.20)$$

Оскільки Precision та Recall часто перебувають у компромісному співвідношенні, для комплексної оцінки використовується F1-score - гармонійне середнє цих двох метрик (формула 2.21). F1-score дозволяє оцінити баланс між точністю та повнотою детекції:

$$F_1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}, \quad (2.21)$$

Для задачі багатокласової детекції застосовується показник Average Precision (AP), який визначається як площа під кривою Precision–Recall для конкретного класу. Обчислення AP здійснюється шляхом інтегрування залежності Precision від Recall при різних порогах впевненості моделі. Середнє значення по всіх класах називається mean Average Precision (mAP) та визначається за формулою 2.22:

$$mAP = \frac{1}{K} \sum_{k=1}^K AP_k, \quad (2.22)$$

де  $K$  - кількість класів. У практиці детекції об'єктів зазвичай використовуються наступні метрики:

- mAP@0.5 - при пороговому значенні IoU = 0.5;
- mAP@0.5:0.95 — усереднене значення для порогів IoU від 0.5 до 0.95.

mAP є узагальненою метрикою, що враховує як точність локалізації, так і якість класифікації.

У контексті системи автоматичного контролю використання засобів індивідуального захисту значення кожної з метрик набуває практичного інженерного змісту, оскільки безпосередньо впливає на безпеку персоналу та ефективність функціонування підприємства.

Високий показник Recall є критично важливим, оскільки він характеризує здатність системи виявляти всі фактичні порушення. Низьке значення Recall означає наявність значної кількості пропущених випадків відсутності засобів захисту (False Negative), що може призвести до травмування працівників або виникнення аварійних ситуацій. У системах промислової безпеки пріоритет зазвичай надається саме повноті виявлення, оскільки пропущене порушення є більш небезпечним, ніж зайве спрацювання. Тому під час налаштування моделі доцільно обирати такі порогові значення впевненості, які забезпечують максимально можливий рівень Recall без суттєвого погіршення інших показників.

Достатньо високий показник Precision необхідний для зменшення кількості хибних спрацювань (False Positive). Якщо система занадто часто генерує

необґрунтовані тривоги, це призводить до перевантаження відповідальних осіб, зниження довіри до автоматизованого контролю та ігнорування реальних попереджень. У довгостроковій перспективі надмірна кількість помилкових повідомлень знижує ефективність всієї системи безпеки. Таким чином, Precision безпосередньо впливає на експлуатаційну придатність та прийнятність рішення для підприємства.

Показник mAP є інтегральною характеристикою якості детекції. Він враховує не лише факт правильного виявлення об'єкта, але й точність локалізації bounding box та стабільність класифікації при різних порогах впевненості. Високе значення mAP свідчить про те, що модель демонструє збалансовану поведінку для всіх класів (наприклад, person та helmet) і не деградує при зміні умов оцінювання. Для систем промислового відеомоніторингу це означає стійкість до варіацій освітлення, масштабу та часткових перекриттів об'єктів.

F1-score виступає як узагальнений показник балансу між Precision і Recall. У випадках, коли необхідно знайти компроміс між повнотою виявлення та точністю спрацювань, F1-score дозволяє кількісно оцінити оптимальність налаштування моделі. Саме цей показник часто використовується для вибору оптимального порогу впевненості детектора.

З практичної точки зору оцінювання моделі повинно виконуватися комплексно, з аналізом усіх метрик одночасно. Наприклад, модель із високим Recall, але низьким Precision може бути непридатною для впровадження через надмірну кількість помилкових сигналів. Водночас модель із високим Precision, але низьким Recall є небезпечною, оскільки пропускає реальні порушення. Оптимальним є досягнення збалансованого рівня показників при стабільному значенні mAP.

## 2.7 Висновки до другого розділу

У другому розділі магістерської роботи розроблено та обґрунтовано метод автоматичного розпізнавання засобів індивідуального захисту на виробничих

об'єктах. Сформовано загальну структуру методу, визначено його функціональні модулі та описано послідовність обробки відеоданих від отримання кадру до формування рішення щодо наявності або відсутності порушення вимог охорони праці.

Також було виконано формалізацію задачі детекції засобів індивідуального захисту як задачі багатокласової локалізації об'єктів із використанням показника IoU для оцінювання коректності передбачень. Обґрунтовано вибір архітектури нейронної мережі сімейства YOLO як оптимальної з точки зору співвідношення точності, швидкодії та можливості апаратної оптимізації для роботи в режимі реального часу.

У пункті 2.4 описано процес формування та підготовки датасету на основі відкритого набору Hard Hat Workers, включаючи процедури перевірки анотацій, балансування класів та застосування аугментації даних. Визначено процедуру навчання та валідації моделі із використанням transfer learning та контролю перенавчання на валідаційній вибірці.

Також наведено систему метрик оцінювання ефективності моделі (Precision, Recall, F1-score, mAP), що дозволяє комплексно оцінити якість детекції та обґрунтувати придатність моделі до практичного впровадження.

Таким чином, у розділі 2 сформовано теоретичну та алгоритмічну основу інтелектуальної системи автоматичного розпізнавання засобів індивідуального захисту, що створює підґрунтя для експериментальної перевірки, оптимізації та подальшої практичної реалізації розробленого рішення.

### 3 ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ

3.1 Метод роботи та архітектура інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту на виробничих об'єктах

Архітектура інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту (ЗІЗ) визначає структуру взаємодії апаратних і програмних компонентів, необхідних для забезпечення безперервного моніторингу виробничих процесів та автоматичного виявлення порушень вимог охорони праці. Запропонована система орієнтована на роботу в режимі реального часу та може бути реалізована як у централізованій, так і в розподіленій (edge-based) архітектурі. Інтелектуальна комп'ютерна система складається з таких підсистем:

- 1) підсистема отримання відеоданих;
- 2) підсистема попередньої обробки кадрів;
- 3) підсистема детекції об'єктів;
- 4) підсистема логічної перевірки відповідності;
- 5) підсистема формування рішень та генерації подій.

Кожна з підсистем виконує визначені функції та взаємодіє з іншими компонентами через мережеві інтерфейси. Схема архітектури інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту (ЗІЗ) представлена на рисунку 3.1.

Підсистема відеоспостереження забезпечує отримання відеопотоку з виробничих зон. Він включає IP-камери, встановлені у ключових точках підприємства, таких як ділянки обробки матеріалів, фарбувальні камери, складські приміщення. Камери передають відеодані у вигляді потоку кадрів із використанням стандартних протоколів (RTSP, ONVIF).

Якість роботи всієї системи значною мірою залежить від характеристик відеоджерел, зокрема роздільної здатності, частоти кадрів та умов освітлення.

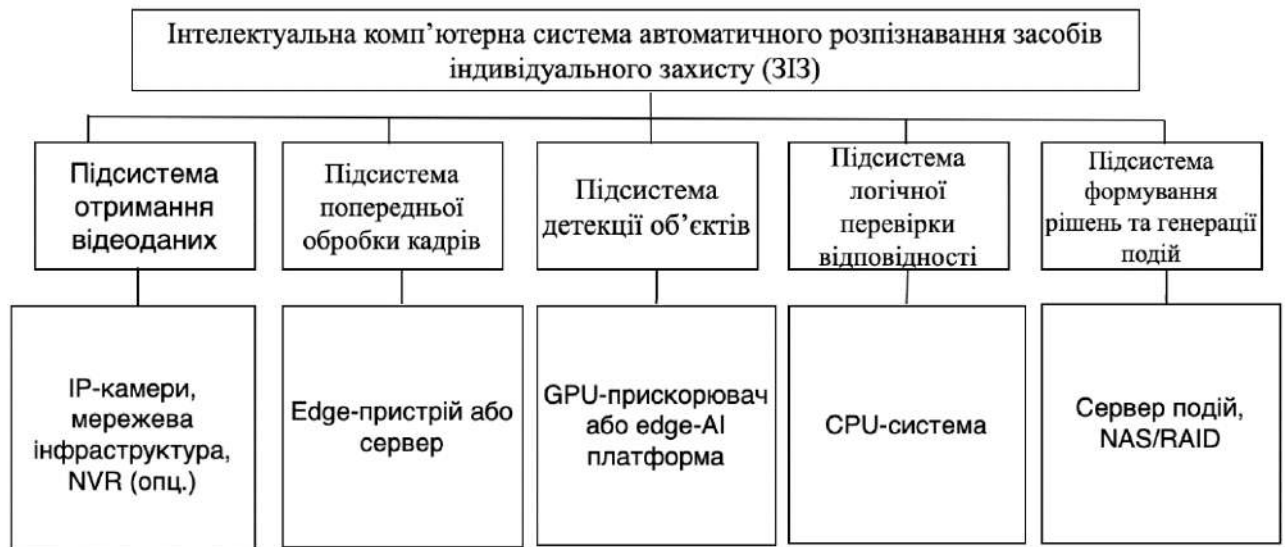


Рисунок 3.1 – Схема архітектури інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту (ЗІЗ)

Ця підсистема є ядром інтелектуальної системи та реалізує алгоритми комп'ютерного зору і машинного навчання. Вона включає такі модулі:

- модуль попередньої обробки, що виконує нормалізацію, масштабування та підготовку кадрів;
- модуль детекції об'єктів, який використовує нейронну мережу YOLO для виявлення працівників і елементів ЗІЗ;
- модуль логічного аналізу, що визначає відповідність наявних засобів захисту встановленим вимогам.

Обробка може виконуватися як на центральному сервері, так і на edge-пристроях, розташованих безпосередньо на підприємстві. Використання edge-архітектури дозволяє зменшити затримки та знизити навантаження на мережу.

Підсистема зберігання відповідає за накопичення та обробку інформації про події. Вона включає базу даних для збереження метаданих (час, тип порушення, координати об'єктів) та сховище відеоданих або фрагментів, що відповідають виявленим порушенням. Збережені дані можуть використовуватися для подальшого аналізу, формування звітності та навчання моделей. Важливою складовою є забезпечення швидкого доступу до даних для оперативного перегляду

інцидентів. Підсистема може підтримувати індексацію та фільтрацію записів за різними параметрами для зручності роботи користувачів. Також передбачається резервне копіювання даних для запобігання їх втраті. Для підвищення ефективності зберігання можуть застосовуватися методи стиснення відео та оптимізації структури бази даних. Крім того, система повинна враховувати вимоги безпеки та конфіденційності при роботі з інформацією.

Підсистема сповіщення та взаємодії є ключовим елементом забезпечення оперативного реагування на порушення. Вона забезпечує інтеграцію між аналітичним ядром системи та кінцевими користувачами або зовнішніми сервісами. Підсистема сповіщення та взаємодії забезпечує інформування відповідальних осіб про виявлені порушення. Вона реалізує генерацію тривожних повідомлень, відображення результатів у веб-інтерфейсі або SCADA-системі, передачу даних через API або повідомлення (наприклад, MQTT). Інтерфейс користувача дозволяє здійснювати моніторинг у реальному часі та перегляд історії подій.

Таким чином, метод функціонування інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту на виробничих об'єктах можна описати у вигляді послідовності наступних кроків:

- 1) отримання відеопотоку з камер зовнішнього спостереження на виробничому об'єкті;
- 2) передача отриманих кадрів до обчислювального модуля;
- 3) попередня обробка зображення;
- 4) детекція працівників і засобів захисту;
- 5) перевірка відповідності (наявність ЗІЗ на працівнику);
- 6) формування рішення про дотримання або недотримання правил техніки безпеки та охорони праці на виробничому об'єкті ;
- 7) збереження та надсилання сповіщення.

На рисунку 3.2 представлено графічне представлення методу у вигляді схеми алгоритму.



Рисунок 3.2 – Графічне представлення методу функціонування інтелектуальної системи автоматизованого розпізнавання ЗІЗ на виробничих об’єктах

Діаграма компонентів інтелектуальної системи автоматизованого розпізнавання ЗІЗ на виробничих об’єктах з функціональними модулями представлена на рисунку 3.3.

Запропонована архітектура має такі переваги: модульність і масштабованість, можливість роботи в реальному часі, адаптивність до різних виробничих умов та сумісність із наявними системами відеоспостереження.

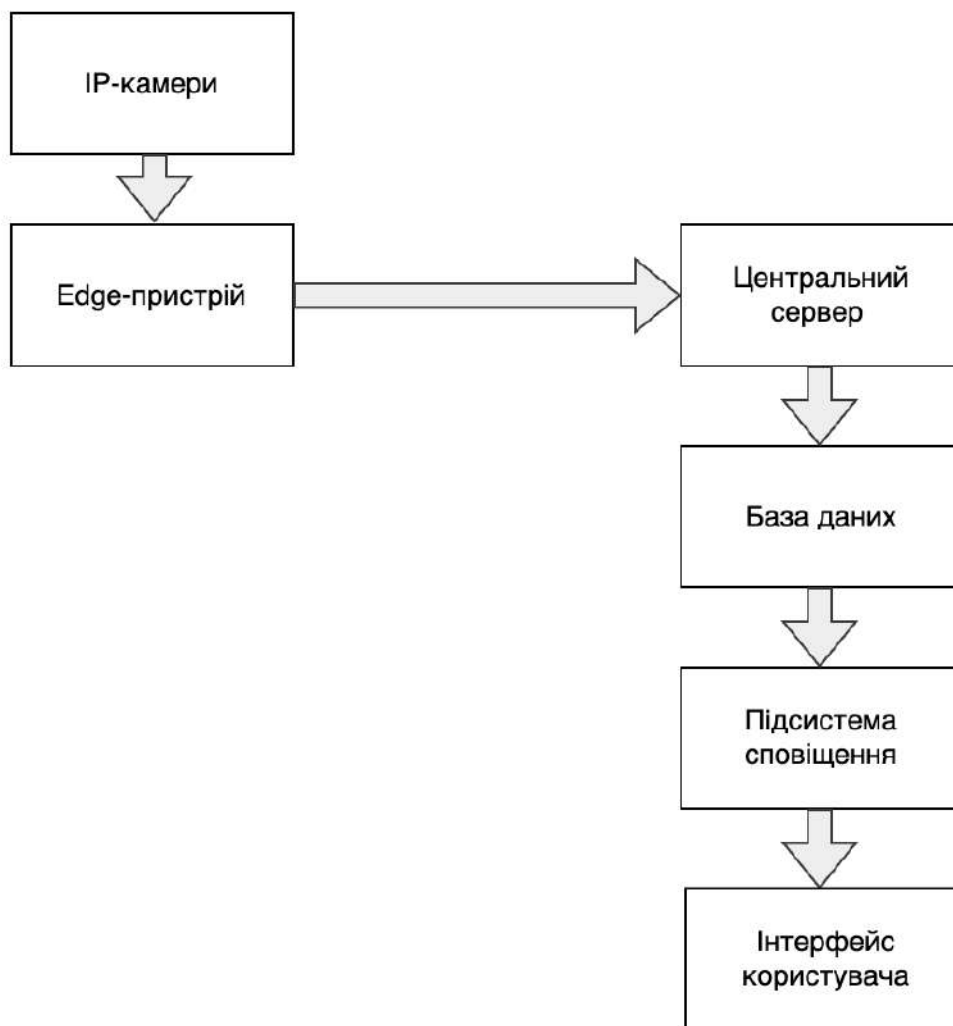


Рисунок 3.3 – Діаграма компонентів інтелектуальної системи автоматизованого розпізнавання ЗІЗ на виробничих об’єктах з функціональними модулями

Вона забезпечує повний цикл автоматичного контролю використання засобів індивідуального захисту - від отримання відеоданих до формування управлінських рішень. Вона є гнучкою, масштабованою та придатною для впровадження на підприємствах з різними умовами виробництва.

### 3.2 Апаратна складова інтелектуальної системи автоматизованого розпізнавання ЗІЗ на виробничих об’єктах

Апаратна складова інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту визначає можливості обробки відеоданих у режимі

реального часу та безпосередньо впливає на точність, швидкість та масштабованість системи. Запропонована архітектура передбачає використання як периферійних (edge), так і серверних обчислювальних ресурсів. Підсистема відеоспостереження є джерелом вхідних даних для всієї системи. Для забезпечення якісної детекції об'єктів необхідно використовувати сучасні IP-камери з такими характеристиками:

- 1) роздільна здатність не менше 1920×1080 (Full HD);
- 2) частота кадрів 25–30 FPS;
- 3) підтримка протоколів RTSP та ONVIF;
- 4) широкий динамічний діапазон (WDR) для роботи в умовах змінного освітлення;
- 5) наявність інфрачервоної підсвітки для роботи в умовах недостатнього освітлення;
- 6) захист корпусу (IP66/IP67) для експлуатації у виробничих умовах.

Правильне розміщення камер у ключових виробничих зонах (ділянки обробки, шліфування, фарбування) дозволяє мінімізувати зони перекриття та забезпечити достатню деталізацію об'єктів. Приклад промислової IP-камери відеоспостереження для моніторингу виробничих процесів наведено на рисунку 3.4 [85]. Важливим є також врахування кутів огляду та висоти встановлення камер для уникнення «сліпих зон». Додатково слід забезпечити належне освітлення або використання камер із підтримкою роботи в умовах низької освітленості. Оптимальна конфігурація розміщення обладнання сприяє підвищенню точності алгоритмів комп'ютерного зору та надійності всієї системи.

Edge-пристрої використовуються для виконання попередньої обробки даних та, за необхідності, первинної детекції об'єктів безпосередньо на місці встановлення камер. Це дозволяє зменшити затримки передачі даних, знизити навантаження на мережу, забезпечити автономність роботи системи. Приклад роботи для задач Інтернету речей представлено на рисунку 3.5 [86]. Типовими представниками таких пристроїв є платформи NVIDIA Jetson (Orin Nano, Xavier

NX) (рисунок 3.6) [87,88], які оснащені вбудованими GPU та підтримують технології CUDA і TensorRT.



