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

# КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Метод та засоби виявлення аномалій в кіберфізичних системах комп'ютерного зору»

КвРКІ. 170140.21.01.12 ПЗ

Виконав: студент 2 курсу, група КІ2м-21-1 _____ Олександр КЛЕЙН
Підпис Ім'я, прізвище

Керівник канд. техн. наук, доцент _____ Дмитро МЕДЗАТИЙ
Науковий ступінь, вчене звання Підпис Ім'я, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Тетяна ГОВОРУЩЕНКО
__ 05 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

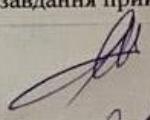
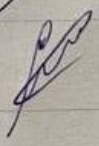
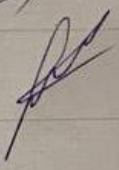
ЗАТВЕРДЖУЮ
Зав. кафедри КІІС
Тетяна ГОВОРУЩЕНКО
"01" 09 2022 р.

**ЗАВДАННЯ**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Клейн Олександр Миколайович
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод та засоби виявлення аномалій в кіберфізичних системах комп'ютерного зору
Керівник проекту (роботи) к.т.н., доцент Медзатий Д.М.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
Затверджена наказом ректора університету від 09.01.2023р. № 1
2. Строк подання студентом проекту (роботи) на кафедру 03.05.2023 р.
3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз відомих методів виявлення аномалій комп'ютерного зору
Архітектура кіберфізичних систем комп'ютерного зору
Метод виявлення аномалій в зображеннях кіберфізичними системами комп'ютерного зору
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів дипломного проекту (роботи)

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Нормоконтроль | Лисенко С.М., професор кафедри КІІС |  |  |
| Антиплагіат | Нічепорук А.О., доцент кафедри КІІС |  |  |

7. Дата видачі завдання «_06_»_____09_____2022 р.

## КАЛЕНДАРНИЙ ПЛАН

| №з/п | Назва етапів (розділів) дипломного проекту (роботи) | Термін виконання етапів проекту (роботи) | Примітка |
|---|---|---|---|
| 1 | Вибір напряму дослідження та узгодження тематики ДРМ з керівником | 01.09.2022 | виконано |
| 2 | Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження | 05.10.2022 | виконано |
| 3 | Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі | 05.11.2022 | виконано |
| 4 | Робота над розділом 2 – розробка архітектури для вирішення поставленої задачі | 05.12.2022 | виконано |
| 5 | Робота над науковою статтею та тезами | 05.01.2023 | виконано |
| 6 | Робота над розділом 3 – розробка методу для вирішення поставленої задачі | 15.02.2023 | виконано |
| 7 | Робота над розділом 4 – проектування та розробка засобів для вирішення поставленої задачі, експериментальна частина | 15.04.2023 | виконано |
| 8 | Оформлення пояснювальної записки згідно вимог | 25.04.2023 | виконано |
| 9 | Попередній захист ВКР | 28.04.2023 | виконано |
| 10 | Захист ВКР на засіданні ЕК | До 30.05.2023 | |

**Студент**  Олександр КЛЕЙН
Підпис Ініціали, прізвище

**Керівник роботи**  Дмитро МЕДЗАТИЙ
Підпис Ініціали, прізвище

# РЕФЕРАТ

Тема дипломної роботи: Метод та засоби виявлення аномалій в кіберфізичних системах комп’ютерного зору

Автор роботи: Клейн Олександр Миколайович

Керівник роботи: Медзатий Д.М.

Пояснювальна записка: 104 с., 3 рис., 81 джерело.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: виявлення аномалій; кіберфізичні системи; комп’ютерний зір.

Об’єктом дослідження є процес виявлення аномалій в кіберфізичних системах комп’ютерного зору.

Предметом дослідження є методи виявлення аномалій в кіберфізичних системах комп’ютерного зору.

Метою кваліфікаційої роботи є розробка методу виявлення аномалій в кіберфізичних системах комп’ютерного зору.

Для розв’язання поставлених задач використовувалися методи теорії комп’ютерних мереж, архітектури комп’ютерів, теорії множин, статисничного аналізу.

Наукова новизна отриманих результатів:

- вперше розроблено метод виявлення аномалій в зображеннях кіберфізичними системами комп’ютерного зору;
- удосконалено архітектуру кіберфізичних систем комп’ютерного зору.

На основі проведених досліджень розроблена архітектура кіберфізичних систем комп’ютерного зору та метод виявлення аномалій в зображеннях, який імплементовано в обчислювальну підсистему кіберфізичної системи.

Практична значимість отриманих результатів полягає у розробленій архітектурі кіберфізичних систем комп’ютерного зору.

**ЗМІСТ**

# СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БД - база даних

ОС - операційна система

ПЗ - програмне забезпечення

КФС – кіберфізична система

ШНМ – штучна нейронна мережа

# ВСТУП

Для виявлення аномалій в зображеннях розроблено багато методів. Важливим напрямом є задачі, в яких потрібно виявити аномалії, коли об’єкти перебувають в русі. З розвитком більш досконалого обміну даними інфраструктури, такої як Інтернет речей з’явилась можливість отримання таких зображень в реальному часі з відеокамер в статичному і динамічному режимах з подальшою їх обробкою. Таку систему доцільно реалізувати як кіберфізичну. В ній стало б можливим отримувати зображення, використання відеозасобів для збору зображень як статичних так і динамічних, а також їх обробка і подальше уточнення за потреби. Інтелектуальні системи комп’ютерного зору є одним з основних компонентів інтелектуального аналізу даних.

Інтелектуальні системи зору та аналітика - це активна дослідницька область, яка поєднує комп'ютерний зір, обробку сигналів та машинне навчання для вилучення та аналізу цінної та значущої інформації з необроблених даних датчиків зору.

Ці системи повинні мати можливість приймати рішення з мінімальною людською взаємодією або навіть без будь-яких людських взаємодій. Системи аналізу зору повинні розуміти місце події шляхом класифікації та відстеження об'єктів, а також вивчення їх поведінки. Однією з найважливіших частин візуального аналізу є виявлення аномалій. Актуальність роботи полягає в необхідності створити кіберфізичну систему комп’ютерного зору з відеокамерами як давачами і розробити метод обробки статичних і динамічних зображень згідно виявлення в них аномалій.

Метою кваліфікаційої роботи є розробка методу виявлення аномалій в кіберфізичних системах комп’ютерного зору.

Поставлена мета досягається розв’язанням таких основних задач:

– проаналізувати відомі методи виявлення аномалій в рухомих зображеннях;

– розробити метод виявлення аномалій в зображеннях кіберфізичними системами комп’ютерного зору;

– удосконалити архітектуру кіберфізичних систем комп’ютерного зору;

– здійснити постановку експерименту та провести еспериментальні дослідження згідно розроблених рішень.

Об’єктом дослідження є процес виявлення аномалій в кіберфізичних системах комп’ютерного зору.

Предметом дослідження є методи виявлення аномалій в кіберфізичних системах комп’ютерного зору.

Наукова новизна отриманих результатів:

– вперше розроблено метод виявлення аномалій в зображеннях кіберфізичними системами комп’ютерного зору;
– удосконалено архітектуру кіберфізичних систем комп’ютерного зору.

На основі проведених досліджень розроблена архітектура кіберфізичних систем комп’ютерного зору та метод виявлення аномалій в зображеннях, який імплементовано в обчислювальну підсистему кіберфізичної системи. Практична значимість отриманих результатів полягає у розробленій архітектурі кіберфізичних систем комп’ютерного зору.

Для розв’язання поставлених задач використовуються основні положення методи теорії комп’ютерних мереж, архітектури комп’ютерів, кіберфізичних систем, розпізнавання образів, виявлення аномалій.

За темою кваліфікаційної роботи опубліковано дві публікації у Збірнику наукових праць за матеріалами XIV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2022». (Хмельницький – 2022. – С.139-141) та у матеріалах 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2023, Vol. 3373, Khmelnytskyi, 22-24 March 2023. – Khmelnytskyi, 2023. – P. 401–410.) [80]. [81]

# 1 АНАЛІЗ МЕТОДІВ І ТЕХНОЛОГІЙ ВИЯВЛЕННЯ АНОМАЛІЙ ТА КОМП'ЮТЕРНОГО ЗОРУ

## 1.1. Аналіз предметної області

Виявлення аномалій найбільш вивчене предметне полем у машинному навчанні та інтелектуальному аналізі даних, які в основному зосереджені на виявленні будь-якої аномальної поведінки. Виявлення аномалій традиційно використовується для очищення даних, тобто виявлення певних екземплярів або вимірювань в наборі даних, що здійснюється засобами статистичного аналізу. Це застосування виявлення аномалій складається з десяти, заснованих на виявленні аномальних спостережень, які мають низьку схожість з усім набором даних [1-3].

З розвитком більш досконалого обміну даними інфраструктури, такої як Інтернет речей (IoT), продемонстрували зростаючий інтерес до використання візуального виявлення аномалій як ключового програмного елемента для безперервного моніторингу складних середовищ. У цьому контексті виявлення аномалій використовувалося для виявлення аномальної/незвичайної поведінки/змін у межах спостережуваного об'єкту. Ці зміни можуть відповідати дефекту виробничої лінії, поведінки людини, а також незвичайної поведінка дорожнього руху, зафіксована за допомогою записів відеоспостереження. Спрямування цієї роботи полягає у проблемах, що виникають для практичного застосування візуального виявлення аномалій. Такі програми включають: виявлення незвичної поведінки людини на виробництві, (2) виявлення виготовлених дефектів та (3) виявлення ненормальної поведінки людини з відео спостереження за камерою відеоспостереження, де коригування рівня кадру є недоступним.

Інтелектуальна система зору є одним з основних компонентів інтелектуального аналізу даних. Інтелектуальні системи зору та аналітика - це активна дослідницька область, яка поєднує різні комп'ютерний зір, обробку сигналів та машинне навчання для вилучення та аналізу цінної та значущої

інформації з необроблених даних датчиків зору. Наявність доступних датчиків зображення і необхідність автоматизації завдань прискорили зростання досліджень в цій області. Велика кількість візуальних даних, що надходять від цих датчиків, вимагає автоматичної системи для аналізу. Ці системи повинні мати можливість приймати рішення з мінімальною людською взаємодією або навіть без будь-яких людських взаємодій. Системи аналізу зору повинні розуміти місце події шляхом класифікації та відстеження об'єктів, а також вивчення їх поведінки. Однією з найважливіших частин візуального аналізу є виявлення аномалій [4-7].

Виявлення аномалій є частиною машинного інтелекту для виявлення будь-якої закономірності у візуальних даних, яка не відповідає нормальній поведінці системи. Методи виявлення аномалій в машинному зорі мають справу або зі статичними зображеннями або з відео. Для нерухомих зображень перспективним є пошук аномальних областей на цих зображеннях. Автоматичне виявлення аномалій має все більший попит у різних промислових застосуваннях, Через величезну кількість необроблених даних, що генеруються датчиком камери, досить великі вимоги до обробки цих даних з точки зору ресурсів і часу. Обробка великої кількості даних є діяльністю, яка вимагає витрат ресурсів, зокрема і людських. Ця теза зосереджена на системі машинного навчання, наприклад, слабокерованому навчанні, що полегшує таке навантаження. Іншим важливим аспектом є проблема дисбалансу даних, яка з'являється в налаштуваннях класифікації, що також мотивує використання виявлення аномалій там, де для навчання моделі використовуються лише нормальні зразки. Ця теза зосереджена на використанні слабокерованого навчання та машинного навчання для виявлення аномалій на зображеннях [8-14].

Багатократне навчання - це слабо контрольований підхід до навчання, коли вхідні дані мають форму *наборів* або *даних точкового шаблону*. Тоді, нагляд передбачений лише для цілих наборів, без маркування окремих екземплярів. Така установка привернула широку увагу в дослідницькому

співтоваристві. Головним чином, це пов'язано з експоненціальним збільшенням даних багатьох реальних проблем і труднощами маркування таких масивних даних. Таким чином, слабкий нагляд, спрощує в такому випадку роботу. Термін "екземпляр" у багатократному навчанні еквівалентний навчанню *точкового* шаблону [15-23]. Точковий шаблон - це множина або багато встановленість невпорядкованих точок, де кожна точка є вектором, що представляє стани або особливості об'єкта, що цікавить. За допомогою класифікатора на рівні набору здійснюють прогнозування результату. У регресійній задачі метою є присвоєння реального значення екземпляру замість прогнозованого. У завданні ранжування мета полягає в тому, щоб ранжувати екземпляри, а не присвоювати мітку або реальну цінність, і вона відрізняється від регресії тим, що мета полягає в тому, щоб встановити кількість точок для виконання сортування. Це ранжування може бути виконано на рівні екземплярів або на рівні екземпляру. Формулювання виявлення аномалій в налаштуваннях дуже обмежена в даних зображення і застосовується тільки для медичних зображень. Основна проблема полягає в тому, коли вхідні функції мають форму наборів. Тим часом спостерігається збільшення застосування багатократного навчання для виявлення аномалій у відео через слабку властивість нагляду, яка використовує потребу в анотації кадрів [24-26].

Зазвичай в алгоритмах виявлення аномалій в дискримінаційних і генеративних моделях вхідні дані представлені з фіксованою розмірністю. Таким чином, коли введені дані мають форму точкового малюнка або наборів, традиційний підхід полягає в тому, щоб зіставити дані цих точкових шаблонів у фіксовані розміри. Було запропоновано кілька методів на основі ядра, які відображають точкові шаблони у вектори, щоб дозволити методи ядра, такі як підтримка векторної машини. Більшість з цих методів на основі ядра моделюють розподіл векторних множин шляхом оцінки його розподілу імовірнісності, а потім використовується міра подібності на основі порівняння розподілу, наприклад як міра подібності, ядра Фішера і імовірнісний продукт ядра. Основні проблеми цих

методів полягають у тому, що складність комутації ядра між множинами квадратична. Іншим інваріантним метричним методом перестановки для порівняння невпорядкованих множин вектору є відстань, впроваджена в комп'ютерний зір для обробки природної мови. Останнім часом зростає інтерес до проектування нейронних мереж, які можуть мати справу з наборами вхідних даних (шаблон точки фіксованої довжини), а не фіксованими даними [27-31].

Формування даних точкового малюнка можна розглядати як набір точок, які є інваріантами перестановки. Ці набори функцій точкового шаблону з'являються в багатьох візуальних аналізах даних. У різних доменах складні дані можуть бути представлені у вигляді складу інших більш простих функцій. Наприклад, при обробці мови документи можуть бути представлені у вигляді набору слів. У комп'ютерному зорі зображення або відео можуть бути описані наборами локальних функцій, витягнутих з різних областей зображень / відео, в яких кожен встановлений вектор представляє єдиний екземпляр класу, що цікавить. Більшість алгоритмів машинного навчання (зокрема, виявлення аномалій) призначені для роботи з екземпляром даних з фіксованою розмірністю, і кардинальність цих екземплярів фіксована і не бере участі в остаточному рішенні. Нещодавно запропоновано новий алгоритм виявлення аномалій, заснований на апроксимації теорії точкових процесів під назвою фреймворк випадкової скінченної множини. В ньому запропонувано статистичну аномалію детекції моделі, в якій кардинальність витягнутих ознак змінюється на основі класу. Щоб підкреслити важливість формулювання модельного підходу до особливостей точкового шаблону, модель наївного бейєсового класифікатора розглядається як приклад, що показує обмеження цього підходу в обробці особливостей точкового шаблону для виявлення аномалій. У класичній генеративній моделі наївного бейєсового класифікатора для задачі класифікації метою є оцінка ймовірності заднього класу з урахуванням щільності попередніх ознак і попередньої щільності класу. Поки що вищезгаданий пункт зосереджений на обмеженнях застосування для виявлення аномалій з

багатократним навчанням. Тепер виділимо деякі практичні проблеми, які виникають із застосуванням виявлення аномалій:

1. Застосовуючи виявлення аномалій на зображеннях, зібраних у дуже складному середовищі, тобто на об'єктах, з метою виявлення порушення безпеки, наприклад, працівники, які дійсно носять жилет з високою видимістю. Таким чином, метод виявлення аномалій повинен вміти виявляти дуже маленький об'єкт з розмитим ефектом, за рахунок коливань вітру.

2. Анотування великої кількості нормальних і аномальних зразків для побудови класифікатора виявлення дефектів не є тривіальним рішенням. Замість цього для виявлення дефектних зразків слід використовувати алгоритм виявлення аномалій без нагляду. Загальний підхід до цього за допомогою глибоких глобальних функцій. Однак цим особливостям може перешкодити найрізноманітніші умови, такі як зміна точки зору та освітлення.

3. Виявлення незвичної поведінки з відео спостереження є дуже трудомістким і дорогим за часом через велику кількість встановлених камер. Ефективний метод - це створення програмного рішення, яке може ідентифікувати будь-яку незвичайну поведінку з відео спостереження. Один з підходів полягає в побудові класифікатора для виявлення незвичайної поведінки. Однак це породжує три проблеми: дисбаланс даних, анотація на рівні кадру та складність отримання всіх аномальних зразків. Тим часом, виявлення аномалій пропонує посильне рішення, в якому більшість цих проблем можна вирішити, але з вибором відповідного підходу [31-36].

## 1.2. Методи виявлення аномалій

Імовірнісне виявлення аномалій ґрунтується на припущенні, що з розподілу генеруються нормальні дані, а аномальні дані або нові дані є даними, які відхиляються від цього розподілу. Нормальна межа оцінюється на основі порогової щільності ймовірності нормальних даних. Передбачається, що

навчальні дані генеруються з деякого базового розподілу, такого як розподіл Гауса, коли його щільність ймовірності оцінюється з нормальних даних. Розрахунковий розподіл генерує нормальний розподіл для нормальних даних. Дані, які не входять від розрахункового розподілу, вважаються аномалією або новими. Однак в деяких випадках порогове значення імовірнісного нормального розподілувстановлюється на визначенні аномальних даних. В цілому імовірнісне виявлення аномалій ділиться на дві структури, засновані на методах, використовуваних для оцінки щільності розподілу: параметричний і непараметричний підходи [37-39].

Параметричні підходи припускають, що нормальні дані відбираються з базового параметричного розподілу. На етапі навчання параметр оцінюється із заданих нормальних тренувальних даних (відео або зображень). Розподіл Гауса є одним з найбільш поширених розподілів, що використовуються для неперервних змінних. Для оцінки параметрів розподілу використовується оцінювач максимальної правдоподібності, в якому завдяки спряженій попередній властивості він має аналітичну закриту форму рішення. Відстань Махаланобіса використовується для вимірювання відстані між тестовим набором до розподілу Гауса як порогового значення. Використовуються різні комплексні розподіли [40-43].

Непараметричні підходи припускають, що дані не підходять під фіксовану модель, а структура змінюється в розмірі, щоб відповідати даним і враховувати складність даних. Одним з непараметричних підходів є оцінювач щільності ядра. У цьому методі функція щільності ймовірності навчальних даних оцінюється за допомогою багатьох ядер, розподілених по простору даних. Розрахункова щільність ймовірності в кожному місці простору даних залежить від кількості точок даних, розташованих у межах локалізованого району ядра [44-51].

Підходи до виявлення аномалій на відстані засновані на припущенні, що нормальні екземпляри даних відбуваються в щільних районах. Однак аномалії виникають далеко не в звичайних випадках. Тому, виявлення аномалій можна

здійснити шляхом вимірювання відстані до найближчого сусіда або кластера. Виявлення аномалій дорожнього руху за допомогою знятих зображень з камери відеоспостереження використовується для виявлення незаконних розворотів запропоновано з використанням алгоритму K-найближчого сусіда в якості класифікатора потоку руху. Оптичний потік використовується для виявлення руху, а потім виявляються функції з послідовних рамок, такі як краї та кути номерних знаків, для відстеження та розмежування напрямку потоку. Наявні підходи до виявлення аномалій на відео спостереження за допомогою алгоритму K-найближчого сусіда [51-53].

Доменні методи засновані на створенні межі між новими даними і нормальними даними на етапі навчання. У більшості аномалій виявлення нових даних не визначено. Тому, межа створюється на основі тільки нормальних даних, яка близька до неї. Оцінка аномалії припиняється на основі відстані даних тесту до межі. Одним з найбільш поширених підходів є однокласна підтримка вектору машини. Загалом, всі методи витягують особливості із зображень або просторово темні функції для відео різними способами, використовуючи локальні або глобальні особливості. Ці функції потім використовуються для навчання [54-61].