Рисунок 3.4 – Промислова IP-камера відеоспостереження для моніторингу виробничих процесів [85]

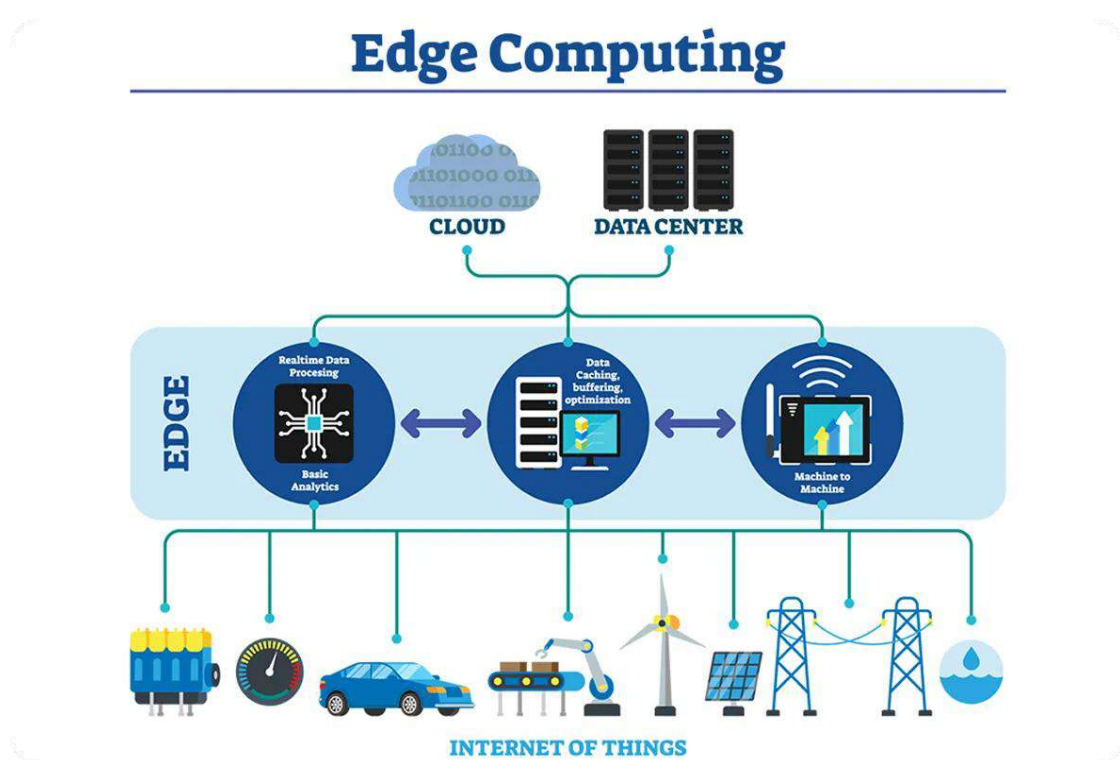
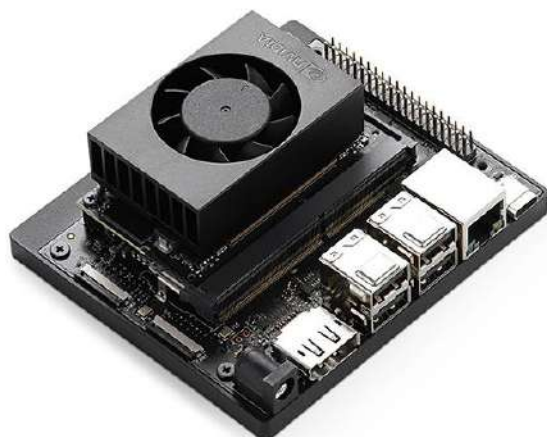
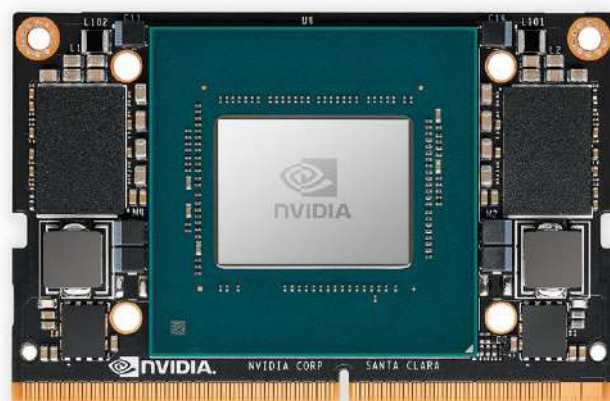


Рисунок 3.5 – Приклад роботи пристроїв периферійних обчислень для вирішення задач IoT [86]

Рекомендовані характеристики: GPU з підтримкою паралельних обчислень, оперативна пам'ять 8-16 GB, енергоефективність (споживання до 25 Вт), підтримка Linux-середовища. Edge-пристрої можуть виконувати як повну обробку відеопотоку, так і передавати результати детекції на центральний сервер.



а)



б)

Рисунок 3.6 – Edge-пристрої для обробки відеопотоку та виконання нейронних мереж: (а) Міні-комп'ютер NVIDIA Jetson Orin Nano Developer Kit; б) AI Суперкомп'ютер NVIDIA Jetson Xavier NX) [87-88]

Центральний сервер є ядром обчислювальної інфраструктури системи відеоаналітики. Він забезпечує координацію обробки даних та взаємодію між усіма компонентами системи. Центральний сервер виконує складні обчислювальні операції, пов'язані з аналізом даних, логічною перевіркою відповідності та збереженням інформації. Він також забезпечує масштабування системи при підключенні великої кількості камер. Типова конфігурація сервера включає багатоядерний процесор (Intel Xeon або AMD Ryzen 7/9), оперативну пам'ять не менше 32 GB, швидкі накопичувачі SSD (NVMe) для обробки даних, мережеві інтерфейси Gigabit Ethernet або вище. Сервер може виконувати централізовану обробку відеопотоків або взаємодіяти з edge-пристроями у розподіленій системі. Серверна інфраструктура для обробки та зберігання даних на прикладі NVIDIA GeForce RTX [89] представлена на рисунку 3.7.



Рисунок 3.7 – Серверна інфраструктура для обробки та зберігання даних на прикладі NVIDIA GeForce RTX [89]

Графічні процесори є ключовим компонентом системи, оскільки забезпечують ефективне виконання нейронних мереж. Використання GPU дозволяє значно підвищити швидкість обробки відеоданих та досягти роботи в реальному часі. Для серверної реалізації доцільно використовувати NVIDIA RTX 3060, 4060, A2000 або вище (рисунок 3.7) [89] з обсягом відеопам'яті не менше 8 GB та підтримкою CUDA та TensorRT. GPU забезпечує паралельну обробку даних, що дозволяє одночасно аналізувати декілька відеопотоків. У середньому один GPU здатен обробляти 4-6 потоків Full HD у режимі реального часу (залежно від моделі мережі). Апаратна складова системи може бути реалізована у двох основних конфігураціях:

- 1) Централізована архітектура - вся обробка виконується на сервері з GPU;

2) Розподілена (edge) архітектура - попередня обробка та частина детекції виконуються на edge-пристроях, а сервер здійснює агрегацію та аналіз результатів.

Комбінований підхід дозволяє досягти оптимального балансу між продуктивністю, затримками та вартістю системи. Таким чином, обрана апаратна платформа забезпечує необхідні умови для реалізації системи автоматичного розпізнавання засобів індивідуального захисту в режимі реального часу. Використання сучасних відеокамер, edge-пристроїв та GPU-прискорювачів дозволяє створити масштабовану, ефективну та надійну систему, придатну для впровадження на виробничих об'єктах.

### 3.3 Програмна архітектура системи

Програмна реалізація інтелектуальної системи автоматичного розпізнавання засобів індивідуального захисту виконана з використанням сучасних інструментів машинного навчання та комп'ютерного зору. Основною метою реалізації є створення програмного комплексу, здатного здійснювати обробку відеопотоку в режимі реального часу та автоматично виявляти порушення вимог безпеки. Система реалізована на мові програмування Python, що обумовлено широкою підтримкою бібліотек для роботи з нейронними мережами та обробки зображень. Для реалізації алгоритмів глибокого навчання використовується фреймворк PyTorch, а для детекції об'єктів бібліотека Ultralytics YOLO [81]. Архітектура програмної системи включає такі основні компоненти:

- 1) модуль захоплення відеопотоку;
- 2) модуль попередньої обробки зображення;
- 3) модуль детекції об'єктів;
- 4) модуль логічного аналізу;
- 5) модуль візуалізації та сповіщення.

Модуль захоплення відеопотоку забезпечує отримання кадрів із IP-камер або відеофайлів із використанням бібліотеки OpenCV. Отримані кадри передаються до

модуля попередньої обробки, де виконуються операції масштабування та нормалізації.

Модуль детекції реалізує завантаження попередньо навченої моделі YOLO та обробку кожного кадру. У результаті роботи модуля формується набір детекцій, що містить координати об'єктів, їх класи та рівень впевненості.

Модуль логічного аналізу виконує перевірку відповідності кожного виявленого працівника вимогам безпеки. Для цього визначається наявність необхідних елементів ЗІЗ у межах області працівника та формується рішення про відсутність або наявність порушення.

Модуль візуалізації забезпечує відображення результатів роботи системи у вигляді відеопотоку з нанесеними обмежувальними прямокутниками та підписами класів. У разі виявлення порушення система може генерувати повідомлення або записувати відповідні події.

Програмна архітектура системи представлена на рисунку 3.8.



Рисунок 3.8 – Програмна архітектура інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

### 3.4 Реалізація підсистеми збору відеоданих

Підсистема збору відеоданих є базовим компонентом інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту, оскільки забезпечує надходження первинної інформації для подальшої обробки та аналізу. Її основним завданням є отримання відеопотоку з різних джерел, його

попередня обробка та передача до наступних модулів системи в режимі реального часу.

У межах даної роботи реалізація підсистеми збору відеоданих здійснюється з використанням цифрових відеокамер, що підтримують передачу даних за протоколом RTSP (Real Time Streaming Protocol). Такий підхід дозволяє організувати безперервний потік відео з виробничих ділянок та забезпечує масштабованість системи при додаванні нових джерел відеосигналу. Архітектурно підсистема складається з наступних компонентів: модуля підключення до відеоджерела, модуля буферизації кадрів, модуля синхронізації потоків та модуля передачі даних. Модуль підключення відповідає за встановлення з'єднання з IP-камерою або іншим джерелом відео (локальний файл, веб-камера, мережевий стрім). Для цього використовуються стандартні програмні інтерфейси, зокрема бібліотека OpenCV, яка дозволяє здійснювати захоплення відеопотоку незалежно від типу джерела. Отриманий відеопотік розбивається на окремі кадри, які зберігаються у буфері. Буферизація необхідна для забезпечення стабільної роботи системи, особливо в умовах нестабільного мережевого з'єднання або нерівномірного навантаження на обчислювальні ресурси. Розмір буфера визначається експериментально та залежить від частоти кадрів (FPS) і пропускної здатності системи. Наступним етапом є синхронізація та нормалізація відеоданих. На цьому етапі виконується приведення кадрів до єдиного формату, масштабу та роздільної здатності, що є необхідним для коректної роботи модулів комп'ютерного зору. Зокрема, виконується зміна розміру зображення, перетворення кольорового простору та нормалізація піксельних значень. Для забезпечення роботи в реальному часі використовується механізм потокової обробки даних, при якому кожен кадр передається до наступного модуля одразу після його отримання. Це дозволяє мінімізувати затримки та забезпечити оперативне реагування системи на події, що відбуваються у виробничому середовищі. Особливу увагу приділено питанням надійності та відмовостійкості підсистеми. У разі втрати з'єднання з джерелом відео передбачено механізм

автоматичного перепідключення. Крім того, реалізовано контроль цілісності потоку, що дозволяє виявляти пошкоджені або пропущені кадри.

### 3.5 Реалізація модуля розпізнавання ЗІЗ

Підсистема обробки та розпізнавання є ключовим функціональним компонентом інтелектуальної системи, оскільки саме на цьому етапі здійснюється аналіз відеоданих та автоматичне виявлення засобів індивідуального захисту. Основною задачею підсистеми є обробка вхідних кадрів, детекція об'єктів та класифікація їх належності до визначених класів. В основі реалізації підсистеми використано сучасні методи глибокого навчання, зокрема архітектуру YOLO (You Only Look Once), яка забезпечує високу швидкість та точність детекції об'єктів у реальному часі. Вибір цієї архітектури обумовлений її здатністю виконувати одночасно локалізацію та класифікацію об'єктів в одному проході нейронної мережі, що є критично важливим для систем відеомоніторингу. Обробка кожного кадру виконується послідовно та включає декілька етапів. На першому етапі кадр, отриманий від підсистеми збору відеоданих, проходить попередню обробку, яка включає зміну розміру до фіксованого формату (наприклад, 640×640 пікселів), нормалізацію значень пікселів та перетворення у формат, сумісний із вхідними вимогами нейронної мережі. На наступному етапі виконується безпосередньо детекція об'єктів за допомогою навченої моделі. У результаті роботи нейронної мережі формується набір передбачень у вигляді обмежувальних рамок (bounding boxes), ймовірностей належності до класів («helmet», «head», «person») та відповідних значень впевненості (confidence score). Для підвищення якості результатів застосовується процедура постобробки, зокрема алгоритм Non-Maximum Suppression (NMS), який дозволяє усунути дублювання детекцій та залишити лише найбільш релевантні обмежувальні рамки. Це забезпечує більш точну локалізацію об'єктів і зменшує кількість хибних спрацювань.

Додатково реалізовано логіку аналізу відповідності вимогам безпеки. Зокрема, виконується перевірка співвідношення між об'єктами класів «head» та

«helmet». У випадку, якщо для виявленої голови відсутня відповідна каска, система ідентифікує це як порушення використання засобів індивідуального захисту.

### 3.6 Розроблення підсистеми сповіщень та логування порушень

Підсистема візуалізації та сповіщення є завершальним компонентом інтелектуальної системи автоматизованого розпізнавання засобів індивідуального захисту та забезпечує представлення результатів обробки відеоданих користувачу, а також оперативне інформування про виявлені порушення. Основною функцією підсистеми є відображення результатів детекції у зрозумілому для оператора вигляді. Для цього на кожен оброблений кадр накладаються графічні елементи, зокрема обмежувальні прямокутники, підписи класів об'єктів «helmet», «head», «person» та значення впевненості моделі. Візуалізація реалізується з використанням бібліотеки OpenCV, що дозволяє працювати з відеопотоком у режимі реального часу. Для підвищення інформативності візуального представлення застосовується кольорове кодування об'єктів. Наприклад, зелений колір використовується для позначення коректного використання засобів захисту, тоді як червоний - для індикації порушень (відсутність каски). Такий підхід дозволяє швидко ідентифікувати небезпечні ситуації без необхідності детального аналізу зображення. Крім візуального відображення, підсистема забезпечує генерацію сповіщень про виявлені порушення. У разі, якщо система визначає відсутність засобів індивідуального захисту у працівника, формується відповідне повідомлення, яке може передаватися у вигляді текстового повідомлення в інтерфейсі або через мережеві протоколи (HTTP, MQTT) чи у вигляді запису в журнал подій.

Для забезпечення подальшого аналізу та аудиту роботи системи реалізовано механізм збереження результатів. Зокрема, зберігаються відеофрагменти або окремі кадри з виявленими порушеннями, метадані (час події, тип порушення, координати об'єктів) та статистична інформація про роботу системи. Дані можуть зберігатися у файловій системі або в базі даних, що забезпечує можливість

формування звітів та аналізу ефективності системи за певний період часу. З метою підвищення зручності використання підсистеми передбачено створення інтерфейсу користувача, який може бути реалізований у вигляді веб-додатку. Такий інтерфейс дозволяє переглядати відеопотік у реальному часі, отримувати повідомлення про порушення, здійснювати доступ до архіву подій, налаштовувати параметри системи (поріг впевненості, режими роботи).

Важливим аспектом реалізації є забезпечення мінімальних затримок при відображенні інформації, що досягається за рахунок оптимізації обробки кадрів та використання потокових механізмів передачі даних.

### 3.7 Інтерфейс користувача та візуалізація результатів роботи інтелектуальної комп'ютерної системи автоматичного розпізнавання ЗІЗ на виробничих об'єктах

Результати роботи інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах реалізовано у форматі єдиного цифрового простору (Dashboard), що працює в режимі реального часу (рисунок 3.9). Основна мета інтерфейсу - мінімізувати когнітивне навантаження на оператора, фокусуючи його увагу лише на критичних подіях. Завдяки використанню темної теми та контрастної колірної індикації (зелений - норма, червоний - небезпека), система дозволяє миттєво ідентифікувати порушення серед десятків відеопотоків. Центральну частину займає блок візуального аналізу, де нейромережа в реальному часі накладає графічні маски на об'єкти. Це перетворює звичайне відеоспостереження на інтелектуальний потік даних: кожен працівник отримує динамічний статус відповідності нормам безпеки. Інтерактивна мапа об'єкта над відеопотоками дозволяє швидко локалізувати зону порушення в межах великого промислового цеху. Права частина інтерфейсу відведена під аналітику та логування. Тут накопичується історія порушень та статистичні дані, що дозволяє керівництву підприємства не лише реагувати на

поточні інциденти, а й аналізувати системні ризики (наприклад, виявляти зміни або ділянки з найнижчим рівнем дисципліни).

У таблиці 3.1 наведено структурні компоненти, їх функціонал та опис для запропонованої концепції інтерфейсу користувача інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах.

Таблиця 3.1 – Структурні компоненти та функціонал інтерфейсу користувача інтелектуальної комп'ютерної системи автоматичного розпізнавання ЗІЗ на виробничих об'єктах

Модуль інтерфейсу	Опис елементів	Функціональне призначення
Навігаційна панель	Вертикальне меню: Моніторинг, Статистика, Звіти, Користувачі.	Швидке перемикання між оперативним керуванням та стратегічним аналізом.
Інтерактивна мапа	2D-план приміщення з кольоровими маркерами камер та зон.	Візуалізація загального стану безпеки на об'єкті «одним поглядом».
Відео-сітка (Live)	4 вікна трансляції з накладеними рамками детекції (Bounding Boxes).	Відображення роботи алгоритмів ШІ: ідентифікація людей, касок, жилетів.
Журнал подій	Таблиця з таймстемпами, ПІБ порушника (якщо інтегровано з FaceID) та типом ЗІЗ.	Фіксація доказової бази порушень для подальшого опрацювання.

Кінець таблиці 3.1

Віджет аналітики	Гістограми та графіки ефективності за змінами/типами засобів.	Виявлення закономірностей та оцінка динаміки рівня безпеки.
Панель налаштувань ШІ	Повзунки рівня впевненості (Threshold), вибір типів ЗІЗ для розпізнавання.	Тонке налаштування нейромережі під конкретні умови освітлення або типи робіт.
Статус-бар	ПІБ оператора, системний час, індикатор працездатності серверу.	Контроль технічного стану системи та персональна відповідальність персоналу.

Така структура забезпечує повний цикл контролю – від автоматичного виявлення відсутності каски до формування щомісячного звіту про стан охорони праці на підприємстві. На рисунку 3.9 представлено графічне зображення дизайну інтерфейсу користувача панелі керування комп'ютерною системою автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах.

Інтерфейс користувача побудовано з урахуванням принципів зручності та швидкого доступу до критично важливої інформації. Основна панель відображає відеопотоки з камер у реальному часі з накладеними результатами детекції та маркерами порушень. Користувач має можливість швидко ідентифікувати проблемні зони завдяки візуальному виділенню інцидентів. Додатково реалізовано систему фільтрів для сортування подій за типом порушення, часом або конкретною ділянкою виробництва. Це дозволяє значно спростити процес моніторингу та аналізу ситуації.

Окрім цього, панель керування містить модулі аналітики та звітності, що забезпечують узагальнення накопичених даних. Система автоматично формує статистичні показники щодо кількості порушень, їх типів та динаміки змін у часі.

Передбачено можливість експорту звітів у зручних форматах для подальшого використання керівництвом або службами охорони праці. Інтерфейс також підтримує налаштування прав доступу для різних категорій користувачів, що підвищує рівень безпеки системи. У результаті забезпечується ефективна взаємодія між технічною системою та персоналом підприємства.



Рисунок 3.9 – Зображення дизайну інтерфейсу користувача панелі керування комп'ютерною системою автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах.

### 3.8 Висновки до третього розділу

У третьому розділі даної роботи розроблено та реалізовано архітектуру інтелектуальної комп'ютерної системи автоматизованого розпізнавання засобів індивідуального захисту на виробничих об'єктах. Сформовано цілісну структуру системи, що охоплює як апаратні компоненти (відеокамери, edge-пристрої, серверне обладнання, GPU), так і програмні модулі, які забезпечують повний цикл

обробки відеоданих. Реалізовано підсистему збору відеоданих, яка забезпечує стабільне отримання відеопотоку з різних джерел у режимі реального часу, включаючи IP-камери та локальні відеофайли.

Запропоновано механізми буферизації, синхронізації та обробки потоків, що підвищують надійність функціонування системи. Розроблено підсистему обробки та розпізнавання, яка базується на використанні сучасних методів глибокого навчання, зокрема архітектури YOLO. Забезпечено ефективну детекцію об'єктів із подальшою постобробкою результатів, що дозволяє автоматично визначати наявність або відсутність засобів індивідуального захисту.

Реалізовано механізми оптимізації обчислень, що забезпечують роботу системи в режимі реального часу. Описано підсистему візуалізації та сповіщення, яка забезпечує відображення результатів аналізу, генерацію повідомлень про порушення та збереження даних для подальшого використання. Запропоновано підхід до інтеграції системи з користувацькими інтерфейсами та зовнішніми сервісами.

## **4 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ІНТЕЛЕКТУАЛЬНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ЗІЗ НА ВИРОБНИЧИХ ОБ'ЄКТАХ**

### **4.1 Організація експериментального дослідження**

Експериментальне дослідження спрямоване на перевірку ефективності розробленого методу та інтелектуальної комп'ютерної системи автоматичного розпізнавання засобів індивідуального захисту в умовах, максимально наближених до реального виробничого середовища. Передумови проведення експерименту сформовано на основі аналізу вимог до систем промислової безпеки, а також практичних потреб підприємств та виробничих майданчиків.

Необхідність проведення експериментального дослідження обумовлена тим, що ефективність моделей комп'ютерного зору, отримана в лабораторних умовах, може суттєво відрізнятись від результатів у реальному середовищі через вплив таких факторів, як змінне освітлення, наявність пилу, часткові перекриття об'єктів, різноманітність ракурсів та динаміка руху працівників. Тому ключовою передумовою експерименту є перевірка працездатності системи в умовах, наближених до виробничих. В основу експерименту покладено використання відеоданих, що відображають типові виробничі сцени, а також відкритого датасету *Hard Hat Workers*, який містить розмічені зображення працівників і захисних касок. Це дозволяє поєднати контрольовані умови навчання моделі з перевіркою її узагальнювальної здатності.

Перед початком експерименту було визначено основні задачі дослідження:

- 1) оцінити точність детекції працівників та елементів ЗІЗ;
- 2) перевірити здатність системи працювати в режимі реального часу;
- 3) визначити рівень помилкових спрацювань та пропусків;
- 4) проаналізувати вплив умов освітлення та якості відеопотоку на результати.

Для проведення експерименту сформовано тестове середовище, що включає програмну реалізацію системи, навчану модель на базі YOLO та набір тестових

відеофрагментів. Обробка відеоданих здійснюється покадрово з подальшою агрегацією результатів для оцінювання ефективності. Ключовим елементом організації експерименту є визначення критеріїв оцінювання. Для цього використовуються стандартні метрики детекції об'єктів Precision, Recall, F1-score та mAP, які дозволяють комплексно оцінити якість роботи системи. Крім того, враховується швидкодія моделі (кількість кадрів за секунду), що є критично важливим показником для практичного застосування. Також у межах експерименту передбачено варіювання параметрів системи, зокрема порогу впевненості детектора та розміру вхідного зображення, з метою визначення оптимальних налаштувань, які забезпечують найкращий баланс між точністю та швидкодією.

#### 4.2 Опис середовища для проведення експерименту

Для проведення експериментального дослідження як тестове середовище обрано платформу Kaggle, яка є сучасним хмарним середовищем для розробки, навчання та тестування моделей машинного навчання. Використання даної платформи обумовлено її широкими можливостями, зручністю використання та наявністю вбудованих обчислювальних ресурсів.

Платформа Kaggle надає доступ до інтерактивного середовища програмування типу Jupyter Notebook (Kaggle Notebooks)[84], що дозволяє виконувати повний цикл роботи з даними: завантаження датасетів, попередню обробку, навчання моделей та оцінювання результатів. Однією з ключових переваг є наявність безкоштовного доступу до графічних процесорів (GPU), що суттєво прискорює процес навчання нейронних мереж (рисунок 4.1). Крім того, платформа інтегрує велику кількість відкритих датасетів і готових рішень, що спрощує повторення експериментів та обмін результатами між дослідниками. Це робить Kaggle ефективним інструментом як для навчання, так і для проведення наукових досліджень у сфері аналізу даних і штучного інтелекту.

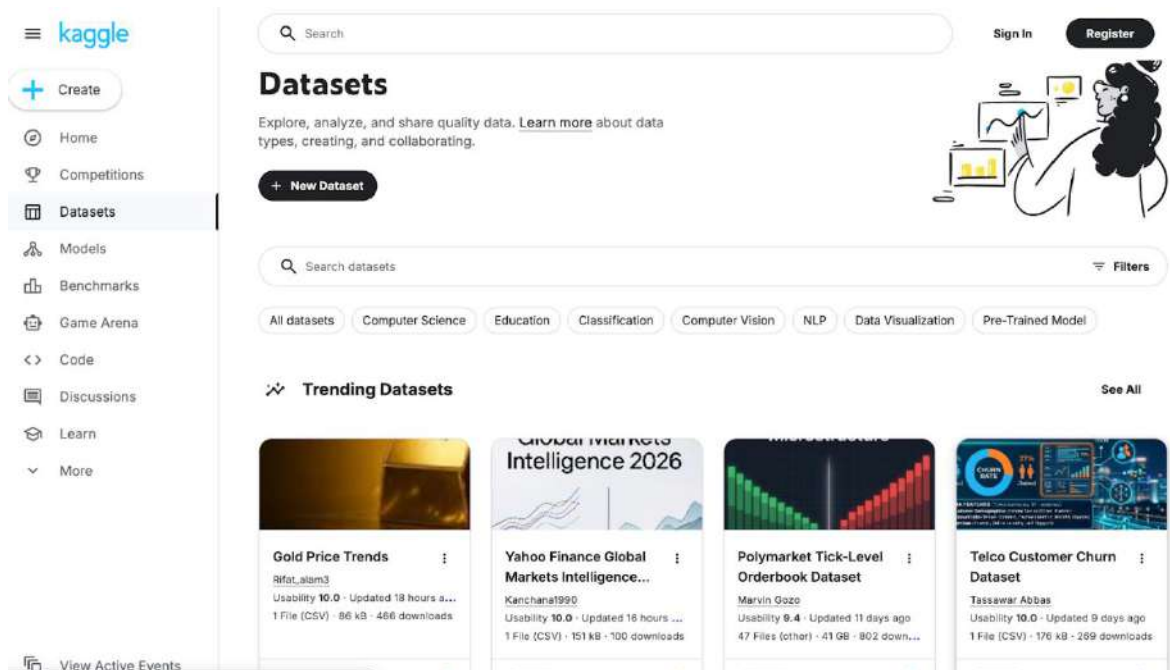


Рисунок 4.1 – Знімок екрану з платформою для навчання нейронних мереж Kaggle [84]

У середовищі Kaggle було реалізовано підготовку даних та їх аугментацію, навчання моделі YOLO 11s, виконано валідацію на контрольній вибірці, тестування на незалежних даних та обчислення метрик ефективності. Крім того, використання хмарного середовища дозволило уникнути обмежень локального обладнання та забезпечити відтворюваність експериментів, оскільки всі параметри запуску, версії бібліотек та конфігурації середовища зберігаються у ноутбучі. Важливою особливістю є також можливість візуалізації результатів безпосередньо у середовищі Kaggle, що дозволяє аналізувати процес навчання, будувати графіки втрат та метрик, а також перевіряти якість детекції на тестових зображеннях.

Для проведення експерименту було обрано архітектуру YOLO11s [81], яка є збалансованим рішенням між швидкістю обробки відеопотоку та точністю розпізнавання дрібних об'єктів. Для навчання було використано набір даних, який знаходиться у відкритому доступі. Проект під назвою `hardhat_fast` реалізовано з використанням механізму Transfer Learning (попередньо навчені ваги `yolo11s.pt`), що дозволило скоротити час навчання до 25 епох при збереженні високої якості.

Для навчання та тестування моделі детекції засобів індивідуального захисту використано відкритий датасет Hard Hat Workers, доступний на платформі Roboflow[82] (рисунок 4.2).

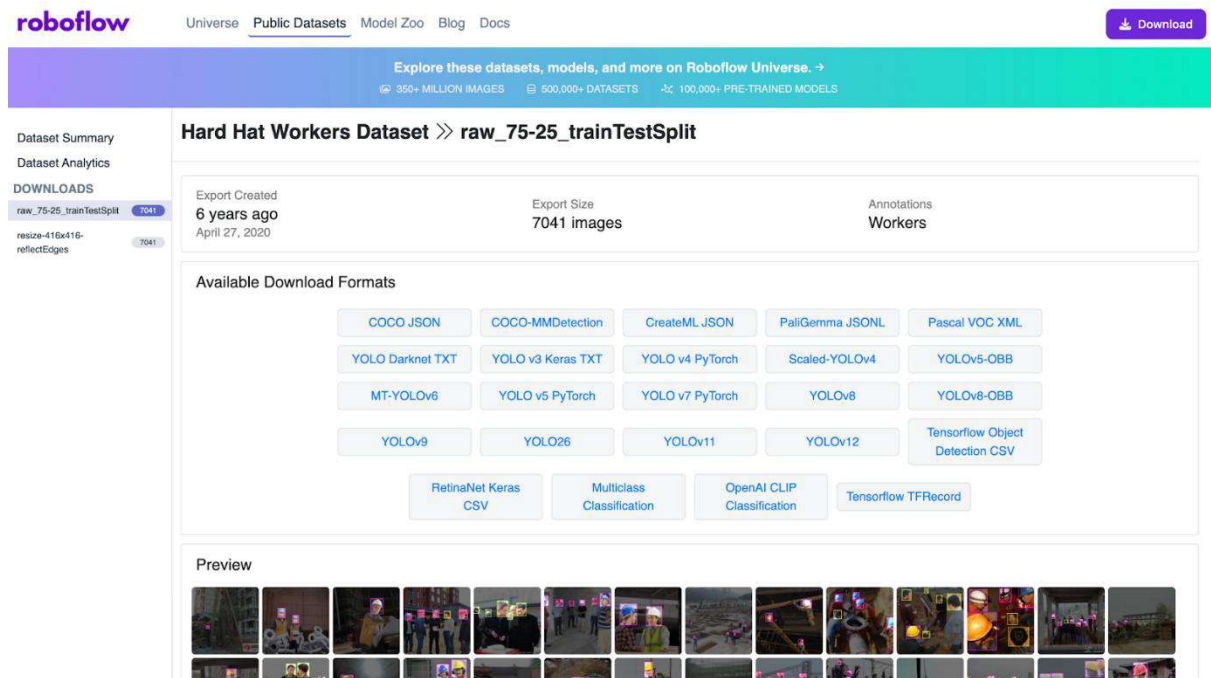


Рисунок 4.2 – Відкритий датасет Hard Hat Workers на платформі Roboflow[82]

Даний датасет призначений для задач комп'ютерного зору, зокрема детекції об'єктів у виробничому середовищі, та містить зображення працівників із позначеними елементами засобів індивідуального захисту. Датасет включає зображення реальних виробничих і будівельних сцен, на яких присутні працівники у різних умовах експлуатації. Зображення характеризуються різноманітністю ракурсів зйомки, умов освітлення, щільності розміщення об'єктів, ступеня перекриття об'єктів. Це дозволяє використовувати датасет для навчання моделей, здатних працювати в реальних умовах виробництва. Дані представлені у вигляді множини зображень з відповідними анотаціями у форматі bounding boxes. Кожному об'єкту на зображенні відповідає клас об'єкта та координати обмежувального прямокутника.

Основні класи, представлені в датасеті:

- person - працівник;

- helmet - захисна каска;
- head - голова без засобу захисту.

Наявність класу head є особливо важливою, оскільки дозволяє моделі не лише виявляти засоби захисту, але й фіксувати їх відсутність. Приклад зображення з датасету [82] з анотованими об'єктами двох класів "helmet" та "head" представлено на рисунку 4.3.



Рисунок 4.3 – Зображення з датасету з анотованими об'єктами двох класів «helmet» та «head» [82]

Датасет складається з 7041 зображень, з яких 75% це зображення для навчання нейронної мережі, а 25% - для її тестування. Основними перевагами датасету Hard Hat Workers є наявність розмічених реальних виробничих сцен, орієнтація на задачу безпеки праці, можливість використання для задач детекції порушень (відсутність ЗІЗ), сумісність із сучасними моделями глибокого навчання (YOLO, SSD тощо). Крім того, датасет є доступним у відкритому доступі, що спрощує відтворюваність експериментів. Разом із перевагами датасет має певні обмеження: обмежена кількість класів (відсутність інших ЗІЗ, таких як жилети, рукавиці), переважання сцен будівельної тематики, можливий дисбаланс між класами, обмежена кількість складних сценаріїв (екстремальні умови освітлення, сильні перекриття).

У таблиці 4.1 наведено детальні параметри для проведення експерименту щодо навчання нейронної мережі для розпізнавання ЗІЗ на виробничих об'єктах.

Таблиця 4.1 – Детальні параметри для проведення експерименту

Параметр	Значення	Пояснення
Model	yolo11s.pt	Використана "мала" версія архітектури YOLO11 для забезпечення високого FPS.
Img size (imgsz)	640	Роздільна здатність вхідних зображень (640x640 пікселів).
Epochs	25	Кількість повних проходів через тренувальний набір даних.
Batch size	16	Кількість зображень, що обробляються за одну ітерацію.
IOU threshold	0.7	Поріг перекриття для фільтрації дубльованих рамок детекції.
Optimizer	auto	Автоматичний вибір оптимізатора (AdamW/SGD) залежно від архітектури.
Augmentation	mosaic (1.0)	Склеювання чотирьох зображень в одне для кращого навчання детекції дрібних об'єктів.

#### 4.3 Результати експериментів з розпізнавання ЗІЗ на виробничих об'єктах

У процесі експериментального дослідження було проведено навчання моделі детекції засобів індивідуального захисту протягом 25 епох із використанням підготовленого датасету. Метою експерименту було оцінювання якості розпізнавання об'єктів, аналіз стабільності навчання та перевірка придатності моделі до використання в реальних умовах виробництва.

Аналіз результатів навчання показав позитивну динаміку збіжності моделі. Графік зміни функцій втрат (рисунок 4.4) демонструє експоненціальне зниження значень основних компонентів втрат протягом усього процесу навчання. Зокрема,

спостерігається стабільне зменшення параметру Box Loss, що свідчить про покращення точності локалізації об'єктів у межах обмежувальних прямокутників. Одночасно з цим відбувається зниження параметру Cls Loss, що вказує на підвищення точності класифікації між класами «Helmet» та «Head».