Розглянемо методи, засновані на реконструкції. Методи виявлення аномалій на основі реконструкції можуть автономно моделювати дані, що не використовуються. У випадку проходження нових даних через систему виникає помилка реконструкції, яка може бути визначена як відстань між тестовим вектором і поза системою. Вона використовується як оцінка аномалії. На цій основі навчається виявлення аномалій на основі нейронних мереж. Існує кілька нейронних мереж, які були використані для загальних методів виявлення аномалій. Однак основна увага приділяється нейронним мережевим методам, які були використані в застосунках машинного зору. Детекції аномальних зображень, таких як зображення з набору даних, використовуючи ймовірність реконструкції з автоматичного варіаційного автокодера, що показує кращу

продуктивність, ніж використання помилки реконструкції як оцінки аномалії. Виявлення аномалій зображення за допомогою глибокої генеративної змагальної мережі та глибокої генеративної змагальної мережі, де метою є пошук зображення, яке не відповідає звичайному шаблону зображення, відомому як класифікація один проти всіх, за допомогою мережі. Перераховані вище методи використовують те, що відомо як глобальна аномалія, де метою є визначення всього зображення як нормального або аномального. Різні нейромережеві методи також застосовуються для виявлення аномальної поведінки у відео. Виявлення аномалій у поведінці людей за допомогою нейронної мережі використовує інформацію про оптичний потік відеокадрів для тренування нейронної мережі. Завдяки успіху нейронної мережі згортки у вирішенні проблеми класифікації зображень, ця мережа була прийнята для відео для розпізнавання дій шляхом розширення 2-D згортки до 3-D згортки. Аналогічно різні спроби запропоновано використовувати 3-D нейронні мережі згортки для детекції аномалій на основі відео. Інший тип методу на основі реконструкції, відомий як метод на основі підпростору, заснований на гіпотезі про те, що нормальні дані можуть бути спроектовані в меншовимірний підпростір. У цьому підпросторі нормальні дані можна чітко відрізнити від аномальних даних. Основний компонентний аналіз є одним з найвідоміших методів зменшення розмірності, що виконує ортогональне перетворення, де кількість ознак у підпросторі менша. Найбільша варіативність у векторах даних у просторі даних може бути представлена першими основними компонентами у новому підпросторі. На відміну від цього, останні кілька основних компонентів представляють риси, які не є очевидними по відношенню до оригінальних змінних. Більшість методів виявлення аномалій використовують PCA для зменшення розмірності та використовують інші методи для моделювання отриманих функцій підпростору. Порівняльний аналіз виявлення різних аномалій за допомогою різних методів проекції, таких як PCA, лінійний дискримінантний аналіз Фішера та перетворення поділу у

гіперспектральних зображеннях є досить ефективними. Це забезпечує лінійне і нелінійне відображення в менших розмірах, з багатьма іншими перевагами порівняно з класичним PCA [61-73].

## 1.3. Застосування випадкових скінчених множин в задачах виявлення аномалій

Статистика випадкових скінченних множин, одна з стохастичних геометричних моделей, є усталеною областю дослідження, яка виходить з відомої голчастої задачі Буффона. Теорія випадкових скінченних множин - це новий підхід, який був запропонований для багатооб'єктної фільтрації для подолання проблеми асоціацій даних, що виникає при стандартній багатооб'єктній фільтрації. Теорія випадкових скінченних множин застосовувалася в різних застосунках, починаючи від відстеження мультиоб'єктів.

Випадкова скінченна множина (ВСМ) - це задана випадкова величина з невідомою кількістю елементів, які самі по собі є випадковими. Це формує суттєву різницю між випадковою скінченою множиною і випадковим вектором. Випадковий вектор має тільки один випадковий елемент. ВСМ є потужним статистичним інструментом для аналізу спостережуваних точкових закономірностей. Ці точки можуть представляти 2-D місця розташування певного об'єкта, що цікавить. ВСМ може бути повністю змодельована дискретним розподілом, що характеризує кардинальність (кількість точок у множині), і сімейством симетричних спільних розподілів, що характеризують розподіл точок, обумовлених кардинальністю. З огляду на базовий простір X, як і в просторі ключових точок цієї тези, випадкова скінченна множина черпає миттєвість з гіперпростору всіх скінченних підмножин. Як правило, випадкова скінченна множина може містити скінченну кількість елементів. Можливі реалізації випадкової скінченної множини. Крім того, ВСМ не накладає упорядкування елементів набору. Загальна кількість елементів у множині визначається розподілом кардинальності на невід'ємне ціле число. Спільний розподіл елементів,

враховуючи, що є n точок, визначається розподілом ймовірностей на декартовий простір. Наприклад, у Пуассона ВСМ кардинальність ВСМ слідує за розподілом Пуассона із заданим середнім значенням, а елементи незалежно та ідентично розподілені відповідно до заданого розподілу на X. ВСМ X на X можна визначити як $\Omega \to F(X)$, відображення з простору вибірки на простір скінченної підмножини X. Розподіл ймовірностей або міра P регулює основну випадковість на просторі вибірки Ω, а розподіл ймовірностей ВСМ X виражається у вигляді індукованого розподілу $P = P \circ X{-}1$. Випадкова скінченна множина X на $X \in RD$ є вимірним відображенням

$$X : \Omega \to F(X), \tag{1.1}$$

де Ω — простір вибірки з мірою ймовірності P, визначеною на σ-алгебрі подій σ(Ω), а F(X) — простір скінченних підмножин X з топологією.

На фундаментальному рівні ВСМ X, як і будь-яка випадкова величина, характеризується розподілом ймовірностей. Імовірність ВСМ на X задається мірою ймовірності P на F(X) наступним чином:

$$P(\tau) = P(\{X \in \tau\}), \tag{1.2}$$

для будь-якої підмножини τ з F(X), де $\{X \in \tau\}$ позначає вимірювану підмножину $\{\omega \in \Omega: X(\omega) \in \tau\}$ Ω.

Теорія ВСМ є відгалуженням точкового процесу. Звідси наводиться контур точкового процесу формулювання ВСМ. Термін точковий візерунок відноситься до будь-якої множини або множини невпорядкованих точок. Точковий візерунок X може бути охарактеризований лічильною мірою n, є мірою, що приймає значення в $N \cup \{\infty\}$ таким чином, що n(B) є скінченною для будь-якої обмеженої підмножини B з X. n(B) = число по точках X, що падають в B, $B \subseteq X$. Лічильна міра називається простою, якщо вона не містить повторюваних точок/елементів, n({x})

$\leq 1$ для всіх $x \in X$, і скінченною, якщо вона має скінченну кількість точок $n(X) < \infty$, і просто-скінченний, якщо він простий і скінченний. ВСМ X і проста скінченна точка N ідентифікуються в наступному сенсі $N(B) = |X \cap B|$ для всіх підмножин B з X, де $|\cdot|$ позначає кардинальність = кількість точок в множині X. З цієї точки зору ВСМ і просто скінченні терміни процесу можуть використовуватися як взаємозамінні [71-73].

Щільність ймовірності точкового процесу, якщо вона існує, є дуже потужним статистичним інструментом, схожим на випадкову щільність вектору. Незважаючи на те, що F(X) і загальний евклідовий простір з RD не мають однакових характеристик, щільність ймовірності на F(X) все ще зберігає ту саму послідовну математичну нотацію ймовірності, яка доступна через ВСМ або теорію точкових процесів. Поняття міри та інтегрування є ядром. Поняття міри визначає загальне позначення довжини, маси, площі, об'єму тощо, в якому міра довільного простору Y визначає «розміри» підмножин Y. Важливою безрозмірною мірою є міра ймовірності, яка показує, що не всі застосування стосуються міри фізичних розмірів. Домінуючою мірою є загальна еталонна міра в ВСМ, яка визначається як лічильно-адитивна функція для кожного $T \subseteq F(X)$. Щоб забезпечити існування такої щільності ймовірності, обмежимося просто скінченним точковим процесом, який схожий на ВСМ.

Наївний байєсів класифікатор зазвичай використовується для вирішення завдань класифікації. Задача формулюється на основі припущення незалежності між виміряними або виявленими ознаками, використовуваними для класифікації.

Коли цей підхід використовується для виявлення аномалій, можливі лише два класи: нормальний/негативний та аномальний/позитивний. За відсутності достатніх даних до моделі для аномального класу можна лише обчислити ймовірність повторного представлення вимірювання негативного класу. У цьому випадку підхід перетворюється на ранжирування точок даних відповідно до їх значень ймовірності для негативного класу та розгляд тих, що менше визначеного користувачем порогу, як аномальних. Модель наївного байєсівського

класифікатору не може бути використана для даних ранжирування точкового шаблону через одиничне вимірювання. Модель наївного байєсівського класифікатору не використовує інформацію про кількість елементів у точкових візерунках (кардинальність).

Розглянемо випадкове виявлення аномалій на основі скінченних множин. Ефективне рішення проблеми виявлення аномалій має бути розроблено на основі характеру інформації, отриманої з джерел/датчиків та використаної для виявлення. Коли така інформація має форму точок даних, природний підхід полягає в тому, щоб розглядати їх як дані точкового шаблону.

У методах виявлення аномалій на основі ВСМ, точка даних моделюється як ВСМ. Обгрунтуванням в основному є спостереження, що в множині Z не тільки члени zi (i = 1, . . . , n) змінюються випадковим чином з часом, але і кардинальність набору |Z | = n може змінюватися випадковим чином з часом. Крім того, функція ймовірності ВСМ не забезпечує послідовного вимірювання ранжирування через неузгодженість одиниці щільності ознак. З метою виявлення аномалій потрібно лише обчислити ймовірність вимірюваного набору ознак Z враховуючи, що він представляє собою негативний випадок.

Якщо припустити, що щільність Пуассона підходить для виявлення аномалій, особливо в таких застосунках, наприклад, як виявлення жилетів безпеки на будівельних об'єктах та дефект виявлення для перевірки контролю якості, то більшість раніше згаданих густин використовувалися для багатооб'єктного відстеження.

Цей підхід полягає в тому, щоб розглядати багатооб'єктну сутність як випадкову скінченну множину і застосовувати кроки прогнозування та оновлення аналогічним чином, то можна застосовувати в традиційному алгоритмі відстеження однооб'єктних, таких як адаптивний комбінований фільтр ядра [72-79].

Таким чином, Застосування випадкових скінчених множин в задачах виявлення аномалій є перспективним.

## 1.4. Висновки

В результаті проведеного дослідження предметної області було встановлено недоліки відомих рішень і виділено їх з метою розробки рішень, які б покращили синтезу оптичних мереж центрів обробки даних.

## 1.5. Постановка задачі

Поставлена мета потребує розв’язання таких основних задач:

– проаналізувати відомі методи виявлення аномалій в рухомих зображеннях;

– розробити метод виявлення аномалій в зображеннях кіберфізичними системами комп’ютерного зору;

– удосконалити архітектуру кіберфізичних систем комп’ютерного зору;

– здійснити постановку експерименту та провести еспериментальні дослідження згідно розроблених рішень.

# 2 МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ КІБЕРФІЗИЧНИМИ СИСТЕМАМИ КОМП'ЮТЕРНОГО ЗОРУ

## 2.1. Автоматизовані системи обробки даних

Для вирішення поставлених завдань розробимо кіберфізичну систему комп'ютерного зору для моніторингу зовнішніх подій. Її основним завданням буде використання зображення в реальному часі для виявлення працівників, які порушують правила безпеки, не надягаючи жилети з високою видимістю. Запропоноване рішення сформульовано у вигляді алгоритму виявлення аномалій, розробленого в рамках RFS. Запропонована система складається з трьох кроків: застосування глибокої нейронної мережі для вилучення людей на зображенні, вилучення особливо інженерних функцій з кожної плями, повернутої глибокою нейронною мережею та застосування rfs-базованого алгоритму виявлення аномалій до кожного набору виявлених ознак. Експериментальні результати демонструють, що з точки зору F1-показника запропоноване рішення (поєднання нових інженерних ознак та алгоритму виявлення аномалій на основі RFS) означає, що воно значно перевершує різні комбінації загальних та найсучасніших ознак і алгоритми виявлення аномалій, що використовуються в застосунках машинного зору.

Однією з поширених причин небезпеки в складних середовищах, таких як місця будівництва, є низька видимість, якій піддаються працівники, які не носять спеціального одягу. Для того, щоб забезпечити безпеку працівників, вони вимагають носити захисний одяг високої життєздатності (ЗОВЖ). У літературі з комп'ютерного зору є велика кількість робіт, в яких пропонуються методи машинного зору для автоматичного виявлення та ідентифікації працівників без ЗОВЖ. З останніми досягненнями в галузі комп'ютерного зору можна виявляти та відстежувати працівників, матеріали та обладнання. Одним з найскладніших завдань є аналіз змісту виявлених об'єктів з метою відмежування небажаних від бажаних ознак.

Найбільш поширений в останніх роботах з виявлення небезпеки низької видимості заснований на класифікації спостережень на два і більше класів. Методи, засновані на класифікації, зазвичай вимагають великої кількості анотованих/мічених даних для їх навчання. Альтернативним підходом є детекція аномалії, яка не вимагає анотування позитивних (аномальних) даних. Колірний простір ЗОВЖ використовується для виявлення працівників, які носять захисні жилети, в яких вони використовували гістограму компонентів при побудові своєї функції. Для навчання різних методів використовувалися різні моделі колірного простору. Однак вони ділять дані навчання на основі кольору захисного жилету (жовтий, помаранчевий) і тренують дві різні мережі. Виявлення аномалій за своєю суттю є класифікаційним методом, проте є деякі важливі відмінності. У методах, заснованих на виявленні аномалій, метою є розрізнення нормальних / негативних та аномальних / позитивних спостережень. Аномальні спостереження не відповідають очікуваній картині інших спостережень у наборі даних. Жодне рішення на основі виявлення аномалій не було зареєстровано для моніторингу безпеки на будівельних об'єктах.

У широкому спектрі застосувань, які включають джерела інформації (дані), крім зображень та відео, численні методи виявлення аномалій були розроблені. Існують класифікаційні основи на основі кластеризації, засновані на статистичних моделях, найближчого сусіду, на спектральній основі та теоретико-інформаційні рішення.

Виявлення аномалій за допомогою зображень та відеоданих було досліджено в різних практичних застосуваннях. Відомо про запропонований метод виявлення у відеопотоках для застосунків спостереження. У ньому оцінювач щільності ядра використовується в поєднанні з підходом кластеризації, придатним для застосунків в реальному часі в повністю автономних і неконтрольованих системах. Крім того, запропоновано також аномалію в реальному часі для відеоспостереження на основі вилучення монохроматичних просторових особливостей у послідовностях зображень для представлення рухомих об'єктів.

Виявлення аномалії має також використовувався для спостереження за дикою природою. Запропоновано дослідниками вирішувати проблему виявлення аномалій у сценах дикої природи шляхом класифікації зображення з точки зору його класу сцен; якщо зображення не належить до жодного класу сцен, воно розглядається як аномалія. Запропоновано, також, рамки для виявлення аномалій з точки зору умов навколишнього середовища. У своєму рішенні вони використовували нейронні мережі як адаптивні класифікатори, що здатні до виявлення аномалій. Запропоновано виявлення аномалій для реальних відео спостереження за допомогою попередньо навченої мережі глибокого навчання для вилучення просторово-часових функцій з подальшим глибоким багаторазовим навчанням для виявлення аномалій.

Основна увага приділяється формулюванню параметричного статистичного рішення (статистична модель, розділ модельних рішень для виявлення аномалій). Таке рішення, завдяки своїй статистичній природі, включало б існуючі або засвоєні знання про невизначеності в рамках механізмів зондування, що беруть участь у застосуванні. У методі, заснованому на статистичній моделі, припущення полягає в тому, що аномалії розподіляються за межами негативного розподілу даних і мають значно нижчі ймовірності порівняно з негативними дата. У машинному навчанні багато джерел даних мають форму даних точкового шаблону. Точковий візерунок - це множина невпорядкованих точок, де кожна точка є вектором, що представляє стан або особливості об'єкта, що цікавить. Зазвичай для точки з даних для представлення позитивних даних використовуються моделі Гауса, в якій параметри моделі можна було б вивчити за допомогою максимізації очікувань. Також, є дослідження, в яких запропоновано використання точкових процесів для моделювання даних точкового шаблону для виявлення аномалій за допомогою навчання декількох екземплярів. Запропонований підхід ґрунтується на розгляді кожної точкової закономірності як RFS і виведенні функцій ймовірності на основі загальних припущень щільності RFS (наприклад, кластерів Пуассона). Використання структури RFS дозволяє сформульованій функції ймовірності

оцінити як кардинальність (кількість вилучених ознак) інформації, так і інформацію про окремі ознаки.

Згідно аналізу відомих рішень пропонується нове рішення для виявлення аномалій для моніторингу безпеки на будівельних об'єктах. Запропонований метод використовує зображення з живої камери для виявлення працівників, які порушують правила безпеки, не надягаючи жилети з високою видимістю. Все рішення реалізується в три етапи. По-перше, для виявлення людей на зображенні використовується нейронна мережа R-CNN. Потім нова функція, розроблена для цієї програми, витягується з кожної точки, повернутої Faster R-CNN. Нарешті, алгоритм виявлення аномалій на основі RFS застосовується до кожного набору витягнутих функцій.

Основними моментами роботи є: застосування вперше виявлення аномалій для виявлення захисних жилетів, які не носять робітники на будівельних об'єктах, нове рішення, яке поєднує в собі силу глибини навчання для виявлення об'єктів (R-CNN) з інженерними функціями для досягнення високої продуктивності виявлення, вперше використовуючи колірний простір для вилучення функцій при виявленні аномалій, ці особливості найкраще працюють при диференціації аномальних подій захисних жилетів, які не будуть зношені від нормальної / позитивної ситуації, та розробка рішення для виявлення аномалій на основі RFS, яке не схоже на найсучасніше, різні мережі для виявлення різних захисних жилетів різних кольорів. Експериментальні результати демонструють, що з точки зору оцінки F1 запропоноване рішення (як поєднання нових інженерних ознак та алгоритму виявлення аномалій на основі RFS) значно перевершує відомі комбінації загальних та найсучасніших ознак та виявлення аномалій алгоритми, що використовуються в застосунках машинного зору.

Основною метою даної роботи є виявлення осіб, які не носять жилетів високої видимості в цифрових зображеннях, зроблених з великих відстаней. На таких зображеннях кожна людина може охоплювати дуже невелику площу і з'являтися в низькій якості/роздільній здатності. Працівники покривають дуже

невелику площу, фото може містити пляму низької роздільної здатності на відміну від усього зображення, яке з'являється в дуже високій якості.

Цю проблему можна вирішити, застосувавши класифікаційне рішення. Однак методи класифікації зазвичай вимагають великого анотованого набору даних для всіх класів, який може бути недоступний у багатьох застосунках. Вирішення проблеми за допомогою детектування аномалії усуває необхідність у великому навчальному наборі даних з анотованим класом інтересів, оскільки для виявлення аномалій потрібні лише тренувальні дані. Розглянемо представлені результати досліджень того, як фреймворк RFS може бути застосований в машинному зорі для виявлення аномалій у візуальних даних. Сформульовано запропонований алгоритм застосування моніторингу безпеки низької видимості в структурних об'єктах, але при незначному налаштуванні параметрів запропонований алгоритм може бути широко використаний для виявлення аномалій на зображеннях в інших застосунках моніторингу безпеки та автономності.

Розглянемо будівельний майданчик, де очікується, що працівники будуть дивитися на свої жилети високої видимості. Ці сутності моделюються як негативні дані; в той час як будь-які інші працівники, які не носять жилет високої видимості, розглядаються як аномальні/позитивні дані. Запропоноване рішення складається з трьох кроків: використання глибокої нейронної мережі для виявлення людей, вилучення функцій з кожної плями, який повертається нейронною мережею, застосовує виявлення аномалій до витягнутих ознак, які утворюють набір вимірювань. Це детектор об'єктів глибокого навчання, заснований на рішенні з покращеною швидкістю навчання та тестування, одночасно знижуючи точність виявлення. Він складається з двох компонентів. Перший компонент - це повністю згорткова регіональна мережа пропозицій, за якою слідує детектор Faster R-CNN. Швидший детектор R-CNN - це суто метод на основі CNN без використання функцій ручної роботи. При виявленні об'єкта спочатку змінено розмір до 200 × 180 пікселів. Це забезпечує узгодженість виявлення ознак, а також збереження

співвідношення сторін об'єктів. Відомо, що колірний простір RGB не є стійким до змін освітленості. Спочатку трансформуємо зображення в колірний простір. Цей колірний простір вибирається завдяки спостереженням, які: у конкретному застосунку блискучі кольори захисних жилетів виділяються в компоненті, точніше негативному, для більшості колірних варіацій, і компонент міститься інформація (інтенсивність) сірого масштабу і може бути використано для виявлення інформації, пов'язаної з формою.