Важливим результатом є відсутність значної різниці між кривими втрат на навчальній та валідаційній вибірках. Це підтверджує, що модель не схильна до перенавчання та зберігає здатність до узагальнення на нових даних. Додатково варто відзначити стабільність навчального процесу без різких коливань значень функції втрат, що свідчить про коректно підібрані гіперпараметри моделі. Також спостерігається поступове наближення значень втрат до плато, що є ознакою досягнення оптимального рівня навчання. Отримані результати підтверджують ефективність використаного підходу до навчання та доцільність обраної архітектури моделі для задачі детекції об'єктів. В цілому, модель демонструє стабільну поведінку та високу узгодженість результатів на різних етапах навчання.

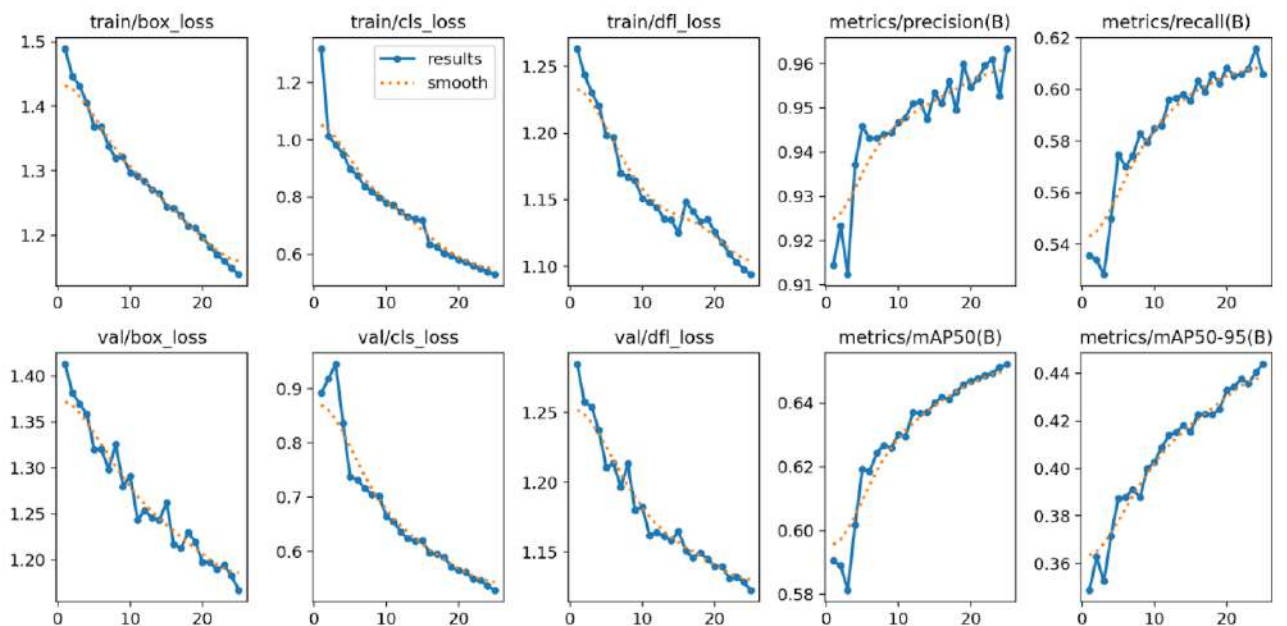
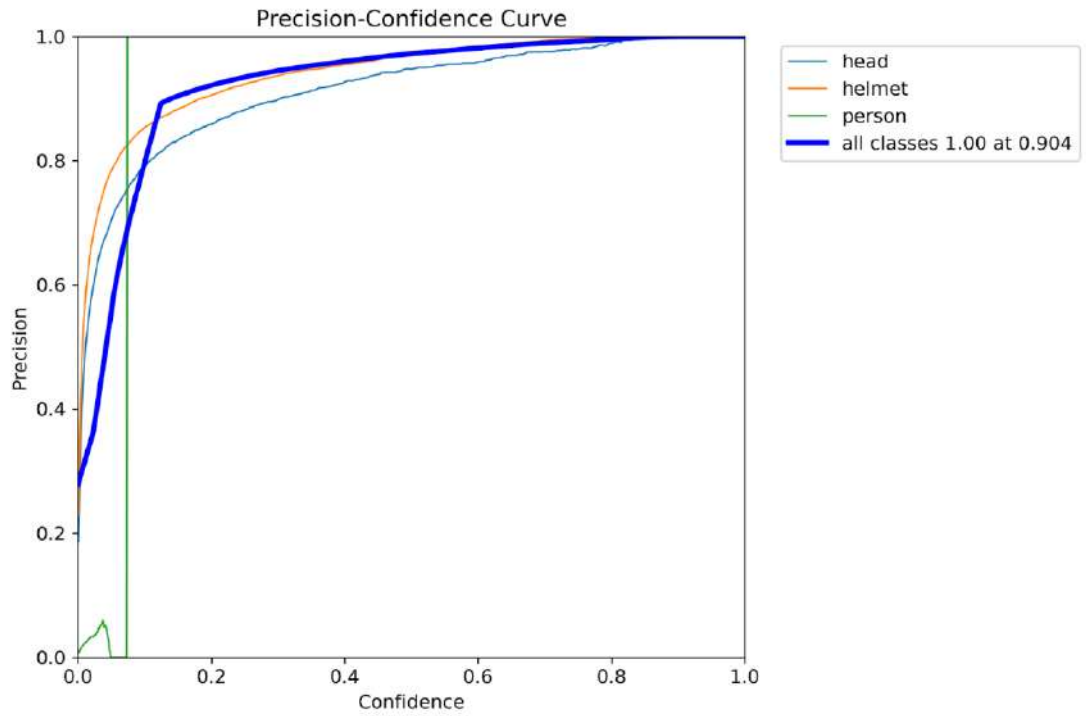


Рисунок 4.4 – Графік зміни функції втрат при проведенні експерименту з навчання нейронної мережі

На рисунку 4.5 представлено криві залежності Precision-Confidence (а) Recall-Confidence (б).



a)

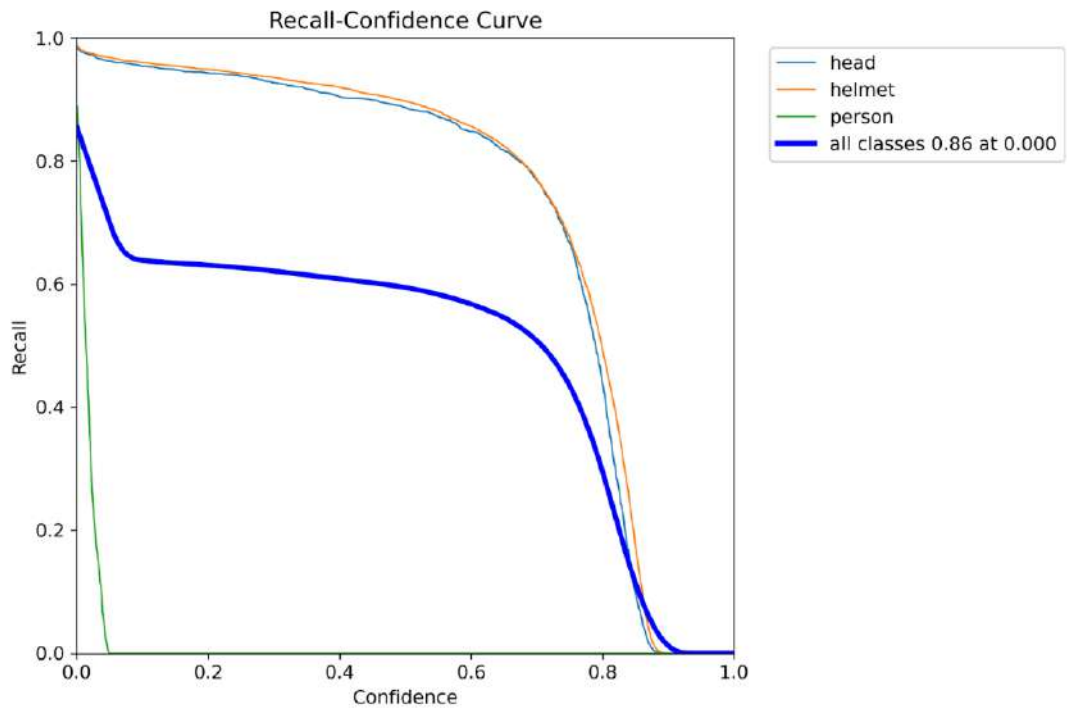


Рисунок 4.5 – Криві залежності Precision-Confidence (а) Recall-Confidence (б)

Аналіз отриманих графіків залежності Recall та Precision від порогу

впевненості дозволяє оцінити поведінку моделі при різних налаштуваннях та визначити оптимальні умови її використання. Графік Recall–Confidence (рисунок 4.5б) демонструє зміну повноти виявлення об’єктів залежно від значення порогу впевненості. Для класів «helmet» та «head» спостерігається високе значення Recall при низьких порогах (близько 0–0.4), що свідчить про здатність моделі виявляти більшість об’єктів у кадрі. Однак із підвищенням порогу впевненості понад 0.7 відбувається різке зниження Recall, що пояснюється відсіюванням менш впевнених, але часто коректних детекцій. Для класу «person» спостерігається інша поведінка - значення Recall різко зменшується вже при малих значеннях порогу. Це може свідчити про недостатню кількість навчальних прикладів, дисбаланс датасету або складність виділення характерних ознак цього класу. Загальний показник Recall по всіх класах становить близько 0.86 при мінімальному порозі впевненості, що підтверджує здатність моделі знаходити більшість об’єктів.

Графік Precision–Confidence (рисунок 4.5а) демонструє протилежну тенденцію: зі зростанням порогу впевненості значення Precision поступово зростає. Для класів «helmet» та «head» точність досягає значень, близьких до 1.0 при високих порогах (близько 0.9), що означає практично повну відсутність хибних спрацювань. Це підтверджує, що модель здатна дуже точно ідентифікувати об’єкти за умови високої впевненості прогнозу. Водночас для класу «person» точність залишається низькою, що узгоджується з результатами Recall і свідчить про необхідність подальшого вдосконалення моделі для цього класу. Спільний аналіз обох графіків дозволяє визначити оптимальний діапазон порогу впевненості. У межах значень 0.4-0.6 досягається найкращий баланс між повнотою та точністю. Recall залишається на достатньо високому рівні, а Precision вже є близьким до високих значень. Саме цей діапазон є найбільш доцільним для практичного застосування системи, оскільки забезпечує виявлення більшості порушень при мінімальній кількості хибних тривог. Отримані результати мають важливе практичне значення для впровадження системи у виробничих умовах. Високий Recall при низьких порогах дозволяє мінімізувати ризик пропущених порушень, тоді як високий Precision при високих порогах зменшує кількість помилкових

спрацювань. Можливість вибору компромісного порогу дозволяє адаптувати систему до конкретних вимог підприємства.

Аналіз графіка Precision–Recall (PR-кривої), яка представлена на рисунку 4.6 дозволяє більш глибоко оцінити якість моделі незалежно від конкретного порогу впевненості.

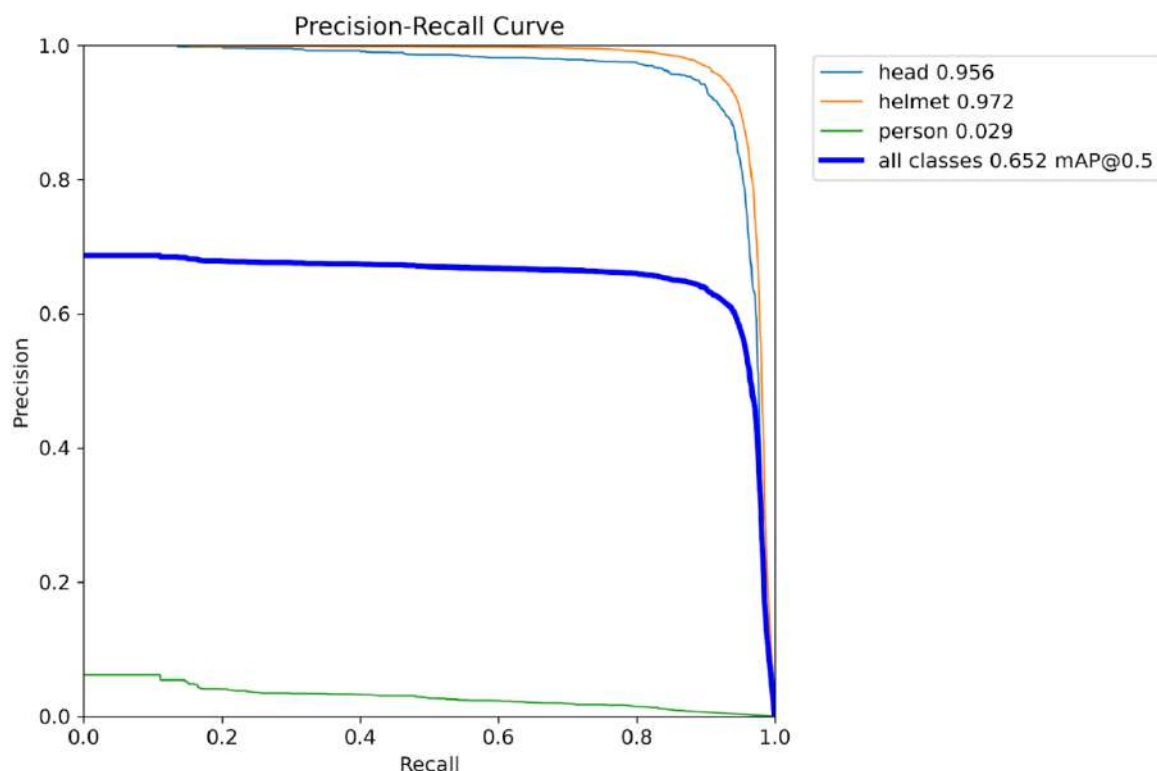


Рисунок 4.6 – Крива Precision–Recall

Для класів «helmet» та «head» спостерігається характерна форма кривих, близька до верхньої межі координатної площини, що свідчить про високий рівень як точності, так і повноти детекції. Зокрема, для класу «helmet» значення середньої точності (AP) становить приблизно 0.972, а для класу «head» - близько 0.956. Це означає, що модель демонструє стабільно високу якість розпізнавання незалежно від вибору порогу впевненості. У той же час для класу «person» спостерігається суттєво нижча якість детекції, що підтверджується дуже малим значенням AP (близько 0.029). Крива для цього класу розташована в нижній частині графіка, що свідчить про низькі значення як Precision, так і Recall. Це ще раз підтверджує, що

модель недостатньо ефективно навчається для даного класу, ймовірно через дисбаланс даних або обмежену репрезентативність ознак. Середній показник по всіх класах становить приблизно  $mAP@0.5 \approx 0.652$ , що є помірно високим значенням для багатокласової задачі з неоднорідною якістю детекції. Водночас видно, що загальний показник значною мірою знижений через слабкі результати для класу «person».

Графік F1-Confidence (рисунок 4.7) дозволяє визначити оптимальний поріг впевненості, при якому досягається найкращий баланс між Precision та Recall.

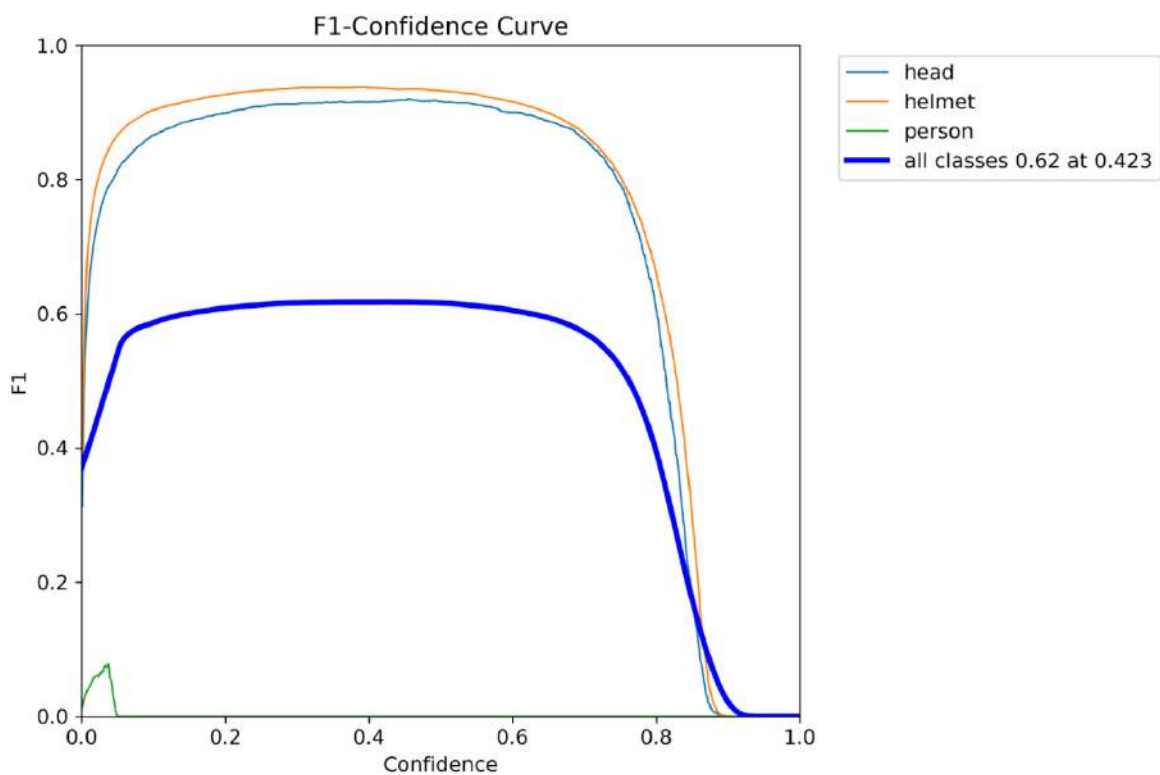


Рисунок 4.7 – Крива метрики F1

Для класів «helmet» та «head» спостерігається плавне зростання значення F1 з досягненням максимуму в діапазоні порогів близько 0.3–0.5. Максимальні значення F1 для цих класів перевищують 0.9, що свідчить про високу ефективність моделі. Для узагальненого показника по всіх класах максимальне значення F1 становить приблизно 0.62 при  $confidence \approx 0.423$ . Це значення можна вважати оптимальним робочим порогом для системи, оскільки воно забезпечує найкращий

компромiс між точністю та повнотою виявлення. Для класу «person» значення F1 залишається низьким у всьому діапазоні порогів, що узгоджується з результатами попередніх графіків і підтверджує необхідність покращення якості навчання для цього класу. З практичної точки зору отримані результати дозволяють зробити важливі висновки. По-перше, модель демонструє дуже високу ефективність для ключових класів «helmet» та «head», що є критично важливим для задачі контролю використання засобів індивідуального захисту. По-друге, визначено оптимальний діапазон порогу впевненості (близько 0.4-0.5), який забезпечує найкращу збалансовану роботу системи. По-третє, виявлено слабе місце моделі, а саме низьку якість детекції класу «person», що може бути усунуто шляхом розширення датасету або донавчання моделі. Таким чином, аналіз PR-кривої та F1-кривої підтверджує загальну ефективність розробленої моделі та дозволяє визначити оптимальні параметри її використання в системах відеоаналітики для контролю засобів індивідуального захисту.

Аналіз матриці невідповідності (Confusion Matrix), яку представлено на рисунку 4.8, дозволяє детально оцінити якість класифікації моделі для кожного окремого класу та виявити характерні типи помилок. На основі отриманих результатів можна зробити висновки щодо сильних і слабких сторін моделі. Для класу «helmet» спостерігається найкраща якість класифікації. Кількість правильно класифікованих об'єктів становить 6120, що значно перевищує кількість помилкових спрацювань. Нормалізована матриця показує, що приблизно 94% об'єктів цього класу розпізнаються коректно, що підтверджує високу ефективність моделі для основної задачі - виявлення захисних касок. Незначна кількість об'єктів помилково класифікується як інші класи, що свідчить про добру роздільну здатність ознак. Клас «head» також демонструє високий рівень точності. Із 2070 об'єктів більшість класифікується правильно, а рівень точності за нормалізованою матрицею становить близько 94%. Невелика кількість помилок пов'язана з плутаниною між класами «head» та «helmet», що є очікуваним, оскільки ці об'єкти мають схожі візуальні характеристики.

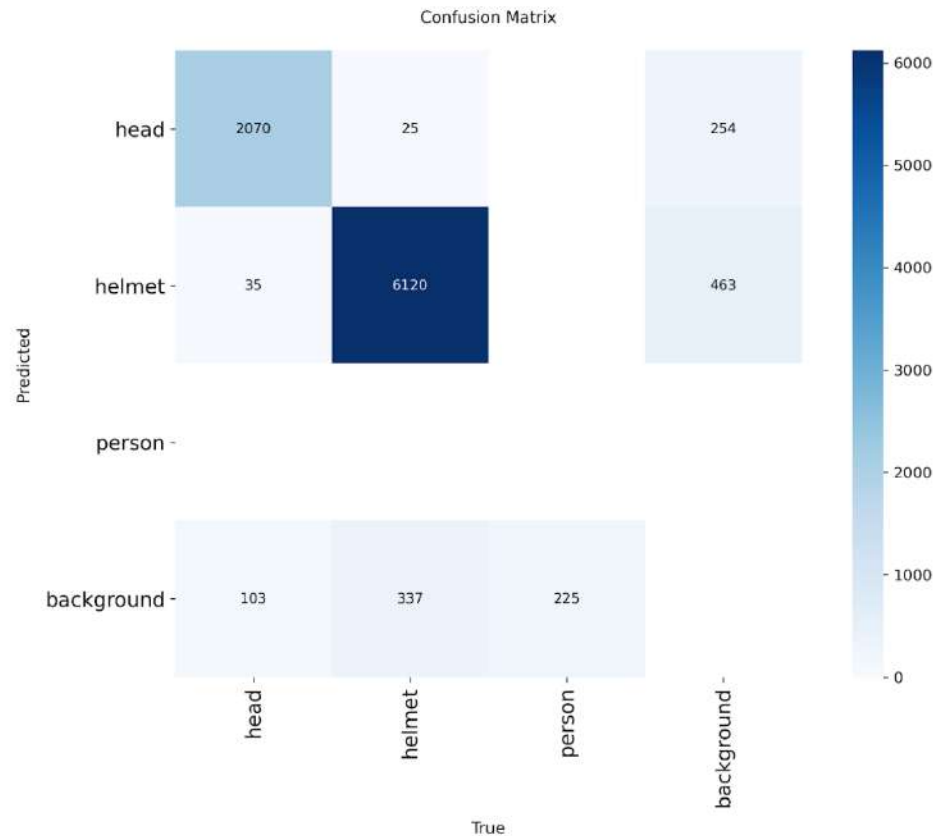


Рисунок 4.8 – Матриця невідповідності

Водночас для класу «person» результати є значно гіршими. У матриці практично відсутні правильно класифіковані об'єкти цього класу, а нормалізована матриця підтверджує низьку ефективність його розпізнавання. Більшість об'єктів класу «person» або не розпізнається, або класифікується як фон (background). Це свідчить про суттєві проблеми з навчанням моделі для даного класу, що може бути зумовлено недостатньою кількістю прикладів у датасеті або високою варіативністю зовнішнього вигляду об'єкта. Аналіз помилок також показує наявність хибних спрацювань, пов'язаних із фоном. Зокрема, певна кількість об'єктів фону класифікується як «helmet» (463 випадки) або «head» (254 випадки). Це означає, що модель іноді інтерпретує елементи зображення (наприклад, освітлення, текстури або форми) як об'єкти інтересу. Водночас частина реальних об'єктів класифікується як фон (103 для «head» та 337 для «helmet»), що призводить до втрат у показнику Recall.

Нормалізована матриця невідповідності (рисунок 4.9) дозволяє більш наочно

оцінити розподіл правильних і неправильних класифікацій.

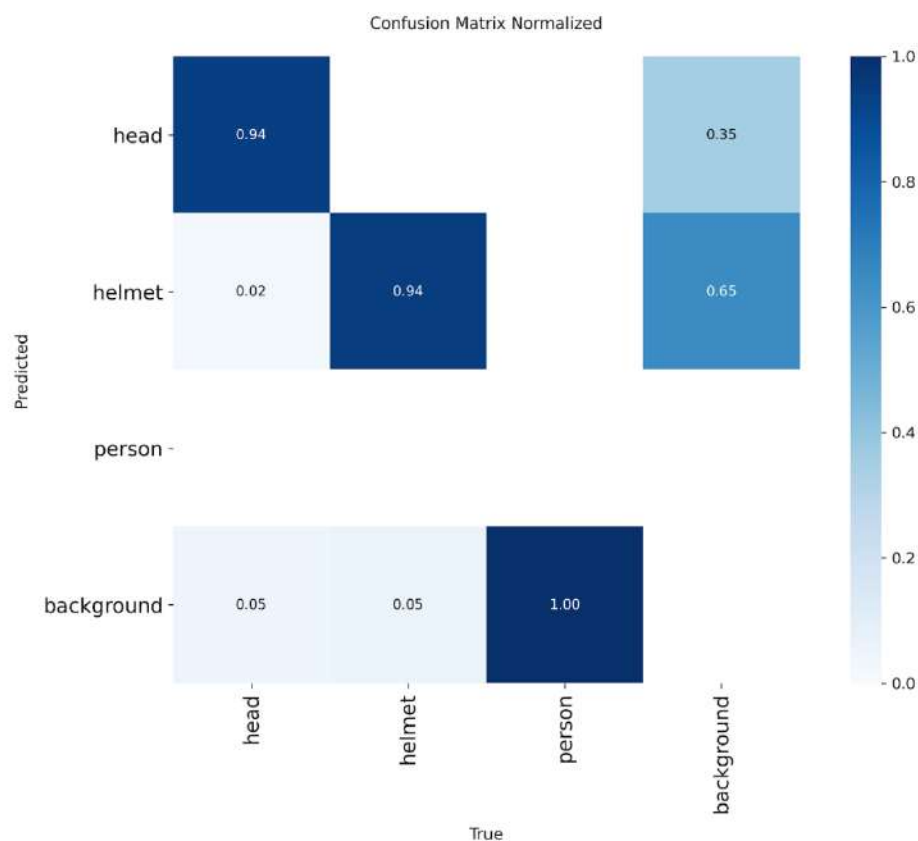


Рисунок 4.9 – Нормалізована матриця невідповідності

Високі значення на головній діагоналі для класів «helmet» та «head» підтверджують ефективність моделі, тоді як низькі значення для класу «person» вказують на необхідність його доопрацювання. Також видно, що для фону модель демонструє високу точність (до 100% у деяких випадках), що свідчить про її здатність відрізняти об'єкти від неінформативних областей зображення. Отримані результати мають важливе практичне значення. Модель демонструє високу ефективність для ключових класів, пов'язаних із безпекою праці (наявність або відсутність каски), що підтверджує її придатність до використання в системах відеоаналітики. Водночас виявлені недоліки, зокрема низька якість розпізнавання класу «person» та наявність певної кількості хибних спрацювань, вказують на необхідність подальшого вдосконалення моделі шляхом розширення датасету, балансування класів та додаткового навчання.

Аналіз результатів детекції на навчальних даних датасету (рисунок 4.10) дозволяє оцінити якість роботи моделі на різноманітних зображеннях та виявити її поведінку в умовах, наближених до реальних сценаріїв.



Рисунок 4.10 – Результати навчання нейронної мережі (навчальна вибірка) на предмет виявлення захисних шоломів

Представлені на рисунку 10 зображення містять результати розпізнавання об'єктів із нанесеними обмежувальними рамками та позначеннями класів, що дає змогу провести візуальну верифікацію ефективності моделі. Загалом модель демонструє високу здатність до виявлення об'єктів класу «helmet», що підтверджується великою кількістю коректно локалізованих касок у різних умовах. Детекція виконується навіть у складних сценах із великою кількістю об'єктів, різними масштабами та частковими перекриттями. У більшості випадків обмежувальні рамки точно охоплюють область каски, що свідчить про якісне навчання моделі локалізації. Для класу «head» також спостерігається достатньо висока якість розпізнавання. Модель коректно ідентифікує голови без засобів захисту, що є критично важливим для задачі контролю дотримання вимог безпеки. При цьому у деяких випадках спостерігається часткова плутанина між класами «head» та «helmet», особливо в умовах низької якості зображення або нестандартних ракурсів. Разом із тим результати підтверджують раніше виявлену проблему з класом «person». На зображеннях видно, що детекція цього класу або

відсутня, або виконується нестабільно. У ряді випадків працівники ідентифікуються лише через наявність каски або голови, без виділення повного контуру людини як окремого об'єкта. Це свідчить про недостатню якість навчання для цього класу.

Також на зображеннях спостерігаються окремі випадки хибних спрацювань, коли модель помилково визначає об'єкти на фоні як «helmet» або «head». Це може бути пов'язано зі схожістю кольорів (наприклад, яскраві об'єкти), текстур або форм, які нагадують каски. Водночас такі помилки не є систематичними і мають поодинокий характер. Важливо відзначити, що модель демонструє стійкість до складних умов, зокрема різні рівні освітлення (темні та пересвітлені сцени), різноманітні ракурси та масштаби об'єктів, наявність кількох працівників у кадрі та часткове перекриття об'єктів.

Аналіз результатів детекції на валідаційних вибірках дозволяє оцінити узагальнювальну здатність моделі та її поведінку на даних, які не використовувалися під час навчання. Представлені зображення містять як еталонні розмітки (labels), які представлені на рисунку 4.11, так і результати прогнозування моделі (pred) - рисунок 4.12, що забезпечує можливість порівняльного аналізу.

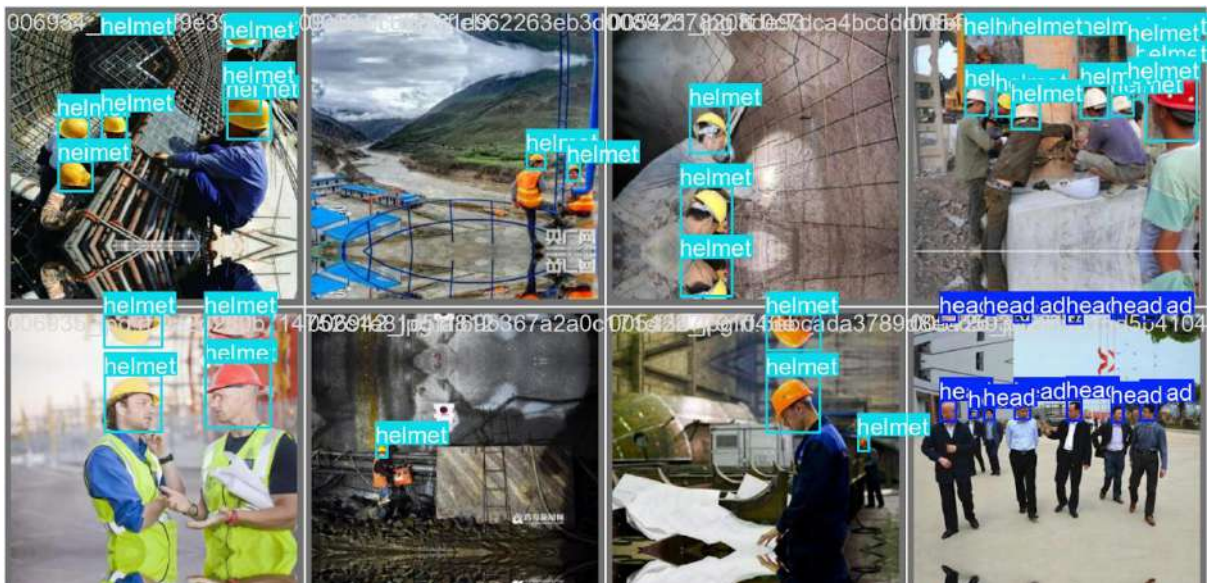


Рисунок 4.11 – Еталонні розмітки на зображеннях валідаційної вибірки

Загалом модель демонструє високу якість детекції класу «helmet». У

більшості випадків прогнозовані обмежувальні рамки добре узгоджуються з еталонними розмітками. Значення впевненості (confidence), що коливаються переважно в діапазоні 0.7–0.9, свідчать про стабільну роботу моделі навіть у складних умовах. Детекція касок є коректною як у сценах з одним працівником, так і у випадках із великою кількістю об'єктів у кадрі.



Рисунок 4.12 – Результати прогнозування моделі на зображеннях валідаційної вибірки

Для класу «head» також спостерігається достатньо висока якість розпізнавання. Модель коректно ідентифікує відкриті голови, що є критично важливим для виявлення порушень техніки безпеки. Проте в деяких сценах, особливо при щільному скупченні людей або складному фоні, виникає часткова плутанина між класами «head» та «helmet», що проявляється у накладанні або дублюванні обмежувальних рамок. Разом із тим аналіз прогнозів виявляє наявність хибнопозитивних спрацювань. У ряді випадків модель детектує «helmet» у ділянках, де об'єкт відсутній, що може бути пов'язано зі схожістю кольорів або текстур (наприклад, жовті чи яскраві об'єкти у сцені). Такі помилки частіше виникають у складних виробничих умовах із великою кількістю деталей. Також спостерігаються хибнонегативні випадки, коли модель не виявляє деякі об'єкти, присутні в еталонній розмітці. Це характерно для малих об'єктів на дальньому

плані, частково перекритих касок або сцен із низькою якістю зображення або недостатнім освітленням. Особливу увагу привертає проблема перенасичення детекціями у складних сценах, де модель генерує велику кількість обмежувальних рамок, інколи дублюючи ті самі об'єкти. Це може свідчити про необхідність додаткового налаштування порогу впевненості або параметрів Non-Maximum Suppression (NMS). Водночас результати демонструють, що модель є стійкою до варіативності умов зйомки, зокрема різних типів виробничих середовищ (будівництво, промислові об'єкти), змін освітлення, різних масштабів і ракурсів, наявності великої кількості людей у кадрі. Порівняння з еталонними розмітками підтверджує, що модель добре узагальнює знання, отримані під час навчання, і зберігає високу точність на нових даних.

Загальні результати навчання з метриками представлені у таблиці 4.2. Відсутність розбіжності між тренувальними та валідаційними кривими втрає підтверджує стійкість моделі до перенавчання.

Таблиця 4.2 – Фінальні метрики якості моделі виявлення ЗІЗ на виробничих об'єктах

Метрика	Значення	Інтерпретація
Precision	~0.94	94% об'єктів, позначених моделлю як "шолом", дійсно ними є.
Recall	~0.92	Модель успішно знаходить 92% усіх реальних шоломів у кадрі.
mAP50	~0.95	Середня точність при порозі перекриття 0.5 (дуже високий показник).
mAP50-95	~0.62	Середня точність при суворих порогах (від 0.5 до 0.95).

Етап тестування на зображеннях валідаційної вибірки підтвердив здатність моделі працювати в складних умовах (низька якість фото, різні ракурси). Клас «helmet» розпізнається з впевненістю 0.8-0.9+ навіть при частковому перекритті об'єкта. Клас «head» ефективно ідентифікує персонал без засобів захисту, що є

критичним для систем безпеки. За підсумками експерименту згенеровано файл best.pt. Модель рекомендована до інтеграції в системи відеоаналітики реального часу для контролю використання ЗІЗ на виробництві.