Використовуючи інформацію, вбудовану в зображення спочатку виявляємо блискучий колір жилетки (фокусуючись на компоненті), а потім перевіряємо інформацію про форму (фокусуючись на другій компоненті). Перевірка інформації про форму має вирішальне значення, оскільки в багатьох практичних обставинах можуть бути частини зображення блискучого кольору, але не представляють жилет. Для кожної ключової точки вектор-дескриптор називається локальним шаблоном порядку інтенсивності потім обчислюється, один раз використовуючи вміст компонента, і один раз з використанням другого компонента.

Потім два вектори об'єднуються у вектор дескриптора і зберігаються як член кінцевого набору ознак, який поступово зростає в міру виявлення та обробки більшої кількості ключових точок. Основною причиною, з якої обчислюємо дескриптори для кожної ключової точки, є його незмінність до обертання і зміни монотонної інтенсивності. Як і раніше, обчислюємо дескриптор для кожної точки, один раз для захоплення кольорової інформації (при застосуванні вмісту компонента) і один раз для захоплення форми (при застосуванні вмісту другого компонента). Захоплення як кольорової, так і афінної інформації про форму підвищує надійність методу до змін роздільної здатності, освітленості та масштабу.

Кількість ключових точок, виявлених методом, може варіюватися від плями до плями. Крім того, порядок не має значення. Отже, дескриптори, обчислені для ключових точок, накопичуються в множині (а не матриці), яка потім розглядається як RFS (головним чином через випадкові варіації її кардинальності).

Наявні особливості розсіювання в зменшеному розмірами просторі, і розподіл їх кардинальності для тренувальних плям, які містять негативні і позитивні (аномальні) події з точки зору робітника, одягненого в жилет високої видимості. З метою візуалізації кожен вектор ознак був зведений в вектор за допомогою методу t-розподіленого стохастичного сусідського вбудовування, який добре підходить для візуалізації високовимірних наборів даних. Результат демонструє, що, хоча індивідуальні щільності ознак для позитивних і негативних випадків розподілені зі значним перекриттям, ймовірна кількість цих ознак для позитивних і негативних плям розподіляється за допомогою. Подібність щільності ознак виправдовує використання моделі Пуассона для дистрибуції наборів функцій у вигляді RFS. Відмінності в розподілі кардинальності призводять до малих значень ймовірності, пов'язаних з позитивними (аномальними) наборами ознак. Використовуючи метод RFS-фреймворка, для виявлення аномальних даних буде використовуватися як інформація про кардинальність, так і ймовірність.

Запропонована підпрограма виявлення аномалій на основі RFS реалізована в рядках. По-перше, рівняння щільності Пуассона використовується для обчислення лог-подібності множини вимірювань, яка складається з усіх ознак, витягнутих із вмісту даної плями. Потім, якщо обчислена ймовірність логування менша за визначений користувачем поріг, вона визначається як аномальна. При цьому використовуються навчені параметри, припускаючи, що вони були розраховані за допомогою навчального набору даних негативних вибірок.

В альтернативному підході можна обчислити і проаналізувати функцію ранжирування. У цьому випадку єдина зміна алгоритму буде в його рядках. На навчальному етапі параметричного статистичного навчання метою є оцінка параметрів функції ймовірності, яка найкраще відповідає навчальним даним (пов'язаним з негативними випадками) за допомогою оцінювача максимальної ймовірності. У фреймворку RFS-робота, припускаючи, що розподіл кардинальності та багатофункціональна щільність з'єднання параметризовані, тоді навчальна фаза перетворюється на оцінку параметрів.

Загальний підхід до прийняття рішення про виникнення аномалії, який використовується практично всіма статистичними методами, такими як Наївний Баєсів класифікатор, полягає в обчисленні спільної функції щільності ймовірності.

Запропонований алгоритм був оцінений на основі виявлень, отриманих в результаті алгоритму Faster R-CNN у вигляді обмежувальних коробок. Оригінальні зображення були зібрані на будівельних майданчиках. Загалом було зібрано 100 ляпів працівників, одягнених у жилети високої видимості, а також ще 100, що містять аномалії (працівники, які не носять захисних жилетів). У цьому експерименті 80% з 400 негативних зразків використовуються для навчання, а комбінація решти негативних зразків і позитивних зразків використовується для валідації. Для оцінки виявлення аномалій найбільш поширеними метриками є оцінка F1 та площа під кривою (AUC). У цьому використовується бал F1 для оцінки ефективності, оскільки він найбільш широко використовується, включаючи основне посилання, де представлено виявлення аномалій RFS. Також, використовується чотириразова перехресна валідація і обчислюється бал F1, який визначається. TP представляє кількість ляпок у наборі даних перевірки, які були правильно ідентифіковані як аномальні, тоді як FP представляє кількість плям у наборі даних тесту, які були неправильно ідентифіковані як аномальні. FN представляє кількість ляпок, неправильно ідентифікованих як негативні. Досліджено деформацію p двох методів на основі SVM, як з параметром гамма, встановленим на 0,07, так і з заданим 0,01 відповідно. Поріг кардинальності є інтуїтивним альтернативним методом та основним фактором, який розрізняє позитивні та негативні набори ознак. Таким чином, перевірити цю гіпотезу і продемонструвати, що вона не є прийнятною, можна, вказавши, що запропонований метод (який використовує як інформацію про кардинальність, так і про щільність ознак) працює значно краще.

Для визначення найефективнішого порогу кардинальності були протестовані і застосовані численні кандидати в межах від 0 до максимального значення 200.  За будь-якого порогу менше 100 буде досягнуто найкращого балу

0,789. 50 зразків, випадковим чином обраних з тих, що виявлені як аномальні за запропонованим алгоритмом (щільність ймовірності RFS), що демонструє свою ефективність у виявленні відсутності захисного жилету. Всі випадково обрані зразки дійсно є репрезентативними для аномалій, і запропонований метод повернув правильне рішення.

Алгоритм складається з таких трьох кроків:

1) виявлення людей за допомогою глибокого навчання;

2) вилучення набору особливо сконструйованих функцій з областей рисунків;

3) детектування аномалій за допомогою RFS на кожному наборі витягнутих функцій.

Інженерні особливості враховують найяскравіший колір захисного жилету. Результати експриментів показують, що запропонована щільність ймовірності RFS перевершує інші методи з оцінкою F=98% F1. Запропоноване рішення залежить від точності плям, повернутих інструментом глибокого навчання, і від погодних умов, таких як туман. Дослідження впливу цих параметрів на продуктивність виявлення та надійність рішення проти них є темою для майбутніх досліджень. Далі розглянемо використання виявлення аномалій RFS для більш складного сценарію, де нормальні та аномальні приклади візуально схожі. Наприклад, при виявленні дефектів існує невелика різниця між нормальними та аномальними зображеннями на відміну від зображень жилетів безпеки та небезпеки, де є суттєва різниця в кольорі.

Таким чином, запропоноване рішення ґрунтується на припущенні, що нормальні та аномальні дані розділені визначеним користувачем пороговим значенням (p квантиль of щільності RFS). Запропонована продуктивність рішення змінюється залежно від порогового значення, і в застосунку (виявлення без жилетів) найкраща продуктивність (найвищий бал F1) досягається з квантилем p, встановленим на 0, 01 його щільності.

## 2.2. Виявлення різниці між нормальними та аномальними зображеннями при невеликих відхиленнях між ними

Виявлення аномалій RFS для безпечного моніторінгу на будівельних об'єктах з використанням високорівневої інформації та низькорівневої інформації, відображеної інженерними функціями, було розглянуто для побудови кіберфізичної системи комп'ютерного зору. Візуальна схожість між нормальними (працівник з захисним жилетом) і аномальними (працівник без захисного жилету) зразками низька. Але потрібно вирішити також проблему щодо високої візуальної схожості, наприклад, дефектне детектування як виявлення аномалій. Виявлення дефектів має першорядне значення для перевірки, наприклад, якості продукції. Останнім часом оптичне виявлення дефектів досліджується як виявлення аномалій за допомогою різних методів глибокого навчання. У більшості сучасних робіт використовуються методи вилучення функцій, які описують весь єдиний вектор ознак, який називають глобальною ознакою. Однак на використання глобальної функції впливає кілька факторів, таких як освітленість і зміна точки зору. Альтернативою є використання функцій точкового шаблону, відомих як локальні особливості або ключові точки, на які не впливають зміни умов, згаданих раніше. Використання надійних функцій точкового шаблону для виявлення дефектів за допомогою розробленого методу на основі множин ще не досліджено. Адаптуємо його для виявлення дефектів. Крім того, оцінимо різні детектори та дескриптори функцій точкових шаблонів, створені вручну функції точкового шаблону (наприклад, SIFT) та попередньо навчені глибокі функції для застосування дефектів.

Візуальний огляд є поширеною частиною процесу контролю якості в багато сучасний виробничих застосунків. Головна метою є заміна візуального огляду людини, такі як помилки ручного візуального огляду, включаючи відсутність або неправильне виявлення дефектів. Такі помилки можуть істотно вплинути на якість продукції, привести до зайвих виробничих витрат і збільшити загальні відходи. У

зв'язку з цим автоматизований візуальний огляд на основі комп'ютерного зору може значно підвищити продуктивність. Різні методи, керовані даними, засновані на глибокому навчанні, були розроблені для візуального контролю в різних областях застосування, таких як виробництво, будівництво, транспорт та обчислювальні системи.

Загальним підходом до розробки автоматизованого виявлення дефектів є використання різних алгоритмів обробки зображень. Деякі приклади включають фільтр для перевірки поверхні плитки, бінарний шаблон локального порядку для виявлення дефектів тканини, а також масштабно-інваріантні ключові характеристики для друкованих плат. Поєднання алгоритмів обробки зображень і машинного навчання показало задовільну продуктивність. Прикладом є використання гістограми особливостей орієнтованих градієнтів з класифікатором опорно-векторної машини (SVM) для залізниці. Істотним недоліком рішень, що використовують традиційні методи обробки зображень, є необхідність неявних інженерних функцій, які можуть бути складними при застосуванні до складних випадків. Спробою вирішити цю проблему було використання рішень на основі глибокого навчання для автоматизованого виявлення дефектів. Розвиток методів глибокого навчання в комп'ютерному зорі проклав шлях до розробки надійних систем візуального контролю. Ці методи використовують навчання представленню даних для виконання різних завдань, де метою є перетворення складних даних в абстрактні уявлення, відомі як функції.

Продуктивність методів глибокого навчання, таких як CNN, обмежена доступністю навчальних зразків, що породжує дві проблеми: дисбаланс класів у нормальних та дефектних вибірках та складність анотації даних. Хоча збір великої кількості немаркованих зображень (як правило, звичайних зразків без дефекцій) є простим завданням, маркування цих зразків є дорогим і вимагає навченого спеціаліста, але людські помилки можуть часто виникати. Ці дві проблеми добре відомі і підлягають подальшим дослідженням. Обмеження, введені дисбалансом класів та відсутністю величезної кількості анотованих зразків для навчання, можна

вирішити шляхом виявлення дефектів як задачі виявлення аномалій, в якій рішення про виявлення приймається на основі відхилення від статистичного розподілу «нормальних» вибірок. Крім того, немає різниці між визначенням виявлення дефектів і виявленням аномалій.

Тому, використаємо функції точкового шаблону для виявлення дефектів і змоделюємо ці функції в рамках RFS. Основна мета полягає в тому, щоб дослідити можливість використання функцій точкового шаблону в рамках виявлення аномалій на основі RFS для виявлення дефектів та вивчити ефективність цього підходу порівняно з іншими найсучаснішими глибокими виявленнями аномалій.

Термін «функція точкового шаблону» відноситься до набору ключових точок (точок інтересу або локальних ознак), а не векторної функції або глобальних ознак, що повертаються будь-яким методом конвеєра вилучення функцій. Ці ключові точки зазвичай є 2D-місцями на зображенні, яке повинно бути стабільним і повторюваним при різних умовах освітлення та точках зору. Функції точкового рисунку використовувалися в різних завданнях комп'ютерного зору, таких як калібрування камери, структура від руху та зіставлення зображень. Як правило, більшість локальних методів виявлення ознак повертають вихід у вигляді набору. На відміну від цього, глобальні методи виявлення ознак зазвичай повертають ознаки у векторному форматі, наприклад, у гістограмі орієнтованих градієнтів. У машинному навчанні традиційним підходом є перетворення ознак точкового малюнка у векторний формат за допомогою різних методів, таких як множина візуальних слів.

Одним з добре розроблених вручну методів виявлення ознак точкового малюнка, який також використовується в цій оцінці, є точковий детектор Харріса-Лапласа, який використовує кутовий детектор Харріса для виявлення масштабно-інваріантних ключових точок. Потім навколо кожної ключової точки розраховується такий дескриптор, де розмір площі залежить від максимального масштабу лапласіанів-гаусів.

Через відсутність доступу до дефектних зразків, неконтрольоване

виявлення аномалій є кращим варіантом для виявлення дефектів. При такому підході на етапі навчання використовуються тільки нормальні зразки (без дефектів). Аналогічно, виявлення дефектів на основі RFS використовує лише нормальні зразки під час навчання, щоб максимізувати щільність набору RFS, в якій параметри моделі вивчаються за допомогою або оцінювача максимальної ймовірності, або максимізації очікувань.

Розглянемо етапи досягнення результату. Першим є етап навчання. На цьому етапі мета полягає в тому, щоб вивчити параметри функції ймовірності RFS, які найкраще відповідають розподілу бездефектних зразків, максимізуючи їх ймовірність за допомогою оцінювача максимальної ймовірності. Однооб'єктна щільність може бути змодельована як суміш гауссового компоненту. При цьому параметрис компонентів Гауса можна вивчити за допомогою алгоритму такого, що ряд гауссових компонентів визначався як попередня інформація. Вибір правильної кількості компонентів для немаркованих даних є складним завданням і вимагає великої тонкої настройки з істотним впливом на продуктивність. Тому пропонується використовувати варіації умовиводу Байєса метод у оцінки параметрів. Після оцінки параметрів ранжирування RFS знову розраховується для всіх навчальних зображень, і встановлюється p−квантиль ймовірності для визначення порогового значення для використання на етапі тестування.

Етапом тестування вводиться виявлення дефектів за допомогою RFS. Це може представляти будь-яку з процедур виявлення точкових шаблонів. На виході виходить набір ключових точок і відповідних їм дескрипторів. Більшість дескрипторів, створених вручну та на основі глибокого навчання, знаходяться у високому вимірі. Таким чином, основна складова PCA проводиться для зменшення розмірності дескриптора до двох вимірів. Нарешті, RFS для дескрипторів набору зображень обчислюється за допомогою рівняння і порівнюється з пороговим значенням. Якщо результат нижче порогу, спрацьовує прапорець виявлення дефекту.

Набір даних має велику колекцію текстурних та об'єктних зображень. Він

має кольорові зображення з високою роздільною здатністю різноманітних об'єктів і текстур. У наборі наявні 15 різних категорій (10 об'єктів і п'ять текстур). Кожен об'єкт має тільки нормальні зразки для навчання і нормальні і дефектні зразки для тестування. Існує 40 різних типів дефектів, таких як подряпини, вм'ятини, забруднення тощо.

Щоб витягти розріджені локальні ознаки з бездефектних зразків, при цій оцінці були використані різні методи екстракції точкових зображень. Було використано виявлення та дескриптор функцій глибокого навчання та дескриптор. LF-Net - це мережа, що не контролюється, яка використовує стратегію виявлення, а потім опису в одній мережі точка-точка. Мережа виводить дескриптор розміром 255-D. Ця мережа забезпечує спільне навчання для виявлення та опису, навченого на наборі даних. Виявлення ключових точок D2-Net базується на локальних максимумах за всіма каналами CNN і просторових карт ознак. Під час виведення в мережі передбачений багатомасштабний варіант, яким називають цю мережу як D2-Net2. R2D2 - ця мережа забезпечує спільне вивчення виявлення та опису. Ця мережа вивчає як повторюваність ключових точок, так і повторюваність з навчального набору, щоб уникнути неоднозначних областей. Мережа R2R2 - це самокерована навчена мережа з використанням синтетичних. Запропоноване виявлення дефектів на основі RFS з використанням різних функцій детектування та опису точкового шаблону оцінюється на наборі даних. Для порівняння з глибинними моделями запропонований підхід порівнюється з різними методами детектування глибоких аномалій, який виглядає наступним чином: глибокий автокодер з використанням функції втрат; глибокий автокодер з використанням піксельної функції втрати; виявлення аномалій за допомогою генеративної мережі; словник функцій згорткової нейронної мережі; перевірка текстури: гаусова модель для текстури. Співвідношення правильно класифікованих (нормальних і дефектних) зразків по кожному об'єкту і середнє значення цих співвідношень визначаємо так: ранжуємо середнє значення кожного об'єкта (нижче - краще) цих методів, і в останньому рядку показується підсумковий ранг середнього рангу.

Виявлення дефектів на основі RFS має найкращу продуктивність, за яким слідують методи на основі автокодерів. RFS (LF-Net) і RFS (R2D2) показують кращу продуктивність. Виявлення дефектів на основі RFS показує перспективні показники порівняно з найсучаснішими методами виявлення дефектів на основі об'єктів.

Розглянемо вплив використання різних параметрів на ефективність виявлення дефектів рангу RFS. Вивчається вплив вибору різної кількості гауссових компонентів для моделювання щільності одинарного дескриптора на продуктивність за допомогою середньої продуктивності. Продуктивність змінюється в залежності від кількості гауссових компонентів. Загальний підхід до роботи з функціями точкового шаблону полягає в перетворенні цих функцій у глобальну функцію за допомогою різних методів відображення. Фреймворк RFS був використаний для оцінки кардинальності та щільності цих функцій як складний спосіб побудови статистичної моделі, яка найкраще відповідає нормальним зразкам, максимізуючи ймовірність логу. Основна гіпотеза тут полягає в тому, що при наявності дефекту змінюється кардинальність і щільність особливостей точкового малюнка, буде більше/менше ребер, і це через щільність RFS. Різні ручні та попередньо навчені функції глибокого точкового малюнка були використані як вимірювання набору функцій, щоб перевірити, яка функція точкового малюнка працює краще. Експеримент над великомасштабним набором даних виявлення дефектів був узгоджений, і порівняно запропоновані функції точкових шаблонів в рамках RFS з різними глибокими глобальними методами функцій і ранжували їх. Експериментальні результати показали, що використання вилучення функцій в рамках RFS для виявлення дефектів має найкращу продуктивність, завдяки своїй здатності фіксувати сильний відгук по краях. Результати свідчать про те, що при наявності дефекту кількість ребер істотно відрізняється. Основним обмеженням використання SIFT є необхідність ручного налаштування крайових і пікових порогів, що може сильно вплинути на продуктивність. З іншого боку, попередньо навчені методи детектування глибоких

точок не дають послідовних кращих результатів. Другим найкращим методом виявлення ознак точкового шаблону був R2D2. В основному це пов'язано з тим, що мережа генерує повторювані та надійні дескриптори функцій точкового шаблону. Крім того, LF-Net не показав себе добре порівняно з SIFT, і бо це пов'язано з тим, що мережа перетворює вхідне зображення в сірий масштаб і нехтування внеском кольорової інформації. Слід також відмітити, що ці мережі навчаються на абсолютно різних наборах даних домену, які використовуються для завдання візуального зіставлення. Хоча ці методи глибокого навчання погано працюють для виявлення, вони все ще можуть генерувати порівняльні результати для деяких об'єктів у поєднанні з виявленням дефектів на основі RFS. Нарешті, результати показують, що якщо функції підібрані правильно, методи виявлення аномалій на основі RFS перевершують глобальні моделі на основі функцій.

## 2.3. Кіберфізична система комп’ютерного зору

Ця кіберфізична система є централізованою системою, яка контролює загальний процес. Автономність агента обмежується заходами безпеки для забезпечення безпечного загального процесу. Більш гнучке рішення призведе до більшої кількості даних для обробки та збільшення обчислювальних витрат. Ці додаткові дані не будуть управлятися в режимі реального часу централізованою системою, оскільки пропускна здатність і обчислювальні витрати будуть занадто високими. В результаті контроль повинен бути розподілений, а агенти повинні отримати більше самостійності у прийнятті рішень. Однак автономні агенти не є добре прийнятими в промислових застосуваннях, і тому необхідно досягти балансу між вимогами, гнучкістю та контролем. В результаті, пропонується гібридна система, яка здатна масштабувати рівень автономності для кожного завдання на вимогу та інтегрувати експертні знання в систему. Типова система зображена на рисунку 2.1.