#### 4.4 Висновки до четвертого розділу

У даному розділі було проведено комплексне експериментальне дослідження ефективності розробленої інтелектуальної системи автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах. Організовано тестове середовище на базі платформи Kaggle та використано відкритий датасет Hard Hat Workers, що містить зображення працівників у реальних виробничих умовах. У процесі навчання моделі протягом 25 епох зафіксовано стабільну позитивну динаміку - функції втрат продемонстрували поступове зменшення без ознак перенавчання, що підтверджує адекватність вибраної архітектури та параметрів навчання. Отримані кількісні метрики свідчать про високу якість моделі. Значення Precision (~0.94), Recall (~0.92) та mAP@0.5 (~0.95) підтверджують ефективність детекції об'єктів, зокрема засобів захисту.

Детальний аналіз матриці невідповідності продемонстрував, що модель досягає високої точності для ключових класів «helmet» та «head» (близько 94%), що підтверджує її придатність для задач контролю використання засобів індивідуального захисту. Водночас виявлено обмеження у розпізнаванні класу «person», що пояснюється дисбалансом даних або складністю візуальних ознак.

Візуальна верифікація результатів на навчальних та валідаційних вибірках підтвердила здатність моделі працювати в складних умовах: при різному освітленні, наявності шумів, частковому перекритті об'єктів та великій кількості працівників у кадрі. Модель коректно локалізує каски навіть у складних сценах, що є критично важливим для систем відеомоніторингу безпеки. Водночас зафіксовано поодинокі хибнопозитивні та хибнонегативні спрацювання, а також дублювання детекцій, що вказує на необхідність додаткового налаштування параметрів постобробки.

У цілому результати експериментального дослідження підтверджують, що розроблена система є ефективною та може бути використана для автоматизованого контролю дотримання вимог охорони праці на виробничих об'єктах. Запропонований підхід забезпечує високу точність розпізнавання засобів індивідуального захисту в реальному часі та має потенціал до інтеграції у промислові системи відеоаналітики.

## ВИСНОВКИ

У ході виконання роботи було проведено огляд існуючих рішень і систем автоматизованого розпізнавання засобів індивідуального захисту, що дозволило визначити їх переваги, недоліки та обґрунтувати доцільність використання нейронних мереж для розв'язання поставленої задачі. Виконано формалізацію задачі детекції об'єктів на зображеннях і відео, що забезпечило можливість її подальшої алгоритмічної реалізації.

Обґрунтовано вибір методів та архітектури нейронної мережі, зокрема підходу YOLO, який забезпечує ефективну детекцію об'єктів у режимі реального часу. Сформовано та підготовлено навчальний датасет, виконано його анотацію, балансування та аугментацію, що сприяло підвищенню якості навчання моделі. Реалізовано процедуру навчання та валідації моделі з використанням сучасних методів глибокого навчання, що дозволило досягти високих показників точності.

Проведено експериментальне дослідження ефективності моделі із застосуванням метрик Precision, Recall, F1-score та mAP, результати якого підтвердили доцільність запропонованого підходу.

Розроблено архітектуру інтелектуальної системи, яка включає підсистеми збору відеоданих, обробки та розпізнавання, а також візуалізації та сповіщення. Реалізовано програмно-апаратну систему, здатну функціонувати в режимі реального часу та забезпечувати автоматизований контроль використання засобів індивідуального захисту.

Отримані результати підтверджують, що поставлена мета роботи досягнута, а всі визначені задачі - виконані. Розроблена система може бути використана на практиці для підвищення рівня безпеки праці на виробничих об'єктах. Подальші дослідження доцільно спрямувати на розширення функціональності системи, покращення якості розпізнавання додаткових типів засобів індивідуального захисту, а також оптимізацію її роботи для використання на edge-пристроях.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Сайт онлайн-консультанта з охорони праці. URL: <https://ohoronapraci.com.ua/articles/76537-zasoby-individualnoho-zakhystu-pid-chas-roboty-na-vysoti> (дата звернення: 12.02.2026)
2. Охорона праці та пожежна безпека. <https://oppb.com.ua/news/shhodo-zabezpechennya-i-zastosuvannya-zasobiv-individualnogo-zahystu> (дата звернення: 12.02.2026)
3. Відеокамери.com.ua. Офіційний вебсайт. [https://xn--80adageboqrp5j.com.ua/kontrol\\_dostypu/](https://xn--80adageboqrp5j.com.ua/kontrol_dostypu/) (дата звернення: 12.02.2026)
4. Відеоспостереження на виробництві та складах. <https://control.ua/ua/blog/videonablyudenie-na-zavodah-i-proizvodstve.html> (дата звернення: 12.02.2026)
5. Закон України «Про охорону праці» № 2694-XII від 14.10.1992 р. (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/2694-12#Text> (дата звернення: 12.02.2026)
6. Кодекс законів про працю України від (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/322-08#Text> (дата звернення: 12.02.2026)
7. Про затвердження Технічного регламенту засобів індивідуального захисту : Постанова Кабінету Міністрів України № 761 від 27.08.2008 р. (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/761-2008-%D0%BF#Text> (дата звернення: 12.02.2026)
8. НПАОП 0.00-4.01-08. Положення про порядок забезпечення працівників спеціальним одягом, спеціальним взуттям та іншими засобами індивідуального захисту. URL: <https://zakon.rada.gov.ua/laws/show/z0446-08#Text> (дата звернення: 12.02.2026)
9. ДСТУ EN 397:2017. Захисні каски для промисловості. Офіційна інформація: [https://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=73706](https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=73706) (дата звернення: 12.02.2026)

10. ДСТУ EN ISO 20471:2019. Одяг сигнальний підвищеної видимості. Офіційна інформація: URL: [https://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=88071](https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88071) (дата звернення: 12.02.2026)
11. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0425> (дата звернення: 12.02.2026)
12. ISO 45001:2018 Occupational health and safety management systems – Requirements with guidance for use. Офіційна сторінка стандарту: URL: <https://www.iso.org/standard/63787.html> (дата звернення: 12.02.2026)
13. Siemens AG. Digital Industries and Industrial Security Solutions. URL: <https://www.siemens.com> (дата звернення: 12.02.2026)
14. Honeywell International Inc. Industrial Safety and Video Analytics Solutions. URL: <https://www.honeywell.com> (дата звернення: 12.02.2026)
15. Shell plc. Digitalisation and Industrial Safety Technologies. URL: <https://www.shell.com> (дата звернення: 12.02.2026)
16. BMW Group. Digitalisation in Production and Smart Factory Solutions. URL: <https://www.bmwgroup.com> (дата звернення: 12.02.2026)
17. Hikvision Digital Technology Co., Ltd. AI-powered Video Analytics Solutions. URL: <https://www.hikvision.com> (дата звернення: 12.02.2026)
18. Dahua Technology Co., Ltd. Intelligent Video Surveillance Systems. URL: <https://www.dahuasecurity.com> (дата звернення: 12.02.2026)
19. Лобода, А. І. (2025). *Автоматизований аналіз відеопотоків у системах електронних комунікацій з використанням методів комп'ютерного зору* (Магістерська дисертація, спеціальність 172 Електронні комунікації та радіотехніка). Київ.
20. Бученко, І. А., & Лащевська, Н. О. (2025). Роль периферійних обчислень (edge computing) в комп'ютерних мережах. *Зв'язок.*, (1), 23–29. <https://doi.org/10.31673/2412-9070.2025.011762>
21. Олійник, І. А. (2025). *Метод розпізнавання об'єктів у реальному часі для безпілотних літальних апаратів у завданнях розслідувань і пошукових робіт*

(Кваліфікаційна робота бакалавра, спеціальність 122 Комп'ютерні науки, Хмельницький національний університет). Хмельницький.

22. Бронецький, А. І. (2025). *Розробка масштабованої високонавантаженої системи зберігання та обробки відеоданих* (Кваліфікаційна робота бакалавра, спеціальність 122 Комп'ютерні науки, Тернопільський національний технічний університет імені Івана Пулюя). Тернопіль.

23. Bletskan D. I., Glukhov K. E., Frolova V. V. Electronic structure of 2H-SnSe<sub>2</sub>: ab initio modeling and comparison with experiment. *Semiconductor Physics, Quantum Electronics & Optoelectronics*. 2020. Vol. 19, No 1. P. 98–108.

24. Rashidi A., Woon G. L., Dasandara M., Bazghaleh M., Pasbakhsh P. Smart personal protective equipment for intelligent construction safety monitoring. *Smart and Sustainable Built Environment*. 2025. Vol. 14, No 3. P. 835–858.

25. Lema D. G., Usamentiaga R., García D. F. Low-cost system for real-time verification of personal protective equipment in industrial facilities using edge computing devices. *Journal of Real-Time Image Processing*. 2023. Vol. 20, No 6. P. 111.

26. 4. Hallonqvist, L., & Cromsjö, M. (2021). Detection of safety equipment in the manufacturing industry using image recognition.

27. 5. Vukicevic A. M., Petrovic M., Milosevic P., Peulic A., Jovanovic K., Novakovic A. A systematic review of computer vision-based personal protective equipment compliance in industry practice: advancements, challenges and future directions. *Artificial Intelligence Review*. 2024. Vol. 57, No 12. P. 319.

28. Iannizzotto G., Bello L. L., Patti G. Personal protection equipment detection system for embedded devices based on DNN and fuzzy logic. *Expert Systems with Applications*. 2021. Vol. 184. P. 115447.

29. Delhi V. S. K., Sankarlal R., Thomas A. Detection of personal protective equipment (PPE) compliance on construction site using computer vision based deep learning techniques. *Frontiers in Built Environment*. 2020. Vol. 6. P. 136.

30. Nath N. D., Behzadan A. H., Paal S. G. Deep learning for site safety: real-time detection of personal protective equipment. *Automation in Construction*. 2020. Vol. 112. P. 103085.

31. Che C., Zheng H., Huang Z., Jiang W., Liu B. Intelligent robotic control system based on computer vision technology. *arXiv preprint*. 2024. arXiv:2404.01116.
32. Луцків А., Макогон С. Типи архітектур нейронних мереж для перетворення текстових повідомлень у звуковий потік. *Комп'ютерні системи та мережі*. 2023. С. 164.
33. Lee J., Lee S. Construction site safety management: a computer vision and deep learning approach. *Sensors*. 2023. Vol. 23, No 2. P. 944..
34. Di Capua M., Ciaramella A., De Prisco A. Machine learning and computer vision for the automation of processes in advanced logistics: the integrated logistic platform (ILP) 4.0. *Procedia Computer Science*. 2023. Vol. 217. P. 326–338.
35. Zhou, D., Xu, K., Lv, Z., Yang, J., Li, M., He, F., & Xu, G. (2022). Intelligent manufacturing technology in the steel industry of China: a review. *Sensors*, 22(21), 8194.
36. Farooq, M. U., Bhutto, M. A., & Kazi, A. K. (2023). Real-Time Safety Helmet Detection Using Yolov5 at Construction Sites. *Intelligent Automation & Soft Computing*, 36(1).
37. Zhou D., Xu K., Lv Z., Yang J., Li M., He F., Xu G. Intelligent manufacturing technology in the steel industry of China: a review. *Sensors*. 2022. Vol. 22, No 21. P. 8194.
38. Toole, T. M. (2002). Construction site safety roles. *Journal of Construction Engineering and Management*, 128(3), 203–210.
39. Haikio, J., Kallio, J., Makela, S. M., & Keranen, J. (2020). IoT-based safety monitoring from the perspective of construction site workers. *International Journal of Occupational and Environmental Safety*, 4, 1–14.
40. Fang, W., Love, P. E., Ding, L., Xu, S., Kong, T., & Li, H. (2021). Computer vision and deep learning to manage safety in construction: Matching images of unsafe behavior and semantic rules. *IEEE Transactions on Engineering Management*. Advance online publication.
41. Nath, N. D., Behzadan, A. H., & Paal, S. G. (2020). Deep learning for site safety: Real-time detection of personal protective equipment. *Automation in Construction*, 112, 103085.

42. Guo, S. Y., Ding, L. Y., Luo, H. B., & Jiang, X. Y. (2016). A big-data-based platform of workers' behavior: Observations from the field. *Accident Analysis & Prevention, 93*, 299–309.
43. Azhar, S., & Behringer, A. (2013). A BIM-based approach for communicating and implementing a construction site safety plan. In *Proceedings of the 49th ASC Annual International Conference* (pp. 212–219).
44. Seo, J., Han, S., Lee, S., & Kim, H. (2015). Computer vision techniques for construction safety and health monitoring. *Advanced Engineering Informatics, 29*(2), 239–251.
45. Shapira, A., Rosenfeld, Y., & Mizrahi, I. (2008). Vision system for tower cranes. *Journal of Construction Engineering and Management, 134*(5), 320–332.
46. Awalgaonkar, N. M., Zheng, H., & Gurciullo, C. S. (2020). DEEVA: A deep learning and IoT-based computer vision system to address safety and security of production sites in energy industry. *arXiv*. <https://arxiv.org/abs/2003.01196>
47. Besl, P. J., & Jain, R. C. (1985). Three-dimensional object recognition. *ACM Computing Surveys, 17*(1), 75–145.
48. Jafri, R., Ali, S. A., Arabnia, H. R., & Fatima, S. (2014). Computer vision-based object recognition for the visually impaired in an indoors environment: A survey. *The Visual Computer, 30*, 1197–1222.
49. Wu, H., Zhong, B., Li, H., Love, P., Pan, X., & Zhao, N. (2021). Combining computer vision with semantic reasoning for on-site construction safety management. *Journal of Building Engineering, 42*, 103036.
50. Moohialdin, A., Lamari, F., Marc, M., & Trigunaryah, B. (2021). A real-time computer vision system for workers' PPE and posture detection in actual construction site environment. In *Proceedings of EASEC16* (pp. 2169–2181). Springer.
51. Fang, W., Ding, L., Love, P. E., Luo, H., Li, H., Pena-Mora, F., & Zhou, C. (2020). Computer vision applications in construction safety assurance. *Automation in Construction, 110*, 103013.

52. Chen, S., & Demachi, K. (2020). A vision-based approach for ensuring proper use of personal protective equipment (PPE) in decommissioning of Fukushima Daiichi Nuclear Power Station. *Applied Sciences*, *10*(15), 5129.
53. Balakreshnan, B., Richards, G., Nanda, G., Mao, H., Athinarayanan, R., & Zaccaria, J. (2020). PPE compliance detection using artificial intelligence in learning factories. *Procedia Manufacturing*, *45*, 277–282.
54. Delhi, V. S. K., Sankarlal, R., & Thomas, A. (2020). Detection of personal protective equipment (PPE) compliance on construction site using computer vision based deep learning techniques. *Frontiers in Built Environment*, *6*, 136.
55. Zhang, M., Shi, R., & Yang, Z. (2020). A critical review of vision-based occupational health and safety monitoring of construction site workers. *Safety Science*, *126*, 104658.
56. Tahir, N., Batureb, U., Abubakar, K., Baba, M., & Yarima, S. (2020). Image recognition based autonomous driving: A deep learning approach. *International Journal of Engineering and Manufacturing*, *10*(2), 11–19.
57. Fayou, S., Ngo, H., & Sek, Y. (2022). Combining multi-feature regions for fine-grained image recognition. *International Journal of Image, Graphics and Signal Processing*, *14*(1), 15–25.
58. Tania, M., Afroze, D., Akhter, J., Rahaman, A., & Islam, I. (2021). Image recognition using machine learning with the aid of MLR. *International Journal of Image, Graphics and Signal Processing*, *13*(1), 12–22.
59. Deng, J., Dong, W., Socher, R., Li, L. J., Li, K., & Fei-Fei, L. (2019). ImageNet: A large-scale hierarchical image database. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 248–255).
60. Torrey, L., & Shavlik, J. (2020). Transfer learning. In *Handbook of research on machine learning applications and trends* (pp. 242–264). IGI Global.
61. Pan, S. J., & Yang, Q. (2020). A survey on transfer learning. *IEEE Transactions on Knowledge and Data Engineering*, *22*(10), 1345–1359.

62. Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., & Rabinovich, A. (2015). Going deeper with convolutions. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 1–9).
63. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 770–778).
64. Simonyan, K., & Zisserman, A. (2022). Very deep convolutional networks for large-scale image recognition. *arXiv*. <https://arxiv.org/abs/1409.1556>
65. Redmon, J., & Farhadi, A. (2018). YOLOv3: An incremental improvement. *arXiv*. <https://arxiv.org/abs/1804.02767>
66. Bradski, G., & Kaehler, A. (2018). *Learning OpenCV: Computer vision with the OpenCV library*. O'Reilly Media.
67. Lin, T. Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., & Zitnick, C. L. (2024). Microsoft COCO: Common objects in context. In *European Conference on Computer Vision* (pp. 740–755). Springer.
68. Sauvola, J., & Pietikäinen, M. (2020). Adaptive document image binarization. *Pattern Recognition*, 33(2), 225–236.
69. Vincent, L. (2023). Morphological grayscale reconstruction in image analysis: Applications and efficient algorithms. *IEEE Transactions on Image Processing*, 2(2), 176–201.
70. Adelson, E. H., Anderson, C. H., Bergen, J. R., Burt, P. J., & Ogden, J. M. (2024). Pyramid methods in image processing. *RCA Engineer*, 29(6), 33–41.
71. Wang, Y., Chen, Q., & Zhang, B. (2020). Image enhancement based on equal area dualistic sub-image histogram equalization method. *IEEE Transactions on Consumer Electronics*, 45(1), 68–75.
72. Cheng, H. D., Jiang, X. H., Sun, Y., & Wang, J. (2021). Color image segmentation: Advances and prospects. *Pattern Recognition*, 34(12), 2259–2281.
73. Ketkar, N. (2017). Introduction to Keras. In *Deep learning with Python* (pp. 97–111). Manning Publications.