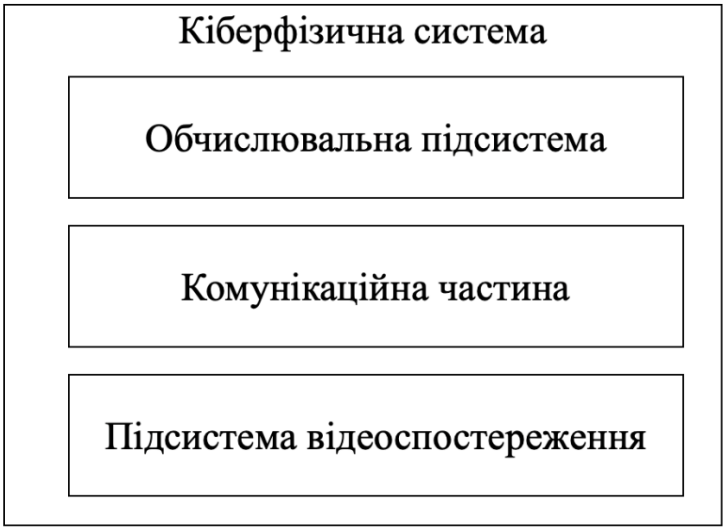



Рисунок 2.1 – Архітектура кіберфізичної системи комп’ютерного зору

Система управління управляється запитами модуля, який розбирає загальні процеси на внутрішні процеси. Загальні процеси - це зовнішні процеси, такі як запити клієнтів, на відміну від внутрішніх процесів, які описують процеси, необхідні для виконання зовнішніх процесів. Таким чином, оперативні замовлення для системи є частиною внутрішніх процесів і повинні бути узгоджені. Система призначає засобам накази на експлуатацію і контролює їх, щоб уникнути тупикових ситуацій. Індустрія автоматизації віддає перевагу простим і нескладним рішенням. Виконуючи управління стеженням з камер, система дає змгу використовувати її за різним призначенням. Перевагою такої локалізації є низькі обчислювальні витрати, необхідні для локалізації та планування траєкторії. Цього типу достатньо для багатьох промислових застосувань. Дорогі сертифіковані за безпекою датчики та контролери потрібні, якщо в одному робочому просторі є люди. У цьому випадку контролери безпеки повинні використовуватися для заміни команд контролера з метою запобігання непередбачуваним випадкам. Використовуємо сертифіковані лазерні сканери, які здатні динамічно адаптувати зони безпеки до швидкості. Перешкоди, виявлені в зоні безпеки, призводять до зупинки. Зупинка означає, що агент повинен перевести себе в безпечний стан і не може просто зупинити рух, наприклад, система повинна запобігти зупинці агентів

перед аварійним виходом. Таким чином, лазерні датчики дальності встановлюються для виявлення перешкод. Однак лазери не обов'язково використовуються для навігації через додаткову складність. Це змушує кожного залишатися на заздалегідь визначених позиціях, тому залишити позицію в разі перешкоди неможливо. Перешкода на позиції - планування та контроль виробництва, маршрутизація треків, маршрути, внутрішні процеси, робота, трекінг, управління. Модулі системи в поєднаній взаємодії зображено на рис. 2.2.

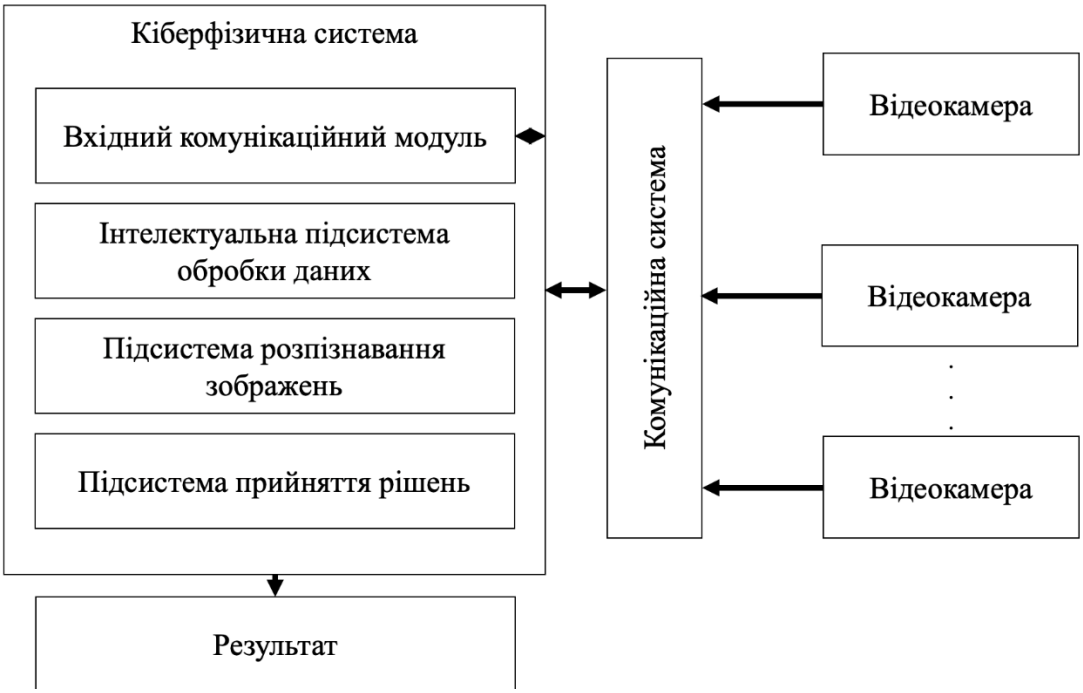



Рисунок 2.2 – Деталізована схема кіберфізичної системи

Єдиний сервер маршрутизує всі агенти вздовж автономних заданих треків. Не задіяння планування шляху призведе до того, що агенти сповільняться і в кінцевому підсумку зупиняться. Навіть, якщо методи локалізації здатні впоратися з відхиленнями від заздалегідь визначених треків, їх зазвичай уникають, щоб зробити системи простими. Система управління розподіляє кожному роботу на наступні сегменти. Це дозволяє запобігати проблемам, призначаючи виключно один сегмент одночасно на одного агента. У зв'язку зі складністю цього завдання тимчасові рамки обмежені і евристику необхідно використовувати для того, щоб

зменшити обчислювальну складність. Метою запропонованого тут підходу є роз'єднання і локальне планування. Система повинна вміти розпізнавати конкретні сценарії і повинна мати справу з ними на місцевому рівні, відповідним чином адаптуючи свою стратегію планування траєкторії. Агенти контролюються централізованим сервером, а всі об'єкти відстежуються стандартизованою системою зору. Можна виявляти конкретні сценарії і швидко реагувати шляхом адаптації. Також, вони можуть передбачати заздалегідь визначені плани з ролями для декількох агентів, які можуть бути адаптовані до сценаріїв, щоб запобігти тупикам, наприклад, у наступному сценарії: проходження двох агентів: вибрати ведучого; лідер вибирає сторону для проходження; послідовник визнає сторону; проходження. Подібні методи, також, використовуються в системі, яка не має централізованої системи команд. У запропонованому підході представляємо ідею того, як інтегрувати експертні знання в систему для підтримки відбору. Це робиться шляхом розширення сегментів доріжки, а також областей навколо сегментів, щоб спростити розпізнавання сценаріїв і забезпечити відтворювану поведінку. Системи, які в даний час використовуються в промислових застосунках, використовують ручні автономні маршрути для планування. Ці маршрути визначаються списком сегментів і розподіляються системою, як показано на рис. 2.2. Завдання системи полягає в тому, щоб слідувати цим сегментам. Дана система має всього два рівні планування: загальна маршрутизація на централізованому сервері і управління на рівні агента. Перешкоди завжди провокують аварійну зупинку. Це може бути реалізовано тільки в тому випадку, якщо агенти здатні локалізувати себе (навіть при виході із заздалегідь визначеного маршруту), спілкуватися один з одним, а також виконувати і адаптувати свою поведінку, вирішувати локальні проблеми без централізованого втручання. Задамо так, щоб система розподіляла сегменти на агентів, подібні до попередніх, але інкапсульовані додатковими атрибутами. Для демонстраційних цілей згрупуємо області у вільні або критичні. Вільна ділянка сигналізує про те, що агентам дозволено для сегментів критичних сегментів і статичних. Пропонований підхід полягає в тому,

що запланована траєкторія колізії безпечного уникнення траєкторії проходження оптимізована. Така система отримує переваги. Критична область вказує на особливу обережність. Додаткові атрибути сегмента використовуються, щоб вказати системі, чого очікувати або яку поведінку слід вибрати для управління сегментом треку. Типовим атрибутом може бути те, що зупинки не допускаються. Це важливо при проходженні: агент повинен перевірити, чи достатньо вільного місця після критичної секції, перш ніж увійти в цю секцію, і вибрати відповідний алгоритм управління. У підході агенти можуть вибрати один з двох алгоритмів управління. Модель прогнозного управління, реалізована, але більш просунутим способом, щоб слідувати за маршрутами, що дозволяє системі відхилятися від маршруту. Контролер стеження на основі плоского виходу системи, який намагається точно слідувати за маршрутами. При наявності перешкоди управління уповільнює проходження потоків даних, в кінцевому підсумку зупиняючи їх. Система, яка використовується в даний час, має централізоване планування шляхів на основі заздалегідь визначених відрізків ліній та дуг. Агент повинен слідувати статичним маршрутам, прокладеним системою управління. На відміну від системи, що використовується в даний час, запропонована тут система використовує заздалегідь визначені зони. Траєкторії локально сплановані і можуть бути оптимізовані за часом, ресурсами або енергією. Перша ітерація – контролер поведінки, рольова гра. Вищезгадані поняття грають рольові ігри описують стратегії для вирішення конкретних сценаріїв. Рольова гра агентів описує вибір параметра і процедуру взаємодії для одного або декількох агентів протягом певного періоду часу. Реалізований контролер поведінки відповідає за розпізнавання сценаріїв і вибір відповідних маршрутів. На першій ітерації реалізуються прості рольові ігри з метою запуску системи. Агенти використовують попередньо визначені маршрути як основу для планування локального шляху, але вони можуть змінювати свій локальний шлях, коли перешкода блокує його або коли вказується заздалегідь визначеними сегментами. Агенти можуть вибирати між двома типами контролю відстеження для різної поведінки руху. Параметри

контролера вибираються на вимогу залежно від виконуваної рольової гри. Це дозволяє системі поводитися по-різному в різних областях, а також дає оператору можливість обмежувати систему, коли це необхідно. Друга ітерація – взаємодія агентів. Другий етап дозволить агентам планувати власні шляхи, якщо це дозволено в межах поточної області. Використання вищезгаданих завдань з рольовими іграми для конкретних сценаріїв дозволяє системі управління виявляти такі сценарії та ініціювати рольові ігри з одним або декількома залученими агентами, наприклад, проходження двох з них. Якщо такий сценарій визнається, залученим агентом дозволяється спілкуватися один з одним, щоб адаптувати відому рольову гру. Це розподіляє компетенції управління між агентами, тим самим роблячи систему більш гнучкою. Загальна архітектура запропонованої системи показана на рис. 2.1 і більш детально на рис. 2.2. Модуль координує загальний процес та взаємодію з системою планування ресурсів. Планування маршруту має справлятися з відхиленнями в часі виконання, оскільки час виконання рольової гри може змінюватися через місцеву навігацію. Агент повинен вивчати та адаптувати такі параметри, як час виконання та успішність рольових ігор, щоб створити таблиці оптимальної маршрутизації. Планування шляху агентом здійснює систма, яка отримує маршрути, які слід слідувати від агентам, і доставляє сегменти для слідування до управління. Планувальник шляху повинен обчислити відповідний шлях, використовуючи відомі карти мережі. Завданням цього планувальника, також, є пошук шляхів. Практично точне управління відстеженням може бути досягнуто за допомогою моделі плоскої вихідної системи і відстеження сегментів як сплайнів для вхідних даних, але запропонована система повинна мати можливість розходитися від треку при необхідності. Вона спочатку генерує можливу траєкторію на основі поточного стану системи і зважує кожну з них на основі функції витрат, яка може включати виявлені перешкоди. Цей елемент управління виконує першу послідовність виграшної траєкторії тільки до наступної ітерації управління. Постійні оновлення необхідні для безпечного і плавного управління. Загальновідомо, що найбільш обчислювально інтенсивними

процедурами в цій витратній функції є виявлення і оцінка витрат на рух, але останні дослідження показали, що впровадження ефектів проевристики призводить до великого підвищення продуктивності. У підході дозволено системі перемикатися між точним контролем відстеження. Поведінковий контролер повинен бути розроблений для спрощення планів, особливо коли задіяно кілька агентів. Однак більш важливими для прийняття системи є інтеграція експертних знань і відтворюваної поведінки. Самолокалізація є ще однією проблемою, яка виникає через неточність самолокалізації при використанні різних методів локалізації. Системі доводиться мати справу з неточностями і врешті-решт доводиться адаптувати свою поведінку, щоб отримати кращу впевненість у локалізації, коли це необхідно. Наприклад, процедура, коли один агент розміщує корисне навантаження, а інший агент забирає його, не вдається при неточній локалізації. Щоб бути економічно ефективними, системи з індивідуальними агентами зазвичай розгортаються протягом тривалого періоду часу. Протягом цього тривалого періоду використання зміни можна очікувати і з ними потрібно боротися. Загальний шар, який представляє зміни, може бути оновлений і поширений серед агентів. Створення карти з декількох вимірювань є складним завданням, і ще не зрозуміло, чи слід виконувати це завдання кожному агенту окремо або централізованим підрозділом, особливо якщо замикання циклу необхідно. Цим всім можна керувати лише за допомогою розподіленої системи, але це за своєю суттю збільшує складність системи. Буде складним завданням знайти правильний баланс, і в цьому дослідженні відповідні рольові ігри з експертними знаннями для того, щоб створити прийнятну систему. Система має безліч функцій безпеки для забезпечення безпечного процесу. Наприклад, всі агенти контролюються, щоб переконатися, що транспортні засоби знаходяться на маршруті, слідуючи призначеному маршруту. Модельоване середовище було створено за допомогою вільно доступного пакету 3D-моделювання, що включає фізичний движок. Змоделювали систему за допомогою кількох агентів. Вони використовують елементи спільної пам'яті для міжпроцесної комунікації.

Бібліотеки використовуються тільки для взаємодії з симулятором, використовуючи налаштовані вузли для обміну даними між повідомленнями і змінними. Рішення уникати затримок у функціональному коді обумовлено поточною системою, яку використовує партнер проекту, який використовує власне проміжне програмне забезпечення. Ще однією причиною виключити затримки була знижена і висхідна сумісність. У порівнянні з циклами функціонування агентів, цикли випуску дуже короткі, і зазвичай системі доводиться підтримувати стабільність визначених маршрутів. Система використовує локальний планувальник маршрутів для пошуку шляху до наступного відомого підмаршруту для отримання можливості виконання завдання. Вищезазначена складна процедура ініціалізації все ще необхідна з міркувань безпеки. Всі сегменти, що включені в агенти, доповнені додатковими параметрами для запуску різних моделей поведінки, наприклад, перемикання між декількома реалізованими методами управління рухом з різними налаштуваннями. Тепер оператор може заздалегідь визначати зони для контролю поведінки агента. Наприклад, це дозволяє агенту вибирати траєкторії в кіберфізичній системі, щоб уникнути проблем із шляхом, але перешкода на шляху призведе до зупинки процесу. Така поведінка була розроблена для підвищення сприйняття системи.

Таким чином, удосконалено архітектуру кіберфізичних систем комп’ютерного зору.

## 2.4. Висновки до другого розділу

В результаті здійснено аналіз та розробку методу виявлення аномалій в статичних зображеннях чіткої видимості, а також удосконалено архітектуру кіберфізичних систем комп’ютерного зору.

# 3 ВИЯВЛЕННЯ ДЕФЕКТІВ АНОМАЛІЙ ЗА ДОПОМОГОЮ ДАНИХ ЗОБРАЖЕННЯ

## 3.1. Виявлення дефектів об’єктів як аномалій

Розглянемо виявлення промислових дефектів за допомогою даних зображення. Виявлення дефектів будемо розглядати як виявлення аномалій. Останні рішення для виявлення аномалій в першу чергу розроблені на основі витягнутих із зображення, і з використанням різних характеристик цих ознак, щоб зробити судження про нормальність вмісту зображення. Однак глобальні зображення не стійкі проти освітлення та зміни точки зору і не містять всієї геометричної інформації, тому виявити аномалію може експерт-людина. Використаємо трансферне навчання локальним/точковим характеристикам шаблону для подолання цих обмежень та всебічного захоплення геометричної інформації та моделювання цих локальних/точкових ознак шаблону як RFS. Розподіл точкового малюнка особливості нормальної вибірки моделюються як багатофакторні гаусові моделі. Це спрощене припущення призводить до вивчення запропонованої енергії RFS, яка є обчислювальною. Запропонований підхід оцінюється на двох наборах даних. Набір даних зазвичай використовується для порівняльного аналізу багатооб'єктних рішень для виявлення дефектів. Експериментальні результати показують, що запропонований підхід, виміряний з точки зору площі за метрикою характеристики оператора приймача (AUC). Запропонований підхід перевершує найсучасніші, особливо в умовах малозйомного навчання. Для набору даних виявлення дефектів голки результати показують покращення на 11,4% в AUC, тоді як його використання пам'яті в 27,5 разів менше.

Метою виявлення дефектів є виявлення різних нерівностей на зображенні. Це означає, що використання локальних функцій для захоплення цих варіацій є більш зрозумілим і практичним, оскільки вони більш стійкі проти освітленості та зміни точки зору. Для виявлення дефектів використовуємо трансферне навчання

локальних ознак або ознак точкового шаблону. Розроблений підхід пропонує вивчити параметри енергії RFS на високій розмірності, щоб уникнути проблеми розв'язки за рахунок зменшення розмірності. Запропонований підхід є обчислювально легким і вимагає декількох зразків для навчання, що було продемонстровано малозйомними експериментами.

Останні методи, які розглядають виявлення дефектів як виявлення аномалій, зазвичай можна розділити на два підходи: генеративні моделі та моделі на основі трансферного навчання (попередньо навчені мережі). Основна увага приділена виявленню аномалій, а не локалізації аномалії на зображенні. Крім того, розглядаємо методи вилучення функцій на основі точкових шаблонів.

Виявлення дефектів за допомогою генеративних моделей. Генеративні моделі є статистичними інструментами для вивчення розподілу даних без нагляду. Ці моделі можуть генерувати зразки з навчального багато виду даних. У цьому контексті виявлення аномалій виконується на основі принципу, що аномалії не можуть бути сформовані, оскільки вони не належать до навчальної множини. Прикладами цих генеративних моделей є автокодер. Підходи, засновані на автокодерах, кодують високовимірні ознаки до їх прихованої змінної форми і реконструюють їх на кінці декодера. Потім розраховується похибка реконструкції між входом і виходом автокодера. Таким чином, висока похибка реконструкції повинна відображати наявність аномалії. Можна, також, використовувати індекс подібності структури як функцію втрат для тренування автокодера. Індекс використовується як реконструкція помилки для фіксації візуальної подібності серед навчальних даних. Основна проблема підходу, заснованого на автокодерах, полягає в тому, що вони можуть занадто сильно узагальнюватися. В результаті вони можуть реконструювати аномалії з подібною якістю до реконструкції нормальних зразків. Щоб пом'якшити цю проблему можна використовувати модуль пам'яті, який дискретизує латентний простір. Є варіанти використання регуляризованого аутоенкодеру з енергетичною моделлю для моделювання розподілу даних нормальних вибірок. Зразки з високою енергією вважаються

аномалією. Методи виявлення аномалій розроблені на основі припущення, що модель може генерувати лише нормальні зразки. Зазвичай моделі складаються з двох ступенів, а саме генератора і дискримінатора. Є, також, двоступеневий підхід до навчання для виявлення аномалій. Вона навчається, потім оптимізується як обернений генератор або використання генератора в якості декодера дає можливість розрахунку похибки реконструкції. Помилка реконструкції моделюється різницею між дискримінаторними ознаками вхідного та реконструйованого виводу зображення і використовується як оцінка аномалії.

Виявлення дефектів за допомогою заздалегідь навчених мереж. Ці методи використовують простір функцій попередньо навченої мережі для виявлення аномалії. Попередньо навчені мережі використовують глибоке навчання репрезентації навчені виявляти кілька шарів представлення в контрольованому підході, для виконання різних завдань, таких як класифікація. Функціональний простір цих мереж часто є досить загальним, щоб бути перенесеним на несхожі завдання і все-таки досягти результатів. Виявлення аномалій попередньо навченою мережею зазвичай виконується за допомогою простого підходу машинного навчання.

Вилучення функцій на основі точкового шаблону. Локальні методи вилучення функцій мають багато застосувань, включаючи отримання зображень, 3D-реконструкція, поза камери та медичне зображення. Ці програми показують перевагу використання розріджених функцій перед прямою мережею (тензорні методи). Вилучення локальних ознак можна класифікувати на методи ручної роботи та методи, засновані на засвоєнні. Класичні методи виявлення локальних ознак (або виявлення ключових точок) виконують два завдання виявлення ключових точок і обчислень дескрипторів, незалежно. Потім розроблений вручну алгоритм локалізує ці ключові моменти, дивлячись на геометричну структуру на зображеннях. Метод видобуває ключові точки, знаходячи плями над багатомасштабними рівнями на зображеннях, і використовує градієнт гістограми як дескриптор. Детектори використовують похідні першого і другого порядку для

знаходження кутів або плям на зображеннях. Пізніше була запропонована варіація багатомасштабних та афінних перетворень цих детекторів. Процес виявлення, також, був прискорений за рахунок використання інтегральних зображень в якості наближення гессіанської матриці. Виявлення ключових точок використовує гессіанський детектор, застосований до нелінійної дифузії на масштабному просторі, на відміну від часто використовуваної піраміди Гауса. Нарешті, метод виявив ключові точки, сегментуючи зображення та шукаючи стабільні регіони.

Детектори репрезентативного навчання ефективні за результатами навчання репрезентації в загальних методах виявлення об'єктів та дескрипторів. Найперша спроба використовувати машинне навчання для виявлення кутових ключових точок була зроблена шляхом впровадження функцій методу прискореного сегментного тесту.

Згодом були запропоновані різні роботи для розширення методу шляхом його оптимізації або додавання дескриптора і додавання оцінки. Останні досягнення для навчання репрезентації, також, вплинули на виявлення ключових точок.

Тимчасовий інваріантний детектор навчання використовується для виявлення ключових точок, які є надійними при суворих погодних умовах та змінах освітленості, а також навчений на декількох штучних моделях лінійної регресії.

Вищезазначені підходи в основному зосереджені лише на виявленні ключових точок. Самоконтрольований глибокий спільний точковий детектор і дескриптор навчається на синтетичних фігурах. Його можна використовувати для виявлення кутів на зображеннях.

Недоліком цього методу є те, що його можна використовувати лише на зображеннях у сірому масштабі, таким чином, дефект на основі кольору неможливо виявити. Наскрізне вивчення виявлення ключових точок, включаючи оцінку орієнтації кожного. Він оцінює масштаб, орієнтацію та положення ознак шляхом спільного вивчення виявлення та опису.

## 3.2. Навчання згідно моделі

Моделі - це сімейство статистичних моделей, які використовують функцію для представлення розподілу ймовірностей через ненормалізовану негативну ймовірність журналу. Функцію щільності вибирають для входу до одиниці. Вивчення параметрів моделей може здійснюватися шляхом підписання меншої енергії (звідси висока ймовірність) до спостережуваних зразків. Навчання за допомогою оцінювача максимальної ймовірності часто не є практичним через нерозв'язність інтеграла в знаменнику. Поширеним способом обчислення функції ймовірності є використання ланцюга Маркова-Монте-Карло і апроксимацію інтеграла. Подібно до імовірнісних генеративних моделей параметри щільності кластера можна вивчити, максимізуючи ймовірність лог-подібності навчальних зразків. З припущенням, що ознаки точки розподілені за багатофакторним гаусовим розподілом з його середнім. Розрахунок має закриту форму. Оціночне середнє значення для одиничних ознак щільності є просто зразок середній і коваріаційний відповідно. Уникнути проблеми сингулярності, пов'язаної з оцінкою коваріаційної матриці у високовимірному просторі розмірності функцій як кроку попередньої обробки, можна використовуючи алгоритм зниження розмірності. Цей підхід може вплинути на відокремлену модель навчання та податливість збереження необхідної інформації завдяки двоступеневому підходу – зменшенню розмірності та вивченню параметрів. Пропонується рішення, де параметри вивчаються у просторі високих вимірів без необхідності тренувальної фази через використання декількох методів навчання і, як наслідок, здатність до навчання з урахуванням декількох навчальних зразків. Пропонується використовувати функцію RFS на основі енергії як оцінку аномалій для виявлення. Запропонований підхід складається з двох частин: локальних особливостей вилучення і розрахунків енергії RFS. Запропонований підхід є обчислювально ефективним і не вимагає важких навчальних обчислень. Для вилучення функцій використовується попередньо навчений класифікатор для захоплення інформації, пов'язаної з

об'єктом, вбудовану в зображення. Вилучені функції моделюються як RFS, а його енергія обчислюється та використовується для прийняття рішень про те, чи існує аномалія (дефект) чи ні. При виявленні аномалій зацікавленість є у виявленні нерівностей на зображенні. Одним із підходів до фіксації нерівностей є вилучення глобальних ознак та виявлення неправильних закономірностей у цих функціях. На глобальні можливості може вплинути широкий спектр умов, таких як освітлення та оглядовий майданчик. Пропонується використовувати локальну методику вилучення ознак, що використовує підхід «опис для виявлення». З огляду на вхідне зображення, мережа екстракторів функцій виробляє тензор. Тензор можна розглядати як набір відповідей ознак карт. Карти особливостей схожі на різницю карт відповіді. Функція повертає набір ключових точок та їх дескрипторів на основі наступного визначення. Ключова точка знаходиться в точці, якщо ця точка є локальним максимумом у певній ознаці карти і що є ознака карти. Попередньо навчена мережа вилучення функцій повертає набір локальних точкових візерунків, які можуть бути взагалі змодельовані у вигляді RFS. Для виявлення аномалій RFS загальний підхід полягає в тому, щоб подивитися на лог-ймовірність RFS кожної нової міри. Підхід за замовчуванням полягає в першій оцінці параметра з ряду раніше придбаних вимірювань із зображень нормальних зразків, потім обчислити подібність будь-якого нового набору вимірювань, і розглянути її, представляючи аномалію, коли обчислена подібність невелика (нижче порогового значення). Однак через неузгодженість одиниць цей підхід працює лише тоді, коли кількість ознак у вимірюваному точковому малюнку змінюється в межах діапазону. Щоб подолати це обмеження запропоновано визначити показник ранжування і використовувати його замість лог-ймовірності. Наведена функція ранжирування пропорційна нормалізації ранжирування та подолання ефекту неузгодженості одиниць.

Обчислення нормованого терма у високій розмірності неможливо через проблему сингулярності. Крім того, все ще функція ранжування RFS не може фіксувати невеликі варіації, викликані дефектами, оскільки їх вплив на значення

функції ранжирування здійснюється нормалізацією.

Тому, пропонується нова енергетичну функція RFS для використання для виявлення дефектів. Вихідне визначення енергії для будь-якої випадкової величини, включаючи RFS, представлено негативним логарифмом її щільності, тобто для вимірюваної як вибірки нормальної сукупності і з кластеру припущення. З розподілом Пуассона і багатофакторними гаусівськими припущеннями про кардинальність і одиничну щільність ознак, вже розраховано лог-ймовірність і енергетичну функцію. Здійснимо видалення терміну, оскільки він не впливає на прийняття рішення про те, чи є нова множина вимірювань нормальним випадком або аномалією (дефектом). Логарифм багатофакторної нормальної щільності включає в себе терми, які є тільки параметрами і можуть бути видалені аналогічно терміну. Таким чином, запропонована нами енергетична функція зводиться до квадратичної відстані Махаланобіса.

Відстань Махаланобіса - це точка до відстані розподілу, яка добре відома моделюванням невизначеності зразка. Крім того, останні роботи показують ефективність використання відстані Махаланобіса для моделювання попередньо навчених особливостей нормальних зразків. Однак, наскільки відомо, жодна робота не використовувала суму в квадраті відстані Махаланобіса для моделювання особливості шаблону точки нормальних зразків у рамках RFS. Визначимо параметри енергетичної функції RFS. Розглянемо вивчення параметрів енергії RFS без протидії проблемі роздільного навчання. Таке вивчення параметрів виконується на високовимірному просторі без подальшого процесингу, наприклад, зменшення ознак PCA. Крім того, під впливом нинішнього успіху використання заздалегідь навченої моделі для виявлення аномалій використовується попередньо навчена мережа для вилучення локальних функцій.

Енергія RFS кластера Пуассона має три параметри для вивчення: інтенсивність Пуассона, середнє і коваріацію багатофакторної щільності Гауса. Дотримуючись підходу, параметри навчання виконуються шляхом розгляду параметрів навчання кардинальності і щільності ознак як двох окремих задач

оптимізації.

Основна істотна відмінність полягає в тому, що вивчення параметрів щільності ознаки здійснюється на просторі високих розмірів. Оскільки справжній розподіл ознак невідомо, потрібно отримати середнє і коваріаційне значення. Однак коваріаційне оцінювання за допомогою рівняння вимагає кількості навчальних ознак вибірки, не може бути більшим за розмірність ознаки. Відповідно, коли існує мало нормальних зразків, як у наборі даних, а також у випадку з медичними додатками, коли отримати велику кількість нормальних зразків дорого, цей відомий як малозахищене навчання, оцінка стає нестабільною і призводить до проблеми сингулярності. Щоб подолати цю проблему, використаємо усадочну коваріаційну оцінку. У багатьох сферах застосування шукаємо дефекти невеликої області на зображенні, які відповідають малим ІК-закономірностям в енергії RFS. Через суми в рівнянні RFS невелика варіація зображення може призвести до незначної зміни енергії. Невелика варіація відбивається через відстань Махаланобіса від нормального розподілу ознак. Очікується, що дескриптор точкового шаблону області дефекту поверне більші відстані Махаланобіса порівняно з бездефектними (нормальними) областями зображення. Тому, для підвищення чутливості енергетичної функції до малих дефектів пропонуємо в розрахунку використовувати особливості, які мають більшу віддаленість від нормального розподілу. Таким чином, це реалізовано через оцінювання відстані Махаланобіса в квадраті і включення лише найбільшого відсотку у розрахунку енергії.

## 3.3. Висновки

Розроблено метод виявлення аномалій в зображеннях в частині виявлення в зображеннях дефектів. Проведено оцінювання якості виявлення з використанням відстані Махалонобіса.

# 4 ПІДХІД ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У РЕАЛЬНИХ ВІДЕО СПОСТЕРЕЖЕННЯ

## 4.1. Виявлення динамічних об’єктів як аномалій

Попередні дослідження виявлення візуальних аномалій здійснювались за допомогою даних зображення. Для цього були представлені модельні рішення, де дані знаходяться у вигляді випадкових множин. В подальшому потрібно розглядати ще одну важливу проблему візуальних даних, яка полягає у виявленні аномальної поведінки у відео. Виявлення аномалій у відеозв'язних даних є складним завданням через динамічне середовище зони спостереження. Для вирішення цієї проблеми було запропоновано кілька рішень, починаючи від використання функцій ручної роботи до наскрізних методів глибокого навчання. Розглянемо модельний підхід до виявлення аномалій для відеоданих спостереження. Це рішення засноване на оцінці розрідженості заздалегідь навчених глибинних особливостей. Мета полягає в тому, щоб зібрати інформацію про розрідженість глибоких рисунків, навчених глибокими функціями, і використовувати її як додаткову інформацію для диференціації нормальних та аномальних подій у відео. Запропонований підхід використовує модель наївного баєсового класифікатору в рамках навчання з декількома екземплярами. Експериментальні результати показують, що розрідженість інформації про глибинні функції може покращити підхід Наївний баєсів класифікатор та підвищити точність межі рішення. Автоматичне розпізнавання дій людини можна визначити як завдання. Виявлення ненормальні події у відео є однією з основних проблем через величезну кількість даних, поданих камерами спостереження. Ручний аналіз даних вимагає великих людських зусиль. Виявлення аномальних подій у відео розглядалося як проблема детекції аномалії, в якій метою є виявлення або виявлення аномальних закономірностей у відеоданих. Зазвичай не вистачає позитивних зразків (аномальних даних) для навчання класифікатора. Тому, для навчання моделі використовуються лише негативні/нормальні вибірки даних.

Отже, будь-які отримані нові дані будуть вважатися ненормальними.

Як правило, виявлення аномалій для поведінки людини у відео спостереження складається з двох кроків: кроку репрезентації поведінки та аналізу поведінки. На етапі представлення поведінки були запропоновані різні методи вилучення просторово-часових особливостей, які фіксують особливості руху, текстури та форми. Ранні методи представлення поведінки передбачали детекцію об'єктів і відстеження для вилучення траєкторних ознак або зробити семантичний аналіз для розрізнення нормальних або анормальних подій. Запропонувано використовувати метод виявлення аномалій, витягнувши функцію піксельної події, а потім змоделювавши імовірнісну копію вилучених ознак. Послідовний метод Монте-Карло, також, використовувався для оцінки попереднього та останнього розподілу станів об'єкта для кожного класу подій ознак. Рішення на основі відстеження не є точними через неточність у передбачуваних треків.

Щоб уникнути недоліків методів, заснованих на відстеженні, були запропоновані різні підходи. Спільною метою цих підходів є вивчення глобальних моделей руху, таких як методи на основі гістограм, тематичне моделювання методів та моделювання моделей руху. Ці методи засновані на вивченні нормального руху патерна у відеоданих і поданні його у вигляді розподілу. Схема руху з малою ймовірністю розглядається як аномалія. У цих рамках було запропоновано кілька функцій ручної роботи. Методи глибокого навчання були використані для вилучення просторово-часових особливостей у відеоданих, таких як функції і виявлення аномалій здійснюється за допомогою SVM або наскрізних мереж. Другий крок – моделювання поведінки. На цьому кроці навчання нормальній поведінці здійснюється за допомогою різних методів навчання. Процес навчання може включати збір зразків нормальних, а іноді ненормальних відео. Ці методи можна класифікувати на три категорії: контрольовані, неконтрольовані і напівкеровані методи. Розглянемо метод напівкерованого. Метод під наглядом заснований на навчанні моделі з використанням даних. Можливий підхід в контрольованому методі заснований на використанні множини візуальних слів для

навчання опорно-векторної машини.

У методі напівкерованого маркування та використання лише звичайних даних для кроку. Напівкерований метод включає в себе засновані на правилах і модельних підходах. Підхід, заснований на правилах, базується на побудові правила, в якому будь-які дані, які не відповідають правилу, вважаються аномалією. Метою модельного методу є побудова моделі нормальних закономірностей. Будь-який екземпляр даних, що відхиляється від нормальної моделі, розглядається як аномалія. Для методу, заснованого на моделі, було запропоновано кілька моделей, таких як випадкове поле Маркова, де прихована марківська модель (HMM) і модель суміші Гауса (GMM). Запропонувано метод детекції аномалії на основі моделі гауссового процесу. У цьому підході для вивчення нормальних закономірностей руху використовуються вироби ручної роботи з використанням гістограми оптичного потоку. Крім того, запропонувано глибоку гаусівську модель процесу для вивчення нормального малюнка в переповнених сценах, в якій 3D-градієнт в поєднанні з глибокою мережею використовується для вивчення нормального шаблону. Ієрархічну структуру виявлення та локалізації аномалій з використанням регресії процесів Гауса використовує створені вручну функції, відомі як точки інтересу в просторі-часі.

Жоден з існуючих методів не досліджував використання розрідженої інформації в глибокій особливості. Натхненна прикладним виявленням аномалій на основі RFS є демонстрація переваги використання інформації про розрідженість порівняно з існуючими так званими еволюціями. Інформація про розрідженість, витягнута з глибоких функцій, може бути використана як додаткова функція в рамках багатократного навчання. Виходячи зі спостережень, що використання додаткової інформації, представленої кардинальністю інстанцій, сприяє виявленню аномалії при побудові межі рішення. Новий метод, заснований на структурі RFS для багатократного навчання має у формулюванні щільності RFS одну важливу властивістю, яка повинна бути задоволена, і є інваріантом перестановки декількох екземплярів або об'єктів. Таким чином, підхід, заснований

на RFS, не може бути застосований до глибоких особливостей, оскільки ці функції не є інваріантними перестановками (часове впорядкування є важливим). Щоб повною мірою скористатися перевагами виявлення аномалій на основі RFS, кардинальність цих функцій також повинна відрізнятися.

Глибоке навчання показало чудову продуктивність для візуальних завдань розпізнавання, таких як розпізнавання дій та виявлення аномалій. Використання манинного навчання для вилучення функцій є звичайною практикою для виявлення аномалій на основі відео. Він показав краще представлення руху та зовнішнього вигляду порівняно з функціями ручної роботи. Як правило, карти глибоких особливостей показують розріджені риси. Останній стовпець може бути нормалізований між нулем і одиницею, тоді як для візуального огляду можна стверджувати, що елементи ознак, близькі до одного, є найбільш дискримінаційними ознаками. Наш аргумент полягає в тому, що ненульові елементи ознаки мають додаткову інформацію про об'єкт, що цікавить.

Розглянемо гіпотезу про те, що розрідженість глибинних рис має додаткову інформацію про клас, що цікавить. Щоб сформулювати це, розглянемо наївний баєсів класифікатор як еталонний підхід, де ми вводимо інформацію про розрідженість так само, ввівши інформацію про кардинальність. Однак підхід, заснованим на RFS, має такі характеристики: тимчасове впорядкування екземплярів глибоких ознак є важливим не інваріантним перестановкою, і маємо фіксовану кількість екземплярів на відео в множину, тоді як припущення RFS базується на рандомізації в обох випадках кількості та екземплярів елементи. Проблема виявлення аномалій реального відео сформульована в рамках декількох екземплярів на основі підходу наївного баєсів класифікатору. Це називається на основі розрідженості наївного баєсів класифікатору. Представлена запропонована структура для виявлення аномалій у відео реального спостереження. Запропоноване рішення, представлене та складається з трьох етапів: генерація множини і вилучення ознак, оцінка розрідженості множини і виявлення аномалії наївним баєсів класифікатором на основі розрідженості.

Розглянемо генерацію множини і особливість екстракції. Для генерації множини такий же підхід використовується для створення екземплярів відео. Ділимо відео на 32 сегменти (кліпи), в яких кожен сегмент представляє екземпляр в негативній множині. Під час тренінгу використовують як негативні, так і позитивні відео. Однак у підході використовуємо лише негативні (нормальні) екземпляри множин для навчання моделі. Для вилучення функцій відома функція використана, що є глибокими особливостями 3D-згортки, які раніше розглядали як просторові, так і часові.

Здійснимо оцінки розрідженості. Оскільки вихід модуля глибокого навчання завжди у векторному форматі, розмірність екземплярів завжди фіксована. Розрідженість глибинних ознак обчислюється шляхом підрахунку ненульових елементів в цифрах. Кожен екземпляр має різне число розрідженості. Запропонований підхід базується на багатократному навчанні, в якому потрібно класифікувати відеомножина як позитивну/аномальну або негативну/нормальну. Розрідженість всієї відеомножини обчислюється шляхом встановлення дискретного розподілу Пуассона по розрідженості кожного екземпляра та використання середнього значення Пуассона як розрідженості для всю відео множину.

У статистичному виявленні аномалій потрібно лише обчислити ймовірність вимірюваного набору екземплярів враховуючи, що він має негативну відеомножину. В даному випадку ймовірність задається рівнянням. Однак це рівняння не враховує розрідженість інформації відеомножини. Тому, передбачається, що відео екземпляри незалежні один від одного. Важливо зазначити, що рівняння є функцією ранжирування. Однак, як зазначалося раніше, функції екземплярів не є функціями RFS, оскільки кардинальність екземплярів фіксована, а не інваріантна перестановка.

На цьому етапі для найбільш параметричного статистичного машинного навчання метою є оцінка параметрів функції ймовірності, яка найкраще відповідає навчальним даним (яка асоціюються з негативними відеомножинами) за

допомогою оцінювача максимальної ймовірності або очікування-максимізації для моделей сумішей. У запропонованій розрідженості на основі виявлення аномалій для параметризованого розподілу розрідженості та мульти екземпляра. Навчальна фаза вищенаведеного рівняння перетворюється в оцінку параметрів. Наведену функцію оптимізації можна розкласти на дві окремі оптимізації для параметрів розрідженості і розподілів ознак. Для моделі розрідженості Пуассона оцінка параметра розрідженості перетворюється в оцінку середнього значення розподілу Пуассона наступним чином. Оскільки розподіл Пуассона має один ступінь свободи, то пропонується використовувати бета-розподіл для моделювання розподілу розрідженості. У запропонованій Бета-моделі оцінка параметрів розрідженості перетворюється в оцінку параметрів бета-розподілу.