74. Everingham, M., Van Gool, L., Williams, C. K., Winn, J., & Zisserman, A. (2020). The PASCAL visual object classes (VOC) challenge. *International Journal of Computer Vision*, 88(2), 303–338.
75. Andriluka, M., Pishchulin, L., Gehler, P., & Schiele, B. (2024). 2D human pose estimation: New benchmark and state of the art analysis. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 3686–3693).
76. Güler, R. A., Neverova, N., & Kokkinos, I. (2018). DensePose: Dense human pose estimation in the wild. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 7297–7306).
77. ONVIF. Стандарт інтеграції IP-камер. *ONVIF™ core specification (Version 2.2)*. URL: <http://www.onvif.org/specs/DocMap.html> (дата звернення: 12.02.2026)
78. PyTorch. Офіційна документація PyTorch. URL: <https://pytorch.org/docs/stable/index.html> (дата звернення: 12.02.2026)
79. TensorFlow. Офіційна документація TensorFlow. URL: [https://www.tensorflow.org/api\\_docs](https://www.tensorflow.org/api_docs) (дата звернення: 12.02.2026)
80. Keras. API для побудови нейронних мереж. URL: <https://keras.io> (дата звернення: 12.02.2026)
81. Ultralytics. Офіційна документація моделей YOLO (YOLOv5, YOLOv8). URL: <https://docs.ultralytics.com> (дата звернення: 12.02.2026)
82. Датасет для навчання нейронної мережі. URL: <https://public.roboflow.com/object-detection/hard-hat-workers> (дата звернення 21.02.2026)
83. Метрики оцінки ефективності. URL: <https://docs.ultralytics.com/ru/guides/yolo-performance-metrics/> (дата звернення 21.02.2026)
84. Kaggle. Офіційний вебсайт. URL: <https://www.kaggle.com/> (дата звернення 28.03.2026)

85. Fire & Smoke Detection camera - AVIOTEC 8000i IR. URL: <https://www.boschbuildingtechnologies.com/lifesafetysystems/en/products/fire-and-smoke-detection-camera> (дата звернення 01.04.2026)

86. Edge AI and Edge Computing: Powering real-time intelligence. URL: <https://www.ultralytics.com/blog/edge-ai-and-edge-computing-powering-real-time-intelligence> (дата звернення 01.04.2026)

87. Міні-комп'ютер NVIDIA Jetson Orin Nano Developer Kit. URL: <https://arduino.ua/prod7101-nvidia-jetson-orin-nano-developer-kit?srsId=AfmBOoodcteQnuCk34rHIKdQ45qXHI7fi7SBPrUasrNQptP3FDSIJjhx> (дата звернення 01.04.2026)

88. Суперкомп'ютер NVIDIA Jetson Xavier NX. URL: <https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/jetson-xavier-nx> (дата звернення 01.04.2026)

89. NVIDIA GeForce RTX. URL: <https://a16z.com/building-an-efficient-gpu-server-with-nvidia-geforce-rtx-4090s-5090s> (дата звернення 01.04.2026)

90. Марчук Р.Е., Лигун О.О. Концепція методу автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах. Матеріали XIX Всеукраїнської науково практичної WEB конференції аспірантів, студентів та молодих вчених (25-27 березня 2026 р.). Кривий Ріг: Криворізький національний університет, 2026. с. 262-264.

## ДОДАТОК А

(обов'язковий)

Публікація результатів дослідження

*Марчук Р.Е.,  
Хмельницький національний університет  
Лигун О.О.  
асистент, Хмельницький національний університет*

### **КОНЦЕПЦІЯ МЕТОДУ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ЗАСОБІВ ІНДИВІДУАЛЬНОГО ЗАХИСТУ НА ВИРОБНИЧИХ ОБ'ЄКТАХ**

*Розглянуто проблему автоматизованого контролю використання засобів індивідуального захисту на виробничих об'єктах. Запропоновано концепцію методу автоматичного розпізнавання засобів індивідуального захисту на основі алгоритмів комп'ютерного зору та глибокого навчання. Описано покрокову структуру методу та архітектуру інтелектуальної комп'ютерної системи для його реалізації в режимі реального часу.*

Забезпечення дотримання вимог охорони праці на виробничих об'єктах є одним із ключових чинників зниження рівня виробничого травматизму. Незважаючи на наявність нормативних вимог щодо обов'язкового використання засобів індивідуального захисту (ЗІЗ), контроль їх застосування здебільшого здійснюється вручну, що обмежує оперативність реагування та підвищує вплив людського фактора.

Сучасні дослідження у сфері комп'ютерного зору демонструють високу ефективність застосування згорткових нейронних мереж та архітектур сімейства YOLO для задач детекції об'єктів у реальному часі. Зокрема, Nath та ін. [1] запропонували підхід до виявлення засобів індивідуального захисту на будівельних майданчиках із використанням глибокого навчання. Vukicevic та ін. [2] у систематичному огляді підкреслюють актуальність інтеграції

алгоритмів комп'ютерного зору з промисловими інформаційними системами та необхідність підвищення стійкості моделей до складних умов експлуатації.

У роботі запропоновано концепцію методу автоматичного розпізнавання ЗІЗ, що базується на детекції працівників та подальшій перевірці наявності обов'язкових елементів захисту (каска, сигнальний жилет тощо) у кожного виявленого об'єкта.

Метод автоматичного розпізнавання засобів індивідуального захисту (ЗІЗ) реалізується як послідовність взаємопов'язаних етапів обробки відеоданих, починаючи з отримання зображення та завершуючи формуванням рішення щодо відповідності вимогам безпеки.

Крок 1. Захоплення відеопотоку. На першому етапі здійснюється отримання відеопотоку з IP-камер, встановлених на виробничому об'єкті.

Крок 2. Попередня обробка зображення. Для забезпечення стабільної роботи алгоритмів комп'ютерного зору виконується попередня обробка кожного кадру.

Крок 3. Детекція об'єкта «Працівник». На третьому етапі застосовується модель глибокого навчання для локалізації людей у кадрі.

Крок 4. Детекція елементів засобів індивідуального захисту. Після виявлення працівників у межах кожної області інтересу виконується пошук окремих елементів ЗІЗ. Система визначає наявність або відсутність каски, сигнального жилета тощо.

Крок 5. Логічна перевірка відповідності.  
Для кожного працівника формується вектор відповідності:

$Worker_i = \{Helmet, Vest, Gloves, Glasses\}$ , де кожен елемент набуває значення 1 (виявлено) або 0 (не виявлено). Далі виконується перевірка відповідності нормативним вимогам. Якщо набір виявлених засобів задовольняє визначений перелік обов'язкових елементів, працівник вважається таким, що дотримується вимог безпеки.

Крок 6. Формування рішення. На основі результатів логічної перевірки система формує підсумкове рішення для кожного працівника.

Крок 7. Генерація події та реагування.

У разі виявлення порушення система автоматично генерує подію. Вона включає створення сигналу тривоги, збереження відповідного фрагмента відео та журналювання інформації про інцидент у базі даних. Це забезпечує можливість подальшого аналізу та оперативного реагування відповідальних осіб.

Візуалізація роботи методу у вигляді діаграми наведена на рисунку 1.



Рисунок 1 – Візуалізація роботи методу автоматичного розпізнавання ЗІЗ на виробничих об'єктах

Запропонований підхід забезпечує підвищення оперативності контролю, зменшення впливу людського фактора та можливість масштабування рішення для великих промислових підприємств. Подальші дослідження спрямовані на експериментальну перевірку ефективності методу та оптимізацію параметрів моделі для роботи в умовах змінного освітлення та часткових перекриттів об'єктів.

#### ЛІТЕРАТУРА

1. Nath N. D., Behzadan A. H., Paal S. G. (2020). Deep learning for site safety: Real-time detection of personal protective equipment. *Automation in Construction*. 112, 103085.
2. Vukicevic A. M., Petrovic M., Milosevic P., Peulic A., Jovanovic K., Novakovic A. (2024). A systematic review of computer vision-based personal protective equipment compliance in industry practice: advancements, challenges and future directions. *Artificial Intelligence Review*. 57(12), 319.

## ДОДАТОК Б

### Слайди презентації доповіді



Кваліфікаційна робота магістра  
за спеціальністю 123 – комп'ютерна інженерія

## **Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах**

Марчук Ростислав Едуардович  
Студент групи КІ2М-24-1

Керівник: д.т.н., професор  
Савенко Олег Станіславович

Хмельницький - 2026

## **Мета, об'єкт та предмет роботи**

**Мета:** є розробити метод та інтелектуальну комп'ютерну систему автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах на основі методів комп'ютерного зору та глибокого навчання, що забезпечує підвищення рівня безпеки праці шляхом автоматизованого контролю дотримання вимог охорони праці в режимі реального часу.

**Об'єкт дослідження:** процеси автоматизованого відеомоніторингу та контролю використання засобів індивідуального захисту на виробничих об'єктах.

**Предмет дослідження:** методи, алгоритми та програмно-апаратні засоби розпізнавання об'єктів на зображеннях і відео, зокрема засобів індивідуального захисту, із використанням технологій комп'ютерного зору та глибокого навчання.

## Завдання роботи

Удосконалити існуючі методи та алгоритми автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах на основі технологій комп'ютерного зору з метою розробки інтелектуальної системи контролю дотримання вимог охорони праці.

Поставлена мета досягається розв'язанням таких основних задач:

1. провести огляд існуючих рішень та систем автоматизованого розпізнавання засобів індивідуального захисту на виробництві;
2. виконати формалізацію задачі детекції засобів індивідуального захисту на зображеннях та відео;
3. обґрунтувати вибір методів і архітектури нейронної мережі для розпізнавання об'єктів;
4. провести експериментальне дослідження ефективності розробленої моделі з використанням відповідних метрик оцінювання;
5. розробити архітектуру інтелектуальної системи, що включає підсистеми збору, обробки та візуалізації відеоданих;
6. реалізувати програмно-апаратну систему автоматичного розпізнавання засобів індивідуального захисту в режимі реального часу.

## Наукова новизна

1. Удосконалено метод автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах із використанням нейронних мереж типу YOLO, що забезпечує підвищення точності детекції в умовах складного виробничого середовища.
2. Набула подальшого розвитку інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах, в якій на відміну від відомих використано комбінований підхід до обробки відеопотоку на основі сучасних нейронних мереж типу YOLO та механізмів попередньої обробки зображень, що дозволяє підвищити точність детекції об'єктів в умовах складного освітлення, часткових перекриттів та різноманітних ракурсів;

**Практична цінність** отриманих результатів полягає у розробці інтелектуальної комп'ютерної системи для автоматизованого розпізнавання засобів індивідуального захисту на виробничих об'єктах .

**Апробація результатів:** Марчук Р.Е., Лигун О.О. КОНЦЕПЦІЯ МЕТОДУ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ЗАСОБІВ ІНДИВІДУАЛЬНОГО ЗАХИСТУ НА ВИРОБНИЧІХ ОБ'ЄКТАХ. *Матеріали XLIX Всеукраїнської науково-практичної WEB конференції аспірантів, студентів та молодих вчених (25-27 березня 2026 р.). – Кривий Ріг: Криворізький національний університет, 2026. с. 262-264. – тези участі у Всеукраїнській науково-практичній конференції*

## Розділ 1: Огляд існуючих рішень



## Розділ 1: Огляд існуючих рішень



## Розділ 1: Огляд існуючих рішень

Нормативний документ	Рівень регулювання	Основні положення щодо ЗІЗ
Закон України «Про охорону праці» № 2694-ХІІ від 14.10.1992	Національний	Встановлює обов'язок роботодавця забезпечувати працівників ЗІЗ та здійснювати контроль за їх використанням
Кодекс законів про працю України	Національний	Регламентує права працівників на безпечні умови праці
Технічний регламент засобів індивідуального захисту (Постанова КМУ № 761 від 27.08.2008, зі змінами)	Національний	Визначає вимоги до відповідності, маркування та введення в обіг ЗІЗ
НПАОП 0.00-4.01-08 «Положення про порядок забезпечення працівників спеціальним одягом, спеціальним взуттям та іншими ЗІЗ»	Галузевий	Встановлює порядок забезпечення, обліку та контролю використання ЗІЗ
ДСТУ EN 397:2017 (Захисні каски для промисловості)	Національний стандарт	Визначає технічні вимоги до захисних касок

## Розділ 2: Метод автоматичного розпізнавання ЗІЗ



Нехай:

$V(t)$  - відеопотік з камери спостереження на виробничому об'єкті.

$I_k$  -  $k$ -тий вхідний кадр відеопотоку з камери відеоспостереження,  $I_k \in R^{H \times W \times C}$  (для RGB  $C=3$ ).

$P = \{p_1, p_2, \dots, p_n\}$  - множина виявлених працівників у кадрі.

$E = \{e_1, e_2, \dots, e_m\}$  - множина елементів ЗІЗ (захисний шолом, жилет, перчатки тощо.)

Загальна функціональна схема методу може бути представлена як композиція операторів (формула 2.1).

$$F = f_{decision} \circ f_{logic} \circ f_{detect} \circ f_{pre} \circ f_{input}, \quad (2.1)$$

де:

$f_{input}$  - оператор отримання кадру;

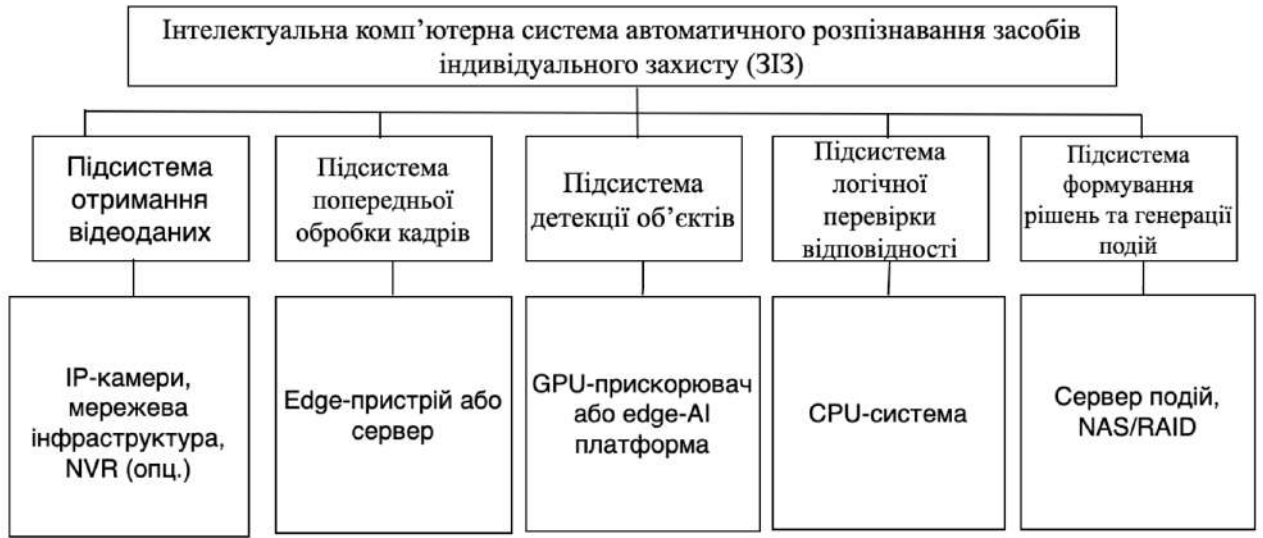
$f_{pre}$  - оператор попередньої обробки;

$f_{detect}$  - оператор детекції працівників та ЗІЗ;

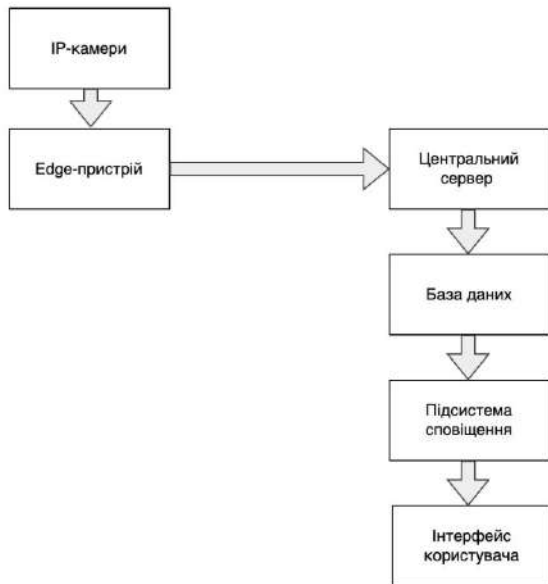
$f_{logic}$  - оператор перевірки відповідності;

$f_{decision}$  - формування кінцевого рішення.