Розглянемо результати експериментів з використанням інформації про розрідженість в моделі наївний баєсів класифікатор для виявлення аномалій з використанням реальних відеоданих спостереження. У експерименті демонструємо перевагу використання додаткової інформації про розрідженість в рамках моделі наївний баєсів класифікатор для виявлення аномалії у відео.

Набір даних складається з 3 різних типів аномалій. Для підготовки даних використовується підхід, в якому відеокадри були зменшені до 240 × 320 пікселів, при цьому частота кадрів була зафіксована до 30 кадрів в секунду. Для вилучення функцій просторово-часові особливості витягуються з повністю підключеного шару мережі. Оскільки мережа витягує функції для 16 послідовних кадрів, кожен екземпляр множини є середнім для всіх 16-кадрних кліпів з подальшою нормалізацією l 2. Розмір функції всього відео - 32× 4096. Для оцінки розрідженості обчислили інтенсивність розподілу Пуассона по розрідженості кожного екземпляра.

Розглянемо метрики оцінки результатів експериментів. Оцінка F1 використовується для оцінки ефективності запропонованого рішення.

Попередні результати запропонованого підходу. При такому підході для навчання моделі використовуються тільки звичайні дані. Заради порівняння

використовуються такі методи. Наївний баєсів класифікатор як метод статистичного розподілу Пуассона, розрідженість, і множина візуальних слів кодування за допомогою двійкового класифікатора. Двійковий SVM навчається з нелінійним ядром з гамма-установкою. Налаштування параметрів для нього виглядає наступним чином: розмір кодової книги встановлюється на кількість ітерацій кластеризації k-середніх, а розмір візуального слова - 50. Налаштування параметрів моделі розрідженості наївного баєсів класифікатору виглядає наступним чином: кількість компонентів Гауса встановлюється на 1, а кількість ітерацій - 30. Для всіх методів, заснованих на статистичних даних, поріг щільності встановлюється в 0.2 квантиль щільності ймовірності.

Кількісне порівняння з точки зору усередненого балу F1, точності та повторного виклику дано у відсотках для кожного методу. Метод виявлення аномалій наївного баєсів класифікатору на основі бета-розрідженості перевершує стандартний метод наївного баєсів класифікатору. Це демонструє, що використання витягнутої інформації про розрідженість підвищує точність граничного рішення. У експерименті моделювання бета-розрідженості досягає найкращого результату, використовуючи середній бал F1. Це пов'язано з більш високим ступенем свободи бета-розподілу порівняно з розподілом Пуассона. У доповненні модель наївний баєсів класифікатор має меншу продуктивність порівняно зі стандартною наївного баєсів класифікатору. представлена гістограма розрідженості інформації як позитивних, так і негативних відеомножин. Це показує, що використання розподілу для моделювання інформації про розрідженість не є доцільним моделюванням.

Пропонується новий підхід до виявлення аномалій на основі множини для реальних відеоданих спостереження. Підхід складається з двох модулів методу вилучення попередньо навчених глибоких ознак та методу виявлення аномалій на основі використаної інформації про розрідженість в межах модельного підходу наївного баєсів класифікатору. Ідея моделювання розрідженої інформації про глибокі функції та її використання як додаткової функції та моделювання

розрідженості за допомогою Пуассона та бета розподілу. Запропонований підхід оцінюється на наборі даних відеоспостереження. Експериментальні результати показують, що використання моделі наївного баєсів класифікатору перевершує стандартну модель наївного баєсів класифікатору за середнім балом F1. Цей підхід може бути розширений на виявлення аномалій на основі екземплярів, а результати можуть бути додатково покращені за допомогою більш точної моделі розподілу розрідженості, яка може бути додатково досліджена в майбутніх дослідженнях. Також, пропонується модель глибокого навчання, яка використовує тимчасову інформацію відеокадрів для виявлення аномалій за допомогою навчання для великомасштабних відео спостереження.

## 4.2. Виявлення аномалій відео згідно декількох екземплярів за допомогою глибокого тимчасового кодування-декодування

Попередньо був представлений модельний підхід до детекції аномалій на рівні множини у відео шляхом збирання розрідженості попередньо навчених глибоких функцій у навчанні. Далі пропонується слабо контрольоване рішення для кодування глибокого виявлення аномалій на рівні прикладу у відео спостереження за допомогою навчання з декількома екземплярами. Запропонований підхід використовує як ненормальні, так і звичайні відеокліпи на етапі навчання, який розроблений у множинній навчальній структурі, де відео розглядається як множина, а відеокліпи як екземпляри в множині. Основним внеском є запропонований новий підхід до розгляду часових відносин між відеосполученнями. Робота з відео-екземплярами (кліпами) як послідовними візуальними даними, а не набором незалежних екземплярів. Використаємо глибоку тимчасову мережу кодування-декодування, яка призначена для фіксації просторово-часової еволюції відео екземплярів з плином часу. Крім того, новою функцією втрат є пропозиція, яка максимізує середню відстань між нормальним і аномальним екземпляром.

Нова функція втрат забезпечує низьку швидкість помилкової тривоги, що має вирішальне значення в практичних програмах спостереження. Запропонований підхід тимчасового кодування-декодування зі зміненою втратою порівнюється з найсучаснішим. Результати показують, що запропонований метод працює аналогічно або краще, ніж найсучасніші рішення для виявлення аномалій у застосунках відеоспостереження та досягає найнижчого рівня помилкової тривоги на наборі даних.

Оскільки аномальні події, за визначенням, відбуваються рідко, їх зазвичай виявляють методи, при яких в навчанні використовуються тільки зразки часто повторюваних (нормальних) подій. Найбільш поширеним підходом є трактування аномальних подій як винятків з моделі, яка навчається за допомогою звичайних відео. Виявлення аномалій зазвичай виконується або за допомогою ручних функцій з подальшим вивченням функцій, або шляхом розробки наскрізної глибокої мережі. Більш раннє наближення до виявлення аномалій зазвичай передбачало вилучення особливостей траєкторії, щоб використовувати її здатність описувати динаміку рухомих об'єктів. Крім того, для виявлення аномалій були використані такі функції, як колір, текстура та оптичний потік, такі як колір, текстура та оптичний потік. Однак через зміни масштабу освітлення та деформації ці особливості погано генеруються для масштабного відеоаналізу. Останні роботи зі створення функцій за допомогою неконтрольованого глибокого навчання довели, що вони мають більшу стійкість до таких варіацій і краще працюють для вилучення функцій та навчання моделей.

Вищезгадані методи засновані на відхиленні від нормальності, що неоднозначно визначає межу між нормальним і аномальним, здебільшого через спостереження, що в багатьох застосунках загальні диференціації нормальних подій не можуть враховувати всі можливі нормальні закономірності або поведінку. Будь-яке нове виникнення нормальної події також може відхилитися від навченої моделі і викликати помилкову тривогу. Ця проблема була вирішена нещодавньою розробкою слабокерованих навчальних рішень для виявлення аномалій відео. Для

тренувань використовуються як звичайні, так і аномальні відео, а відео позначається як нормальне, тільки якщо всі відеокадри нормальні. На практиці маркування всіх кадрів у навчальних відео (тимчасове маркування) нездійсненне в багатьох застосунках. Так, використовуються слабокеровані мережі. Запропоновано впровадити рішення в рамках навчання декількох екземплярів, де доступна позначка множини (відео), а модель є навчена робити висновки про шаблон примірника. Вони використовують функцію втрати з декількома екземплярами і розробили мережу, яка обробляє послідовні сегменти відео (звані «кліпами») незалежно один від одного. Ще один слабо контрольований підхід до навчання - це навчання класифікатора під потреби. Мітки відносяться до нормальних сегментів в аномальному відео.

Пропонується нове слабокероване рішення, яке ієрархічно фіксує низьку, в термінах і високорівневу часову і просторову інформацію. Результат цієї роботи такий: нове рішення для виявлення аномалій у відео, яке використовує тимчасову мережу кодування для захоплення часової та просторової інформація відео-екземплярів, і формулювання цього рішення реалізується в рамках слабо контрольованих множинних екземплярів, де пропонується функцію втрат для плавного (диференційованого) відображення екземплярів у множини. Експерименти, що використовують два набори даних виявлення аномалій відео, демонструють, що рішення для повторного результату працює з точністю, порівняно з сучасним станом, і повертає нижчі показники помилкових спрацьовувань.

Найбільш поширеним підходом до виявлення візуальних аномалій є вилучення створених вручну або глибоких функцій представлення та вивчення їх як моделі. При такому підході аномалія виявляється, коли витягнуті ознаки не дуже добре підходять для вивченої моделі. Як наслідок, виявлення аномалії відстані зазвичай формулюється як проблема виявлення. Іншим класом рішень для виявлення аномалій є методи, засновані на відстеженні. У цих методах моделюється нормальна закономірність рухів об'єктів, що цікавлять, і будь-яке

відхилення ідентифікується як аномальне. Аналогічним підходом є виявлення аномалій на основі семантичної траєкторії сцени, в якому вперше виявляється об'єкт, що цікавить, з подальшим вилученням просторових і швидкісних ознак, які потім кластеризуються на основі їх подібності (з точки зору розмірів об'єктів і їх швидкостей). Результат використовується для формування траєкторій. Взагалі запропоновано ще одну методику виявлення аномалій — кластеризацію траєкторії моделей руху. По-перше, пікселі переднього плану виявляються за допомогою віднімання фону. Потім функції кластеризуються за допомогою алгоритму K-mean. Потім виявлення аномалій здійснюється шляхом порівняння вивченого розподілу ймовірностей моделі руху, отриманого з траєкторій. Загалом, методи на основі відстеження недостатньо надійні для складної відеосцени. Здійснимо аналіз, оскільки вони включають різні складні кроки, такі як виявлення об'єктів, асоціація даних та відстеження, і будь-який збій на цих етапах викликає збій у виявленні аномалій.

У зв'язку з обмеженнями методів, заснованих на відстеженні, для моделювання схеми руху для виявлення аномалій були використані створені вручну просторово-часові функції. Найбільш простим підходом є вилучення низькорівневих особливостей зовнішнього вигляду та сигналів руху, таких як колір, текстура та оптичний потік, і використання їх для моделювання рухової активності закономірності. Запропоновано використовувати модель соціальної сили в поєднанні з особливостями оптичного потоку для вивчення нормальної закономірності глобального руху, і будь-яке відхилення від цієї моделі (з малою ймовірністю) вважається аномалією. Використано при цьому детектор просторово-часової точки інтересу для виявлення області, що цікавить, а потім гістограму градієнта як дескриптор ознаки зовнішнього вигляду та гістограму оптичного потоку, оскільки дескриптор функцій руху використовувалися для виявлення аномальної активності у відео. Вирішують проблему виявлення просторових і часових аномалій у переповнених сценах шляхом спільного моделювання суміші зовнішнього вигляду та динаміки. Просторові аномалії виявляються за допомогою

дискретної імінантної саліентності, в той час як тимчасові аномалії виявляються як подія з низькою ймовірністю.

Останнім часом без нагляду глибоке навчання з використанням автокодера широко використовується для представлення прихованих ознак і виявлення аномалій. Далі використовують помилку реконструкції повністю підключеного автокодера згортки як оцінку аномалії. Запропоновано описове представлення ознак та зовнішнього вигляду за допомогою складеного автокодера. Виявлення аномалій виконується на основі оцінки аномалії, розрахованої за допомогою декількох однокласних SVM на основі вивченого представлення ознак. Запропоновано неконтрольоване виявлення аномалій, поєднавши автокондер з мережею. Отримана мережа намагається вивчити нормальний вигляд просторової структури через автокодер і пов'язану з ними картину руху від оптичного потоку через другий потік. Модифікована версія початкового модуля була інтегрована в мережу, що призвело до схеми на основі патчів для оцінки аномалії на рівні кадру. Мережа була навчена наскрізно з використанням трьох функцій втрати: функції втрати відстані, оптичної втрати потоку та змагальних втрат. В результаті розв'язано проблему виявлення аномалій шляхом використання здатності мережі запам'ятовувати нормальні події та оцінювати ступінь мережі. Запам'ятовування аспекту мережі криється помилкою реконструкції автокодера. Сюрпризальний аспект мережі моделюється шляхом розрахунку щільності латентних ознак за допомогою авторегресивної мережі. На тренувальному етапі функція втрати, що поєднує негативний журнал похибки реконструкції і щільність ймовірності прихованих ознак, полягає в моделюванні щільності ймовірності латентних ознак. Основа цього етапу роботи полягає в моделюванні щільності ймовірності латентних функції з використанням авторегресійної моделі. Більшість мереж на основі автокодерів засновані на елементарних заходах, таких як помилка в квадраті. Однак проблема метрики полягає в її поганих показниках при моделюванні властивостей зорового сприйняття людини. Наприклад, невеликий переклад зображення може спричинити велику піксельну помилку.

Більшість рішень, розроблених для виявлення аномалій у відео, засновані на неперевіреному навчанні, де для навчання використовуються лише звичайні відео, а виявлення аномалій виявляється як проблема виявлення, що відпадає (низька ймовірність, оцінка аномалій та помилка повторної побудови). Більшість наборів даних про аномалії відео, які використовуються для навчання та тестування, є короткими сценами і не можуть узагальнюватися на всі можливі нормальні закономірності. В результаті дуже важко побудувати межу між нормальними та аномальними подіями через відсутність відео, які моделюють усі можливі нормальні шаблони. Запровадив новий підхід, заснований на слабких наглядах, де для виявлення аномалій використовуються як нормальні, так і аномальні відео. У їх вирішенні проблема виявлення аномалій формулюється в рамках навчання декількох екземплярів, де доступна лише етикетка множини. Відео розділене на фіксовану кількість екземплярів (кліпів) і багатошарова мережа персептронів навчена прогнозувати мітки екземплярів на основі підходу глибокого ранжирування. Запропоновано вирішити проблему слабкого нагляду як контрольованого завдання навчання під міткою, в якому пропонують графік згорткової мітки. Ця мережа використовує відеооптималізатори, такі як схожість функцій та тимчасова узгодженість фрагментів відео для очищення шуму (нормальні сегменти аномального відео). На відміну від його чудової продуктивності і оскільки метод навчається з використанням всього відео на кожній ітерації, метод схильний до відношення даних. Щоб подолати проблему кореляції даних запропоновано тренувати мережу за допомогою пакетного підходу, де кожна партія складається з часово послідовних сегментів відео. Крім того, запропоновано механізм придушення нормальності, щоб придушити нормальні риси. Мережа займається екземплярами (кліпами) самостійно і не фіксує низьку, проміжну і довгу часову інформацію. Моделювання послідовностей використовувалося в різних областях, таких як моделювання мови, відео-узагальнення та сегментація дій для фіксації тимчасової інформації.

У зв'язку з успіхом тимчасової згортки в моделюванні послідовностей

представляємо тимчасову мережу кодування для виявлення аномалій у відео спостереження. Запропонована мережа має на меті зафіксувати часову інформацію між відео позиціями. Крім того, проблема також вирішується в рамках слабо контрольованої, і формулюємо функцію втрат, яка використовує середнє відображення, яке є більш плавним, ніж зазвичай використовувана операція. Функція втрат безпосередньо штрафує помилкові тривоги, що призводить до зниження показників помилкової тривоги на практиці.

Загальна архітектура запропонованого рішення реалізована як прямий шлях навченої мережі. У мережу передається послідовність відеокадрів. Потім за допомогою 3D-мережі витягуються просторово-часові функції і згодом розділені на послідовність з множин, що не перекриваються, кожна з яких називається кліпом. У цих дослідах n = 16. У контексті завдання відеовхід - це множина, а кліпи утворюють послідовні екземпляри в множині. Потім екземпляри обробляються тимчасовою мережею згортки, яка виступає в ролі класифікатора і виробляє прогнози для нормальності кожного кліпу. Кожне передбачення є нормалізованим скаляром, де одиниця має «аномальний екземпляр зі 100% впевненістю» і навпаки. Кінцевим виходом мережі є передбачення для всього відео. Це результат операції об'єднання над усіма прогнозами інстанцій. Використовуємо середнє об'єднання.

Тимчасова мережа згортки є основним елементом у загальній архітектурі запропонованого рішення, який виконує задачу моделювання послідовності шляхом побудови відображення. Важливим принципом, який необхідно враховувати при моделюванні послідовностей, є причинність. Кожна змінна повинна залежати тільки від попередніх ознак.

Пропонується до розгляду модифікована мережа. Нова мережа складається з тимчасового кодера /декодера, який складається з двох кроків. Кожен крок має тимчасовий згортковий шар, тимчасовий шар об'єднання для підвищення роздільної здатності та канальний шар нормалізації. У частинковій частині шар в мережі кодувальника/декодера містить набір тимчасових фільтрів, параметризованих тензором та індекс шару, тимчасову довжину тривалості

згортки і кількість фільтрів згортки в шарі. Ці фільтри призначені для уловлювання часових особливостей та їх еволюції до інших. Архітектура декодера схожа на кодер за винятком шару, який замінюється шаром підвищення роздільної здатності. Останній шар декодера - це сигмоїдний шар, який обчислює оцінку аномалії з тимчасовим доменом. Навчання проводиться в слабо контрольованих рамках з використанням нормальних і ненормальних відео. Тимчасова анотація ненормальних відео не надається. В результаті функція втрати формулюється в рамках навчання з декількома екземплярами.

Розглянемо навчання за допомогою багатократного навчання. У багатьох програмах відеоаналітики виявлення аномалій все відео позначено як звичайне/ненормальне, і присвоєння таких міток для індивідуальних кадрів або невеликих багатокадрових послідовностей (кліпів) не є ні практичним, ні середнім. Тому, для навчання запропонованої мережі в таких застосунках кращим варіантом є розробка навчального модуля в рамках машинного навчання, де, в цілому, завдання полягає в тому, щоб вивчити класифікатор на основі набору множини, кожен з яких містить кілька екземплярів. У цьому параметрі під час навчання доступні лише шаблони на множинах (а не шаблони примірників).

Запропонований підхід задає собою слабокероване рішення, сконструйоване в рамках машинного навчання. Навчальний набір даних спочатку включає різні відео (множини), кожне з яких позначено як звичайне або ненормальне. Набір даних перероблений в ансамбль відеопар, при цьому кожна пара складається з одного нормального і одного аномального відео. Елементи пар можуть бути обрані випадковим чином. Позначаються елементи навчального зразка (відеопара або пара «Множини»). Два відео передаються на вхід мережі і записуються на вихід мережі (прогнози на рівні екземпляра). Відзначимо, що в процесора машині це може бути реалізовано паралельно. Для навчальної вибірки позначимо прогнози на рівні екземпляра корекції. Спочатку цей екземпляр прогнозує, обчислює функцію втрат і згодом вага мережі змінюється.

У міні-пакетному навчальному модулі зміни ваги підсумовується для

кожної випадково обраної міні-партії, і далі застосовуються. У експериментах кожна партія включала 10 пар нормальних-аномальних відео.

Формулювання функції втрати таке, що кожна аномальна множина повинна мати більш високу аномалію. Тобто, бути більше, ніж будь-яка норма. Вони обчислюють оцінку аномалії, взявши максимальне об'єднання над прогнозами на рівні екземплярів. Розглянемо для обраної нотації припущення.

Перша складова частина задає екземпляр (сегмент), який має найвищий бал аномалії в даному аномальній підмножині (відео), і з високою ймовірністю є аномалією. Однак друга складова частини задає сегмент відео з найвищим балом аномалії в даному звичайному відео, яке, ймовірно, буде нормальним екземпляром. Рівняння втрат підтримує це припущення разом із максимізацією тимчасової плавності аномальних сегментів відео, а також мінімізує розрідженість їхніх оцінок. Вони є гіперпараметрами, що контролюють на розрідженість, Відповідно і дискретний градієнт прогнозів екземплярів, що використовується як міра тимчасової плавності. Дійсно, це термін регуляризації, щоб гарантувати, що оцінка аномалії аномального відео плавно змінюється від кожного сегмента відео до наступного. Останньою частиною є регуляризація розрідженості, яка відображає загальне очікування, що аномалія виникає протягом короткого періоду часу під час відносно тривалого аномального відео.

Вищезазначені втрати отримані відповідною функцією є в припущенні, що множина міток є виведено з максимуму. Проблема в тому, що максимальна функція не є гладкою і оптимізація страждає від зникаючих градієнтів. Щоб полегшити цю проблему, запропоновано використовувати середню різницю між нормальними та аномальними множинами в функції-втрати. Замість цього з операції при такому формулюванні враховуються оцінки всіх примірників в множині, включаючи той, що має максимальний бал. Визначена функція втрат максимізує дистанцію між вартістю. Всі максимальні операції замінені з усередненням і операцією, яка відома своєю швидкою конвергенцією. Подібно доданий терм регуляризації, щоб мінімізувати загальну суму.

Період аномальних екземплярів в множині для придушення балів нормальних екземплярів, який додає ще один термін регулярної доцільності. Функція кінцевих втрат може бути виражена через швидкість помилкової тривоги.

Використання функції в запропонованих втратах призводить до особливого акценту на зменшенні помилкових спрацьовувань, що повертаються навченою мережею. Помилкова тривога (помилкове спрацьовування) під час тренування означає, що для істинного нормального відео (множини), мережа повертає неправильно великий середній бал і відстань є негативною, Повернення терму у функції втрат - це чітко візуалізується. Отже, мінімізація такої функції втрат призводить до навченої мережі, яка робить акцент на придушенні помилкових спрацьовувань.

Навчання мережі шляхом мінімізації функції втрат також супроводжує негативи. Але меншого розміру. В вартості подія детальніше. Негативний фактор є для підстави-істини. Ненормальні відео мережа повертає при відносно малому значенні оцінки. Але це робить те саме для звичайних відео тому, що відстань незначна. Мережа є підготовкою для нормального відео. Вартість при цьому близька до нуля, залишаючи позитивну відстань, що становить і вносить менше, ніж помилкове спрацьовування, до загального значення втрат.

Розглянемо експеримент з двома наборами даних, які є набором даних і використовуються для проведення експериментів. Перший - це масштабний набір даних довгих відео з різними сценами, які відображають реальні ситуації. Набір даних складається з більше 40000 відео, розділених на навчальні та тестові набори. Навчальні набори складаються з 800 звичайних відео і 800 аномальних відео, а набори тестування включають 15 нормальних і 15 аномальних відео (200 відео). Аномальні відео як у навчанні, так і в тестуванні охоплюють 15 реальних сцен. Загальна тривалість набору даних становить 128 годин. У наборі даних немає тимчасової анотації (на рівні кадру), за винятком тестових відео. Набір даних є найбільшим набором даних про відеоагенції та єдиним, який має кілька сцен із реальними відео спостереження.

Другим набором даних є набір даних середнього масштабу, який містить 540 різних відео, знятих в університетському кампусі. Він має 25 різних сцен загальною кількістю 34555 кадрів з роздільною здатністю 456×956 пікселів з різними умовами освітлення та кутами камери. Набір даних зазвичай використовується для виявлення аномалій без нагляду, тому немає аномальних відео для навчання. Щоб пристосувати цей набір даних для слабо контрольованої проблеми, в якій навчальний набір має нормальні та ненормальні відео. Новий спліт має 145 нормальних і 62 аномальних тренувальних відео, а тестовий набір має 15 нормальних і 48 аномальних відео. Для справедливого порівняння використано той самий розподіл у експерименті. Особливість вилучення та генерації множини полягає в тому, що перед подачею кожного відеокадру в мережу його розмір змінюється до 240 × 320 з фіксованою частотою кадрів 30 кадрів в секунду. Та сама технологічна процедура використовується для вилучення майбутніх зображень. Просторово-часові особливості витягуються з повністю підключеного шару мережі пройшовши попередню підготовку на наборі даних. Мережа обчислює функції для кожних 16 кадрів (кліпу), а потім застосовує нормалізацію. Кожне відео розділене на 32 кліпи, що не перекриваються. Відео розглядається як множина, і кожен кліп розглядається як екземпляр в множині. Оскільки на множина є фіксована, то кількість екземплярів, функція екземпляра відео (кліп) генерується шляхом взяття середнього значення для всіх функцій 16-кадрового кліпу в межах цього відеокліпу. Під час навчання випадковим чином вибираються 30 нормальних і 30 аномальних відео, і використовуються в якості міні-партії в запропонованій мережі.

Запропонована мережа реалізується за допомогою python. Довжина тимчасового згорткового ядра встановлена на 4, і перевіряється та повідомляється про різні довжини ядра. Всі тимчасові шари згортки встановлюються в причинно-наслідковому режимі, щоб уникнути витоку майбутньої інформації. Фільтрам згортки, що використовуються в мережі, встановлено значення. Останній шар мережі - це тимчасовий повністю пов'язаний шар з активацією сигмоїдів.

Використаємо регуляризатор для параметрів ваги ядра в кожному шарі, і використаємо відсів зі швидкістю, встановленою на 0,7, щоб запобігти перенавантаженню. Адаптивний субградієнтний використовується для оновлення параметрів мережі з встановленою швидкістю навчання. Гіпер-параметр в функції втрат встановлений на 8. Для оцінки запропонованого методу використовуються характеристика приймача на основі рівня кадру (ROC) та площа під метриками кривої (AUC). Ці показники розраховуються за допомогою анотації до тестових відео на рівні кадру. Не використовуємо рівний рівень помилок, оскільки він не вимірює аномалію правильно.

Для справедливого порівняння запропонований метод порівнюється з методом базової лінії, а також додатковими методами. Запропонований метод використав словниковий підхід для вивчення нормального шаблону зі звичайних відео та використав помилку реконструкції як оцінку аномалії. Можна, також, використовувати глибокий автокодер, використовуючи звичайні відео для вивчення нормальних уявлень функцій, і використовувати помилку реконструкції як оцінку аномалії.

ROC-крива є графіком, що використовується для оцінки якості бінарної класифікації. Вона відображає співвідношення між часткою об'єктів, які мають ознаку і правильно класифіковані, та часткою об'єктів без ознаки, що помилково класифіковані. Цей аналіз називається ROC-аналізом, а показник AUC дає кількісну інтерпретацію ROC. Високе значення AUC свідчить про високу якість класифікатора, а значення 0,5 вказує на непридатність методу класифікації.

Математична модель - це наближений опис явищ зовнішнього світу, виражений математичною символікою. Вона використовується для пізнання, прогнозування та управління. Моделювання полягає у дослідженні властивостей об'єкта шляхом аналізу аналогічних властивостей іншого об'єкта, який знаходиться у відповідності з першим. Модель може бути реалізована у вигляді макета, пристрою, або зафіксована у вигляді рівнянь, формул, графіків, креслень тощо. Характеристики математичних моделей включають ступінь універсальності,

точність, адекватність та економічність. Вибір об'єктів та методів моделювання залежить від поставленої задачі.

Для оцінки точності математичної моделі, порівнюють значення параметрів реального об'єкта зі значеннями тих же параметрів, що отримані за допомогою моделі. Здійснюють це через розрахунок відхилення цих параметрів.

Адекватність моделі - її здатність відображати властивості об'єкта з похибкою, не більше заданої. Зазвичай адекватність моделі спостерігається в обмеженій області зміни зовнішніх параметрів, яку називають областю адекватності математичної моделі. На практиці, подібність моделі та оригіналу є важливим фактором для досягнення адекватності моделювання. При повній подібності, перебіг процесів у часі та просторі повністю співпадає, що характеризує досліджуване явище стосовно конкретної постановки задачі дослідження. Якщо подібність перебігу процесів лише в просторі чи лише в часі, то таку подібність називають неповною. Наближена подібність характеризується застосуванням спрощених допущень, що дозволяють вважати подібними відмінні процеси за рахунок свідомих спотворень деяких їх властивостей. Така подібність може бути як повною, так і неповною. Наприклад, якщо порівнюють два генератори на основі спрощених рівнянь, що не враховують аперіодичну складову струму статора і періодичну складову струму ротора, то таку подібність можна вважати наближеною.

Кількісні порівняння в розрізі методів спостерігається такими, що використання нормальних та аномальних відео на тренувальній фазі збільшує справжню позитивну швидкість. Крім того, очевидно, що запропонований нами підхід має вищий справжній позитивний показник порівняно з базовим методом. Отримана мережа зі зміненою функцією втрат досягає третього місця в порівнянні з найсучаснішими результатами з виявлення аномалій відео. Тренування мережі з втратами досягає більш високих результатів у порівнянні з іншою мережею, оскільки отримана мережа використовує тимчасові зв'язки між відео екземплярами через просторово-часовий автокодер.

Зразки якісних результатів на чотирьох різних відео, що представляють випадки успіху та невдачі, проаналізуємо так. Два випадки показують, як запропонований метод своєчасно дає високий бал аномалії для аномальних відео. В основному це пов'язано з використанням тимчасової згортки над екземплярами в запропонованій мережі.

На рис. 4.1 зображена візуалізація еволюції оцінок аномалій на рівні кадру над навчальними ітераціями. Очевидно, що зі збільшенням ітераційного числа запропонований метод починає прогнозувати правильні оцінки аномалій для обох нормальних і аномальних. Запропонована функція втрат поверне дуже малі показники помилкових спрацьовувань на практиці. Щоб перевірити це, продуктивність запропонованого методу порівнюється на звичайних тестових відео. Рівень помилкової тривоги повідомляється на рівні 50% порогу для різних методів. Запропонована модель навчається на вибірці за допомогою тестового набору. Використовується той самий протокол з вилучення функцій та параметрів моделі. Результати продемонстрували, що запропонована модель генерує конкурентні результати порівняно з найсучаснішими. Точність моделі (AUC) перевершує на значних 16,4 %.

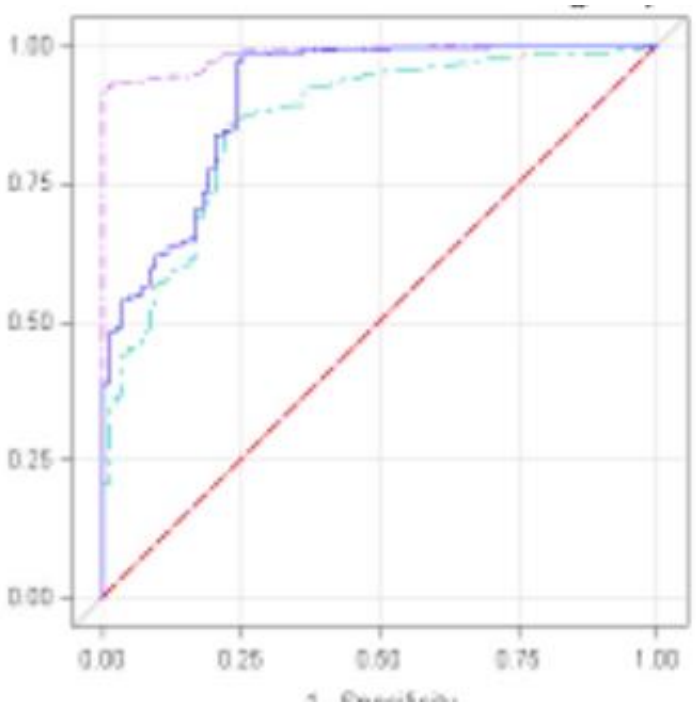



Рисунок 4.1 – ROC – криві за результатами експериментів

Мережева архітектура відрізняється так.

По-перше, мережа використовувалася для сегментації дій і пройшла навчання під наглядом.

Також, мережа навчається за допомогою слабкого нагляду.

Щоб пристосувати мережу до проблеми, змінено останній рівень, регуляризацію мережі та кількість наповнювачів згортки.

Крім того, використано функцію і аналогічні налаштування параметрів.

Розглянемо представлення дослідження впливу різних комбінацій функції втрат, таких як тимчасова гладкість і терміни розрідженості.

У загальному випадку різні терміни функції втрат можна виразити наступним чином: вплив тимчасового розміру ядра згортки.

Розглянемо глибоку тимчасову мережу кодування-декодування для виявлення аномалій в застосунках відеоспостереження.

Запропоноване рішення базується на глибокому ранжируванні множинного прикладного навчання, де під час навчання використовуються звичайні та аномальні відео для локалізації події аномалії у відео реального спостереження.

Маємо відео-екземпляри (кліпи) як послідовні візуальні данні та будуємо тимчасову мережу кодування, яка використовує низьку, проміжну та високорівневу просторово-часову еволюцію між екземплярами функцій.

У зв'язку з відсутністю часової анотації екземплярів відео, використовуємо середню суму предикації екземпляра для об'єднання від прикладного рівня до предикації на рівні множини.

Тому, запропонована функція втрат є більш плавною, ніж використана. Крім того, функція втрати забезпечує низьку помилкову тривогу під час тренування.

Результати експериментів з використанням нормальних і аномальних відео в наборі даних продемонстрували ефективність запропонованого рішення.

## 4.3. Висновки

В результаті розроблено новий метод виявлення аномалій в зображеннях кіберфізичними системами комп’ютерного зору. Проведені експериментальні дослідження підтвердили ефективність запропонованого рішення.

- удосконалено архітектуру кіберфізичних систем комп’ютерного зору.

На основі проведених досліджень розроблена архітектура кіберфізичних систем комп’ютерного зору та метод виявлення аномалій в зображеннях, який імплементовано в обчислювальну підсистему кіберфізичної системи.

# ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень новий метод виявлення аномалій в зображеннях кіберфізичними системами комп’ютерного зору удосконалено архітектуру кіберфізичних систем комп’ютерного зору.

У першому розділі проведено аналіз відомих рішень з виявлення аномалій в зображеннях.

У другому розділі удосконалено архітектуру кіберфізичних систем комп’ютерного зору та розроблено метод виявлення аномалій в частині статичних зображень.

У третьому розділі розроблено метод виявлення аномалій в частині виявлення дефектів в зображеннях.

У четвертому розділі розроблено метод виявлення аномалій в частині динамічних зображень.

На основі проведених досліджень розроблена архітектура кіберфізичних систем комп’ютерного зору та метод виявлення аномалій в зображеннях, який імплементовано в обчислювальну підсистему кіберфізичної системи [80, 81]. Проведені експериментальні дослідження підтвердили ефективність запропонованого рішення.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Bay H., Ess A., Tuytelaars T., Van Gool L. Speeded-up robust features (SURF). *Computer vision and image understanding.* 2008. Vol. 110(3). P. 346–359.

2. Beaudet P. R. Rotationally invariant image operators. *Proc. 4th Int. Joint Conf. Pattern Recog*, Tokyo, Japan, 1978.

3. Mabrouk A. Ben and Zagrouba E. Abnormal behavior recognition for intelligent video surveillance systems: A review. *Expert Syst. Appl.* ISSN 0957-4174. doi: 10.1016/J.ESWA.2017.09.029, 2018, P. 480–491.

4. Bergeron C., Moore G., Zaretzki J., Breneman C. M., and Bennett K. P. Fast Bundle Algorithm for Multiple-Instance Learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2011. P. 1068–1079.

5. Bergman L. and Hoshen Y. *Classification-based anomaly detection for general data.* arXiv preprint arXiv:2005.02359, 2020.

6. Bergmann P., Fauser M., Sattlegger D., and Steger C. MVTec AD–A Comprehensive Real-World Dataset for Unsupervised Anomaly Detection. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2019. P. 9592–9600.

7. Bishop C. M. Pattern Recognition and Machine Learning. springer, Springer New York, USA, 2006. Bosch A., Zisserman A., and Mu˜noz X. *Scene Classification using a Hybrid Generative/Discriminative Approach*. *IEEE transactions on pattern analysis and machine intelligence*, 2008. P. 712–727.

8. B¨ottger T. and Ulrich M. Real-Time Texture Error Detection on Textured Surfaces with Compressed Sensing. *Pattern Recognition and Image Analysis*, 2016. P. 88–94.

9. Buda M., Maki A., and Mazurowski M. A. A systematic study of the class imbalance problem in convolutional neural networks. *Neural Networks*, 2018. P. 249–259.

10. Burghouts G. J. and Geusebroek J.-M. Material-Specific Adaptation of Color

Invariant Features. *Pattern Recognition Letters*, 2009. P. 306–313.

11. Busam B., Ruhkamp P., Virga S., Lentes B., Rackerseder J., Navab N., and Hennersperger C. Markerless inside-out tracking for 3d ultrasound compounding. In Simulation, Image Processing, and Ultrasound Systems for Assisted Diagnosis and Navigation, 2018. P. 56–64.

12. Cai Y., Wang H., Chen X., and Jiang H. Trajectory-Based Anomalous Behaviour Detection for Intelligent Traffic Surveillance. *IET intelligent transport systems*, 2015. P. 810–816.

13. Cao B., Araujo A., and Sim J. Unifying deep local and global features for image search. *In European Conference on Computer Vision*, Glasgow, United Kingdom, 2020. P. 726–743.

14. Cao N., Lin C., Zhu Q., Lin Y.-R., Teng X., and Wen X. Voila: Visual anomaly detection and monitoring with streaming spatiotemporal data. *IEEE transactions on visualization and computer graphics*, 2017. P. 23–33.

15. Carbonneau M.-A., Cheplygina V., Granger E., and Gagnon G. Multiple Instance Learning: A Survey of Problem Characteristics and Applications. *Pattern Recognition*, 2018. P. 329–353.

16. Cavalli R. M., Licciardi G. A., and Chanussot J. Detection of Anomalies Produced by Buried Archaeological Structures using Nonlinear Principal Component Analysis Applied to Airborne Hyperspectral Image. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2012. P. 659–669.

17. Cha Y.-J., Choi W., Suh G., Mahmoudkhani S., and B¨uy¨uk¨ozt¨urk O. Autonomous Structural Visual Inspection using Region-based Deep Learning for Detecting Multiple Damage Types. *Computer-Aided Civil and Infrastructure Engineering*, 2018. P. 731–747.

18. Chalapathy R., Menon A. K., and Chawla S. Anomaly Detection using One-Class Neural Networks. arXiv preprint arXiv:1802.06360, 2018.

19. Chandola V., Banerjee A., and Kumar V. Anomaly Detection: A Survey. ACM Comput. Surv., 41(3):15:1–15:58. ISSN 0360-0300. doi: 10.1145/ 1541880.1541882,

2009.

20. Chang C.-C. and Lin C.-J. LIBSVM: A library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2011, 2:27:1–27:27.

21. Chen F.-C. and Jahanshahi M. R. NB-CNN: Deep Learning-Based Crack Detection using Convolutional Neural Network and Na¨ıve Bayes Data Fusion. *IEEE Transactions on Industrial Electronics*, 2017. P. 4392–4400.

22. Chen W.-Y., Liu Y.-C., Kira Z., Wang Y.-C. F., and Huang J.-B. A closer look at few-shot classification. arXiv preprint arXiv:1904.04232, 2019.

23. Chen Y., Wang J., Xia R., Zhang Q., Cao Z., and Yang K. The Visual Object Tracking Algorithm Research Based on Adaptive Combination Kernel. *Journal of Ambient Intelligence and Humanized Computing*, 2019.

24. Cheng K.-W., Chen Y.-T., and Fang W.-H. Video Anomaly Detection and Localization using Hierarchical Feature Representation and Gaussian Process Regression. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015. P. 2909–2917.

25. Chiu S. N., Stoyan D., Kendall W. S., and Mecke J. Stochastic geometry and its applications. John Wiley & Sons, 2013.

26. Cho S.-H. and Kang H.-B. Abnormal Behavior Detection using Hybrid Agents in Crowded Scenes. Pattern Recognition Letters, 2014. P. 64–70.

27. Chollet F. et al. keras, 2015. Choukroun Y., Bakalo R., Ben-Ari R., Akselrod-Ballin A., Barkan E., and Kisilev P. Mammogram Classification and Abnormality Detection from Nonlocal Labels using Deep Multiple Instance Neural Network. *In VCBM*, 2017. P. 11–19.

28. Christiansen P., Nielsen L. N., Steen K. A., Jørgensen R. N., and Karstoft H. DeepAnomaly: Combining background subtraction and deep learning for detecting obstacles and anomalies in an agricultural field. Sensors, 2016, 16(11):1904.

29. Cong Y., Yuan J., and Liu J. Sparse Reconstruction Cost for Abnormal Event Detection. In CVPR 2011. P. 3449–3456.

30. Cribari-Neto F. and Vasconcellos K. L. P. Nearly Unbiased Maximum

Likelihood Estimation for the Beta Distribution. *Journal of Statistical Computation and Simulation*, 72(2):107–118, 2002. doi: 10.1080/00949650212144. URL https://doi.org/10.1080/00949650212144.

31. Cui P., Sun L.-F., Liu Z.-Q., and Yang S.-Q. A sequential monte carlo approach to anomaly detection in tracking visual events. *In 2007 IEEE Conference on Computer Vision and Pattern Recognition*. P. 1–8. IEEE, 2007.

32. Cui X., Liu Q., Gao M., and Metaxas D. N. Abnormal Detection using Interaction Energy Potentials. *In Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, P. 3161–3167. IEEE, 2011. ISBN 9781457703942. doi: 10.1109/CVPR.2011.5995558. URL http://ieeexplore.ieee.org/document/5995558/.

33. Dai A., Chang A. X., Savva M., Halber M., Funkhouser T., and Nießner M. ScanNet: Richly-annotated 3D Reconstructions of Indoor Scenes. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2017. P. 5828–5839.