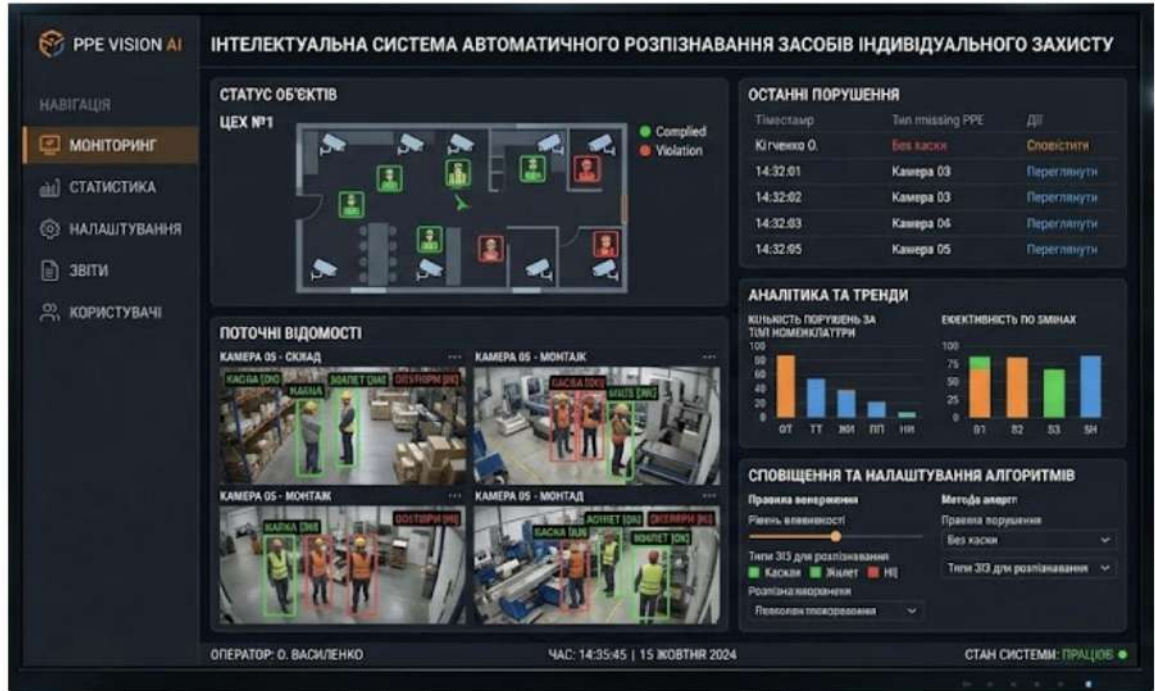
### Розділ 3: Проектування та реалізація інтелектуальної комп'ютерної системи



### Розділ 3: Проектування та реалізація інтелектуальної комп'ютерної системи



## Розділ 3: Проєктування та реалізація інтелектуальної комп'ютерної системи



## Розділ 4: Експерименти та результати

The screenshot shows the Roboflow website interface for the 'Hard Hat Workers Dataset'. The page includes the following elements:

- Navigation:** 'Universe', 'Public Datasets', 'Model Zoo', 'Blog', 'Docs', and a 'Download' button.
- Header:** 'Explore these datasets, models, and more on Roboflow Universe.' with statistics: '350+ MILLION IMAGES', '300,000+ DATASETS', and '100,000+ PRE-TRAINED MODELS'.
- Dataset Summary:** 'Hard Hat Workers Dataset >> raw\_75-25\_trainTestSplit'.
  - Export Created: 6 years ago (April 27, 2020)
  - Export Size: 7041 images
  - Annotations: Workers
- Available Download Formats:** A grid of buttons for various formats: COCO JSON, COCO-MMDetection, CreateML JSON, PaliGamma JSONL, Pascal VOC XML, YOLO Darknet TXT, YOLO v3 Keras TXT, YOLO v4 PyTorch, Scaled-YOLOv4, YOLOv5-CBB, MT-YOLOv6, YOLO v5 PyTorch, YOLO v7 PyTorch, YOLOv8, YOLOv8-CBB, YOLOv9, YOLOv10, YOLOv11, YOLOv12, RetinaNet Keras CSV, Multiclass Classification, OpenAI CLIP Classification, and Tensorflow TFRecord.
- Preview:** A grid of image thumbnails showing workers in various industrial settings.

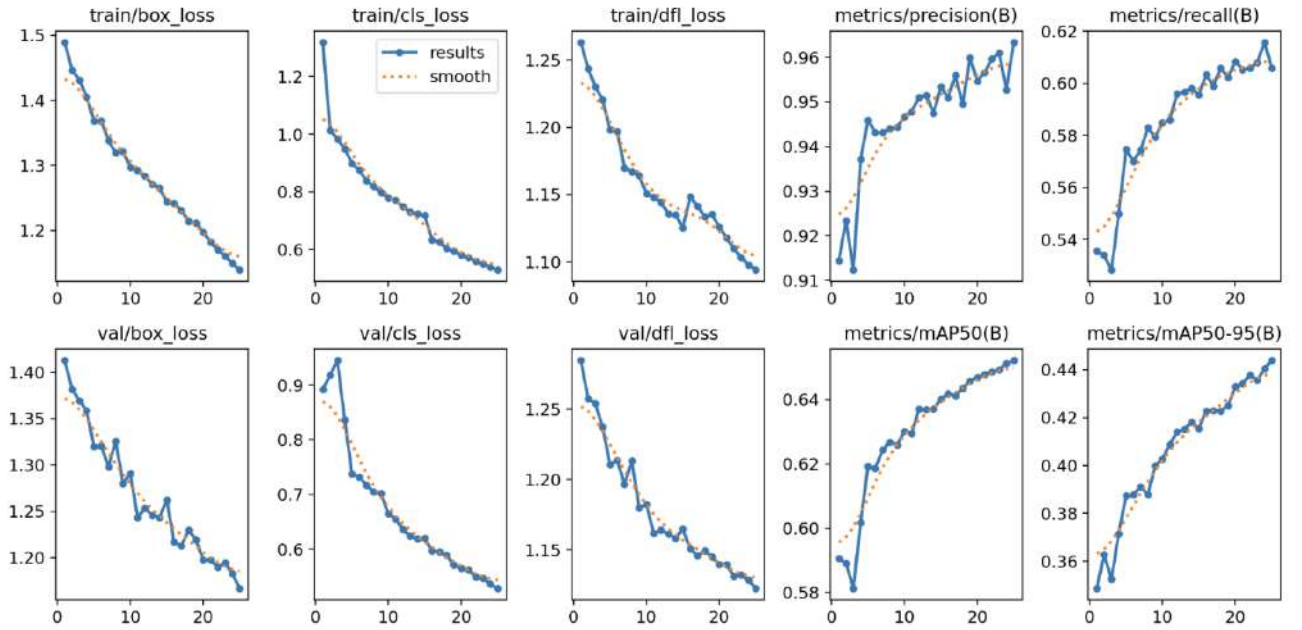
## Розділ 4: Експерименти та результати



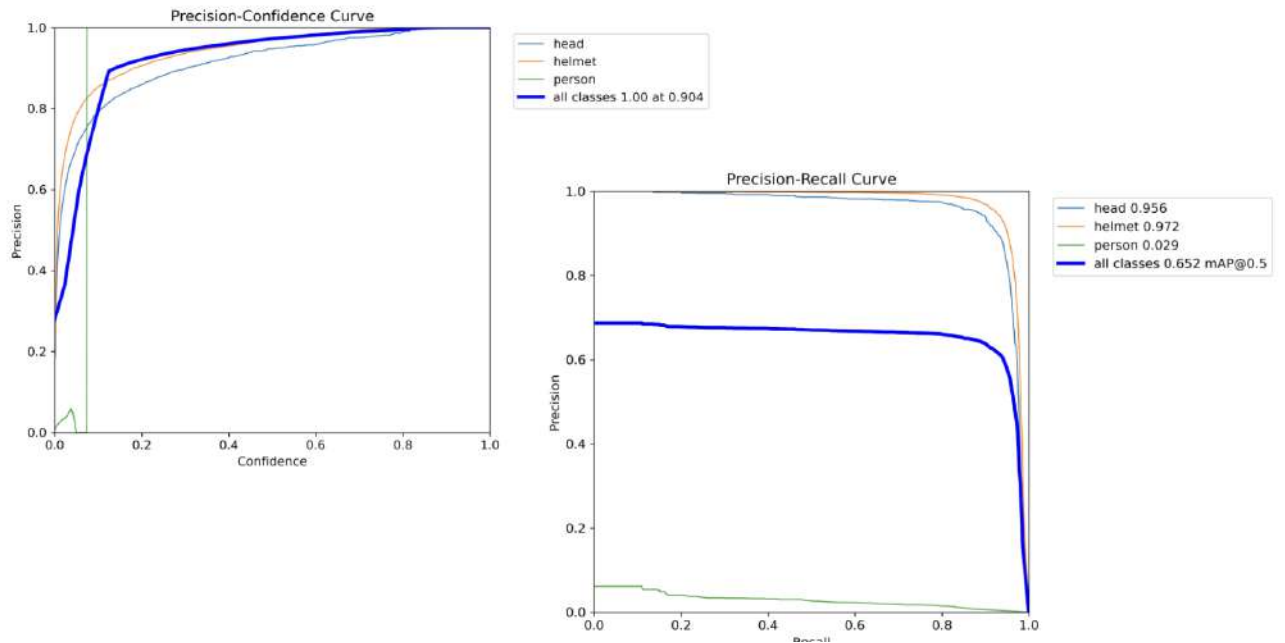
## Розділ 4: Експерименти та результати

Параметр	Значення	Пояснення
Model	yolo11s.pt	Використана "мала" версія архітектури <u>YOLO11</u> для забезпечення високого FPS.
Img size (imgsz)	640	Роздільна здатність вхідних зображень (640x640 пікселів).
Epochs	25	Кількість повних проходів через тренувальний набір даних.
Batch size	16	Кількість зображень, що обробляються за одну ітерацію.
IOU threshold	0.7	Поріг перекриття для фільтрації дубльованих рамок детекції.

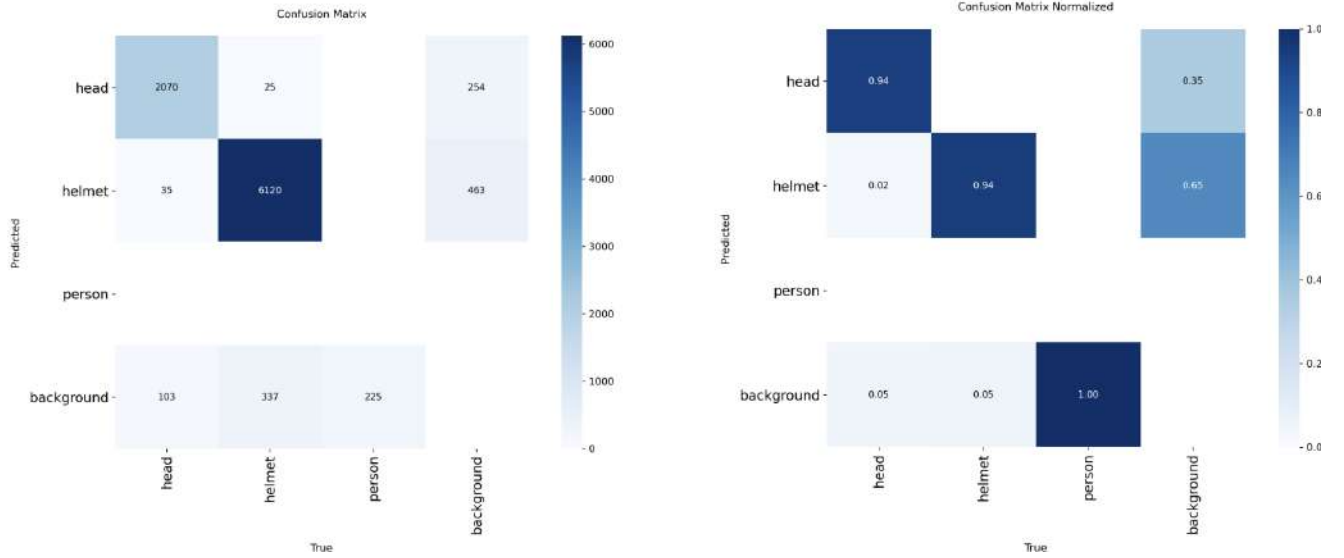
## Розділ 4: Експерименти та результати



## Розділ 4: Експерименти та результати



# Розділ 4: Експерименти та результати



# Розділ 4: Експерименти та результати



## Розділ 4: Експерименти та результати

Метрика	Значення	Інтерпретація
Precision	~0.94	94% об'єктів, позначених моделлю як "шолом", дійсно ними є.
Recall	~0.92	Моделю успішно знаходить 92% усіх реальних шоломів у кадрі.
mAP50	~0.95	Середня точність при порозі перекриття 0.5 (дуже високий показник).
mAP50-95	~0.62	Середня точність при суворих порогах (від 0.5 до 0.95).

### Висновки

У ході виконання роботи було проведено огляд існуючих рішень і систем автоматизованого розпізнавання засобів індивідуального захисту, що дозволило визначити їх переваги, недоліки та обґрунтувати доцільність використання нейронних мереж для розв'язання поставленої задачі. Виконано формалізацію задачі детекції об'єктів на зображеннях і відео, що забезпечило можливість її подальшої алгоритмічної реалізації.

Обґрунтовано вибір методів та архітектури нейронної мережі, зокрема підходу YOLO, який забезпечує ефективну детекцію об'єктів у режимі реального часу. Сформовано та підготовлено навчальний датасет, виконано його анотацію, балансування та аугментацію, що сприяло підвищенню якості навчання моделі. Реалізовано процедуру навчання та валідації моделі з використанням сучасних методів глибокого навчання, що дозволило досягти високих показників точності.

Проведено експериментальне дослідження ефективності моделі із застосуванням метрик Precision, Recall, F1-score та mAP, результати якого підтвердили доцільність запропонованого підходу. Розроблено архітектуру інтелектуальної системи, яка включає підсистеми збору відеоданих, обробки та розпізнавання, а також візуалізації та сповіщення. Реалізовано програмно-апаратну систему, здатну функціонувати в режимі реального часу та забезпечувати автоматизований контроль використання засобів індивідуального захисту.

Отримані результати підтверджують, що поставлена мета роботи досягнута, а всі визначені задачі - виконані. Розроблена система може бути використана на практиці для підвищення рівня безпеки праці на виробничих об'єктах. Подальші дослідження доцільно спрямувати на розширення функціональності системи, покращення якості розпізнавання додаткових типів засобів індивідуального захисту, а також оптимізацію її роботи для використання на edge-пристроях.

Зав. кафедри КПС  
д-р. філософії Ользі ПАВЛОВІЙ

Ростислав МАРЧУК

---

ІІБ здобувача вищої освіти

ФІТ. 2 курсу, групи КІ2М-24-1

### ЗАЯВА

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

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

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

1 травня 2026 року



РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Ростислав Марчук

Тема: Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень \_\_\_\_\_; кількість сторінок записки 80

1. Короткий зміст роботи та прийнятих рішень. У роботі розглянуто проблему автоматизованого контролю використання засобів індивідуального захисту на виробничих об'єктах. Запропоновано метод розпізнавання ЗІЗ на основі нейронних мереж та розроблено інтелектуальну систему відеоаналізу. Реалізовано архітектуру системи, що включає підсистеми збору відеоданих, обробки та розпізнавання, а також візуалізації результатів. Проведено експериментальні дослідження ефективності моделі.

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

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз сучасних методів комп'ютерного зору та існуючих систем контролю використання засобів індивідуального захисту. У другому розділі розроблено метод автоматичного розпізнавання ЗІЗ, виконано формалізацію задачі, обґрунтовано вибір нейронної мережі та описано процес підготовки даних і навчання моделі. У третьому розділі запропоновано архітектуру інтелектуальної системи та описано її програмно-апаратну реалізацію. У четвертому розділі проведено експериментальне дослідження та оцінювання ефективності системи із використанням сучасних метрик.

4. Позитивні сторони роботи: Робота має практичну спрямованість та присвячена актуальній задачі підвищення безпеки праці. Запропоновано ефективний підхід до розпізнавання засобів індивідуального захисту в режимі реального часу. Використано сучасні методи глибокого навчання та досягнуто високих показників точності. Архітектура системи є масштабованою та придатною для впровадження у виробничих умовах.

5. Негативні сторони роботи: У роботі недостатньо розглянуто питання розпізнавання менш представлених класів об'єктів, зокрема «person», що вплинуло на якість моделі для цього класу.

6. Оцінка графічного оформлення та пояснювальної записки роботи: =

7. Відгук про роботу в цілому: В загальному робота виконана на високому науково-технічному рівні.

8. Інші зауваження: =

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «добре» 85.00 (B)

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

Бедрашні Леонід Леонідович, з.св. каф. ІІІЗ, УДУ

“ 04 ” 05 2026р.



## Протокол аналізу звіту подібності експертом

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

**Автор:** Ростислав МАРЧУК

**Співавтор:**

**Назва:** Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах

**Експерт:** Олег САВЕНКО

**Підрозділ:** Кафедра комп'ютерної інженерії та інформаційних систем

**Коефіцієнт подібності 1:** 8.54%

**Коефіцієнт подібності 2:** 3.76%

**Мікропробіли:** 7

**Заміна букв:** 6

**Інтервали:** 0

**Білі знаки:** 5

**Дата створення звіту:** 2026-04-29 16:34:32.0

Після аналізу Звіту подібності констатую наступне:

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

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

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

Обґрунтування:

2026-04-29

Дата



Доцент Андрій Нічепорук

експерт

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

**Максимальне співпадіння з одним документом 20.0%**

Словники перевірки: en\_US, ru\_RU, ua\_UA. Помилки в документах: 12%

ID: 270805 Назва: МКР Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах Додано в БД: 2026-04-29 Автора: Ростислав МАРЧУК Керівники: Олег САВЕНКО Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	116741	906	24528 (21%)	199 (22%)

## Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми
269755	Назва: Звіт з ПДП Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах Додано в БД: 2026-03-11 Автора: Р. Е. Марчука Керівники: Капустян М.В Консультанти: Опоненти:	23027 (20.0%)	187 (21.0%)

## РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

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

Назва кваліфікаційної роботи Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах  
 Автор Ростислав МАРЧУК  
 Освітня програма Комп'ютерна інженерія та програмування  
 Рівень вищої освіти другий (магістерський)  
 Спеціальність 123 Комп'ютерна інженерія  
 Науковий керівник: д.т.н., професор Олег САВЕНКО

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

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

#### Підтвердження:

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

- 1) усі запозичення фрагментарні, або мають належним чином оформлені посилання;
- 2) окремі виявлені збіги є загальноживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;
- 3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.
- 4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 8,54%; та системою Anti-Plagiarism складає 20% і адресується на «Звіт з ПДП Метод та інтелектуальна комп'ютерна система автоматичного розпізнавання засобів індивідуального захисту на виробничих об'єктах» автор роботи: Р. Е. Марчука, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

29.04.2026

Завідувач кафедри

Гарант освітньої програми

Керівник кваліфікаційної роботи

  
Підпис  
  
Підпис  
  
Підпис

Ольга ПАВЛОВА  
Ім'я, ПРІЗВИЩЕ

Олег САВЕНКО  
Ім'я, ПРІЗВИЩЕ

Олег САВЕНКО  
Ім'я, ПРІЗВИЩЕ