34. Dai W., Mujeeb A., Erdt M., and Sourin A. Soldering defect detection in automatic optical inspection. Advanced Engineering Informatics, 43:101004, 2020.

35. Dalal N. and Triggs B. Histograms of Oriented Gradients for Human Detection. *In 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05), volume 1, IEEE*, 2005. P. 886–893.

36. Deecke L., Vandermeulen R., L. Ruff, S. Mandt, and M. Kloft. Image Anomaly Detection with Generative Adversarial Networks. *In Joint european conference on machine learning and knowledge discovery in databases*, 2018. P. 3–17.

37. Defard T., Setkov A., Loesch A., and Audigier R. PaDiM: a patch distribution modeling framework for anomaly detection and localization. arXiv preprint arXiv:2011.08785, 2020.

38. Giorno A. Del, Bagnell J. A., and Hebert M. A Discriminative Framework for Anomaly Detection in Large Videos. *In Proceedings of European Conference on Computer Vision (ECCV)*, 2016. P. 334–349.

39. DeTone D., Malisiewicz T., and Rabinovich A. Toward geometric deep slam. arXiv preprint arXiv:1707.07410, 2017.

40. DeTone D., Malisiewicz T., and Rabinovich A. Superpoint: Self-Supervised Interest Point Detection and Description. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2018. P. 224–236.

41. Deusch H., Reuter S., and Dietmayer K. The labeled multi-Bernoulli SLAM filter. *IEEE Signal Processing Letters*, 2015. P. 1561–1565.

42. Diehl C. P. and Hampshire J. B. Real-Time Object Classification and Novelty Detection for Collaborative Video Surveillance. *In Proceedings of the 2002 International Joint Conference on Neural Networks.* IJCNN'02 (Cat. No.02CH37290), volume 3, May 2002. P. 2620–2625 vol.3. doi: 10.1109/ IJCNN.2002.1007557.

43. Ding C., Fan S., Zhu M., Feng W., and Jia B. Violence Detection in Video by Using 3D Convolutional Neural Networks. *In International Symposium on Visual Computing*, 2014. P. 551–558.

44. Domingues R., Michiardi P., Zouaoui J., and Filippone M. Deep Gaussian Process Autoencoders for Novelty Detection. Machine Learning, 2018. P. 1–21.

45. Donahue J., Jia Y., Vinyals O., Hoffman J., Zhang N., Tzeng E., and Darrell T. DeCAF: A Deep Convolutional Activation Feature for Generic Visual Recognition. In Xing E. P. and Jebara T., editors, *Proceedings of the 31st International Conference on Machine Learning, Proceedings of Machine Learning Research*, P. 647–655, Bejing, China, 22–24 June 2014. PMLR. URL https:// proceedings.mlr.press/v32/donahue14.html. J. Dong and S. Soatto. Domain-Size Pooling in Local Descriptors: DSP-SIFT. *In The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2015.

46. Du B. and Zhang L. Random-Selection-Based Anomaly Detector for Hyperspectral Imagery. *IEEE Transactions on Geoscience and Remote Sensing*, 2010. P. 1578–1589.

47. Duchi J., Hazan E., and Singer Y. Adaptive Subgradient Methods for Online Learning and Stochastic Optimization. *Journal of machine learning research*, 2011. P. 2121–2159.

48. Dusmanu M., Rocco I., Pajdla T., Pollefeys M., Sivic J., Torii A., and Sattler

T. D2- Net: A Trainable CNN for Joint Description and Detection of Local Features. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2019. P. 8092–8101.

49. Elbehiery H. M., Hefnawy A. A., and Elewa M. T. Visual Inspection for Fired Ceramic Tile's Surface Defects using Wavelet Analysis. *GVIP* (05), 2005. P. 1–8.

50. Fan Y., Wen G., Li D., Qiu S., Levine M. D., and Xiao F. Video anomaly detection and localization via gaussian mixture fully convolutional variational autoencoder. Computer Vision and Image Understanding, 195:102920, 2020.

51. Fang Q., Li H., Luo X., Ding L., Luo H., Rose T. M., and An W. Detecting non-hardhat-use by a deep learning method from far-field surveillance videos. Automation in Construction, 85:1–9, January 2018a. doi: 10.1016/j.autcon.2017. 09.018.

52. Fang Q., Li H., Luo X., Ding L., Rose T. M., An W., and Yu Y. A deep learningbased method for detecting non-certified work on construction sites. Advanced Engineering Informatics, 35:56–68, 2018b. ISSN 1474-0346. doi: https://doi.org/ 10.1016/j.aei.2018.01.001.

53. Farha Y. A. and Gall J. MS-TCN: Multi-Stage Temporal Convolutional Network for Action Segmentation. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019. P. 3575–3584.

54. Feng Y., Yuan Y., and Lu X. Learning deep event models for crowd anomaly detection. Neurocomputing, 2017. P. 548–556.

55. Fr´enay B. and Verleysen M. Classification in the presence of label noise: a survey. *IEEE transactions on neural networks and learning systems*, 2013. P. 845–869.

56. Galata D. L., M´esz´aros L. A., K´allai-Szab´o N., Szab´o E., Pataki H., Marosi G., and Nagy Z. K. Applications of machine vision in pharmaceutical technology: A review. *European Journal of Pharmaceutical Sciences*, 159:105717, 2021.

57. Gao Y., Li X., Wang X. V., Wang L., and Gao L. A Review on Recent Advances in Vision-based Defect Recognition towards Industrial Intelligence. *Journal of Manufacturing Systems*, 2021.

58. Garg S., Kaur K., Kumar N., and Rodrigues J. J. P. C. Hybrid Deep-

LearningBased Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective. *IEEE Transactions on Multimedia*, 2019. P. 566–578. ISSN 1520-9210. doi: 10.1109/TMM.2019.2893549.

59. Gibert X., Patel V. M., and Chellappa R. Robust Fastener Detection for Autonomous Visual Railway Track Inspection. *In 2015 IEEE Winter Conference on Applications of Computer Vision*, IEEE, 2015. P. 694–701.

60. Gibert X., Patel V. M., and Chellappa R. Deep Multitask Learning for Railway Track Inspection. *IEEE transactions on intelligent transportation systems*, 2016. P. 153–164.

61. Girshick R. Fast R-CNN. In Proceedings of the 2015 IEEE International Conference on Computer Vision (ICCV), ICCV '15, pages 1440–1448, Washington, DC, USA, 2015. *IEEE Computer Society*. ISBN 978-1-4673-8391-2. doi: 10.1109/ICCV.2015. 169.

62. Gnanavel V. and Srinivasan A. Abnormal Event Detection in Crowded Video Scenes. *In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (Ficta)* 2014. P. 441–448.

63. Golan I. and El-Yaniv R. Deep anomaly detection using geometric transformations. In Advances in Neural Information Processing Systems, 2018. P. 9758–9769.

64. Golnabi H. and Asadpour A. Design and application of industrial machine vision systems. Robotics and Computer-Integrated Manufacturing, 2007. P. 630–637.

65. Gong D., Liu L., Le V., Saha B., Mansour M. R., Venkatesh S., and Hengel A. v. d. Memorizing normality to detect anomaly: Memory-augmented deep autoencoder for unsupervised anomaly detection. *In Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2019. P. 1705–1714.

66. Goyal S., Raghunathan A., Jain M., Simhadri H. V., and Drocc P. Jain. Deep robust one-class classification. *In International Conference on Machine Learning PMLR*, 2020. P. 3711–3721.

67. Grathwohl W., Wang K.-C., Jacobsen J.-H., Duvenaud D., Norouzi M., and

Swersky K. Your classifier is secretly an energy based model and you should treat it like one. arXiv preprint arXiv:1912.03263, 2019.

68. Graves A., Fern´andez S., and Schmidhuber J. Bidirectional LSTM Networks for Improved Phoneme Classification and Recognition. *In International Conference on Artificial Neural Networks*, 2005. P. 799–804.

69. Guan H., Zhang Y., Xian M., Cheng H.-D., and Tang X. Smote-wenn: Solving class imbalance and small sample problems by oversampling and distance scaling. Applied Intelligence, 2021. P. 1394–1409.

70. Han S., Mao H., and Dally W. J. Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding. arXiv preprint arXiv:1510.00149, 2015.

71. Harris C. G., Stephens M., et al. A combined corner and edge detector. In Alvey vision conference, pages 10–5244. Citeseer, 1988. Harrou F., Zerrouki N., Dairi A., Sun Y., and Houacine A. Automatic human fall detection using multiple tri-axial accelerometers. *In 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT).* IEEE, 2021. P. 74–78.

72. Suto K., Nishiyama H., Kato N., Nakachi T., Sakano T., and Takahara A. A failure-tolerant and spectrum-efficient wireless data center network design for improving performance of Big Data mining. *Proceedings of IEEE Vehicular Technology Conference (VTC Spring).* 2015. P. 1–5.

73. Riza N. and Marraccini P., Power smart indoor optical wireless link applications. Wireless Commun. and Mobile Comput. 2012. P. 327–332.

74. Hamedazimi N., Gupta H., Sekar V., and Das S. Patch panels in the sky: A case for free-space optics in data centers. ACM Hotnets. 2013. P. 1–23.

75. Bao J., Dong D., Zhao B., Luo Z., Wu C., and Gong Z. Flycast: Free-space optics accelerating multicast communications in physical layer. SIGCOMM Comput. Commun. Rev. 2015. vol. 45, no. 5. P. 97–98.

76. Arnon S. Next-generation optical wireless communications for data centers, *Proc. SPIE*. 2015. vol. 9387. P. 703–938.

77. Joseph J., Lear K, and Abell D. High speed free-space optical communications. *WO Patent App.* PCT/US2012/052,397, Mar. 7. 2013.

78. Hu W. and Zeng Q. Multicasting optical cross connects employing splitterand-delivery switch. *Proceedings of IEEE Photon.* Technol. Lett. 1998. vol. 10, no. 7. P. 970–972.

79. Zhang C. and Hu W. Design and analysis of a multicast-capable optical crossconnect. *Proc. SPIE.* 2008. vol. 7136.

80. Клейн О. Метод та засоби виявлення аномалій в системах комп'ютерного зору / *Збірник наукових праць за матеріалами XIV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2021»*. Хмельницький, 2022, С.139-141.

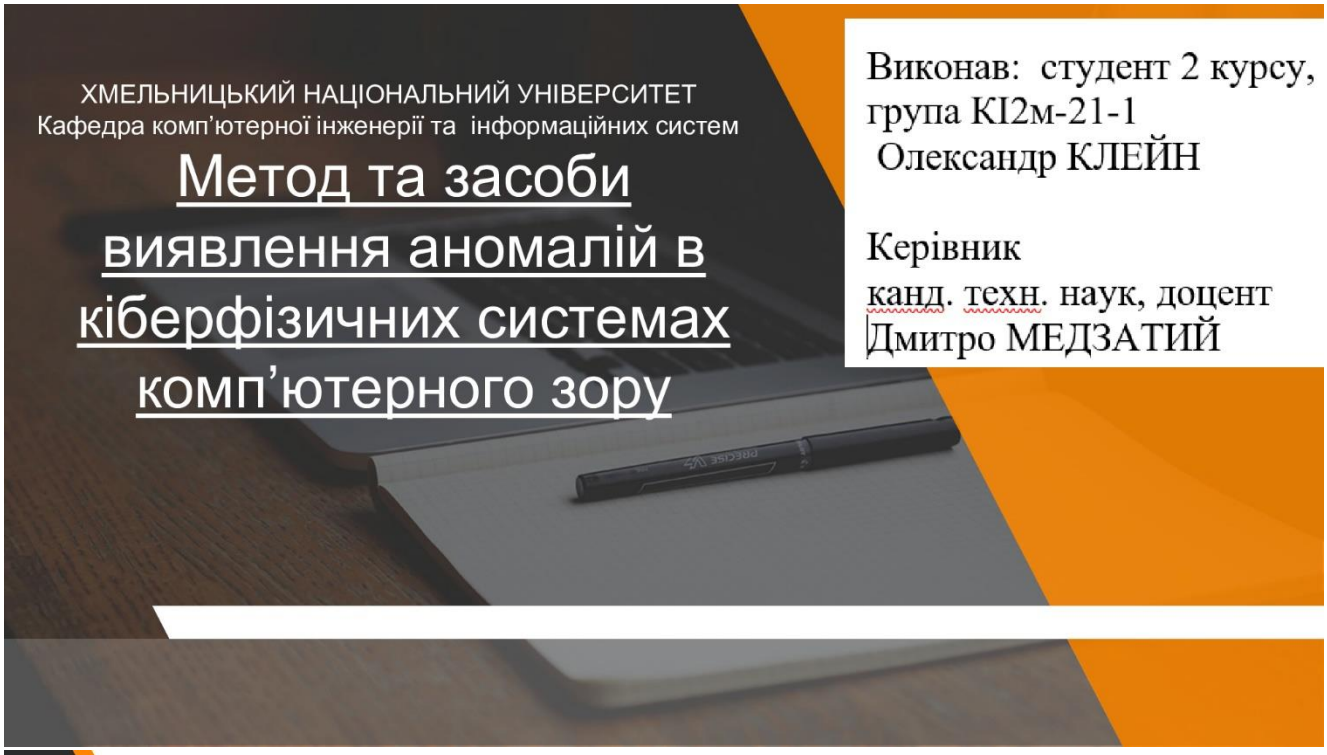
https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn2022_corpuspaper.pdf

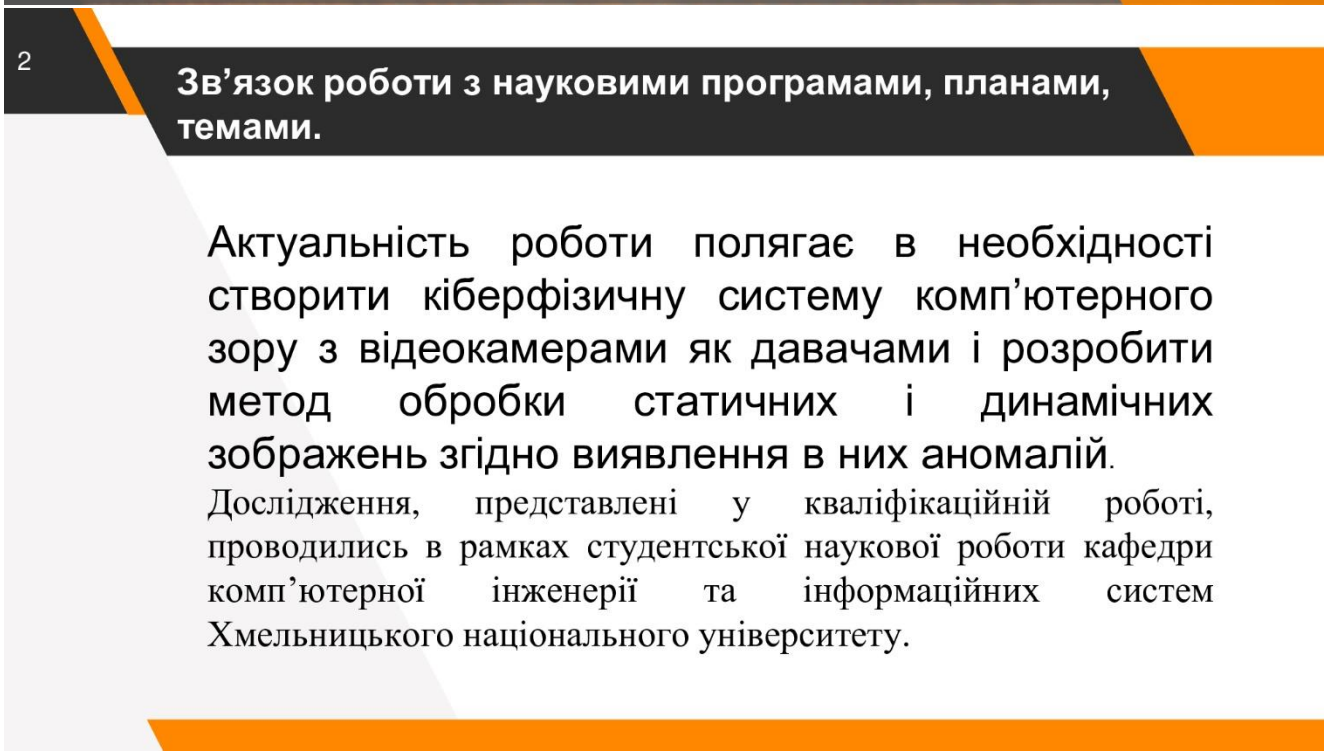
81. Denys Liubinetskyi, Antonina Kashtalian, Tomas Sochor, Andrii Selskyi, Olexandr Klein. Distributed System for Predicting Malicious Activity in Computer Networks. The 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2023) : *CEUR-Workshop Proceedings*. – Vol. 3373. (Khmelnytskyi, 22-24 March 2023). – Khmelnytskyi, 2023. – P. 401–410.

https://ceur-ws.org/Vol-3373/

**ДОДАТОК А**
(обов'язковий)

**ПРЕЗЕНТАЦІЯ**



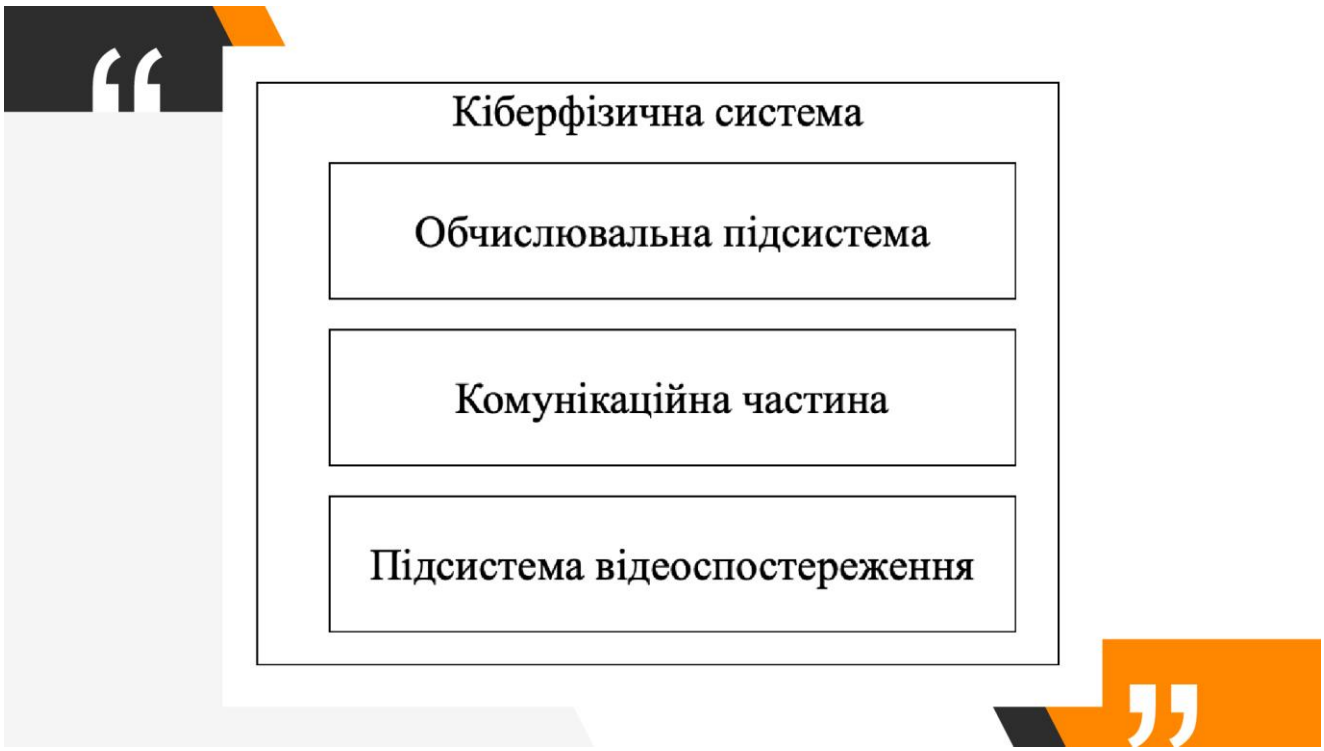
- *Метою кваліфікаційої роботи є розробка методу виявлення аномалій в кіберфізичних системах комп'ютерного зору.*
- *Поставлена мета досягається розв'язанням таких основних задач:*
- *проаналізувати відомі методи виявлення аномалій в рухомих зображеннях;*
- *розробити метод виявлення аномалій в зображеннях кіберфізичними системами комп'ютерного зору;*
- *удосконалити архітектуру кіберфізичних систем комп'ютерного зору;*
- *здійснити постановку експерименту та провести есперементальні дослідження згідно розроблених рішень.*

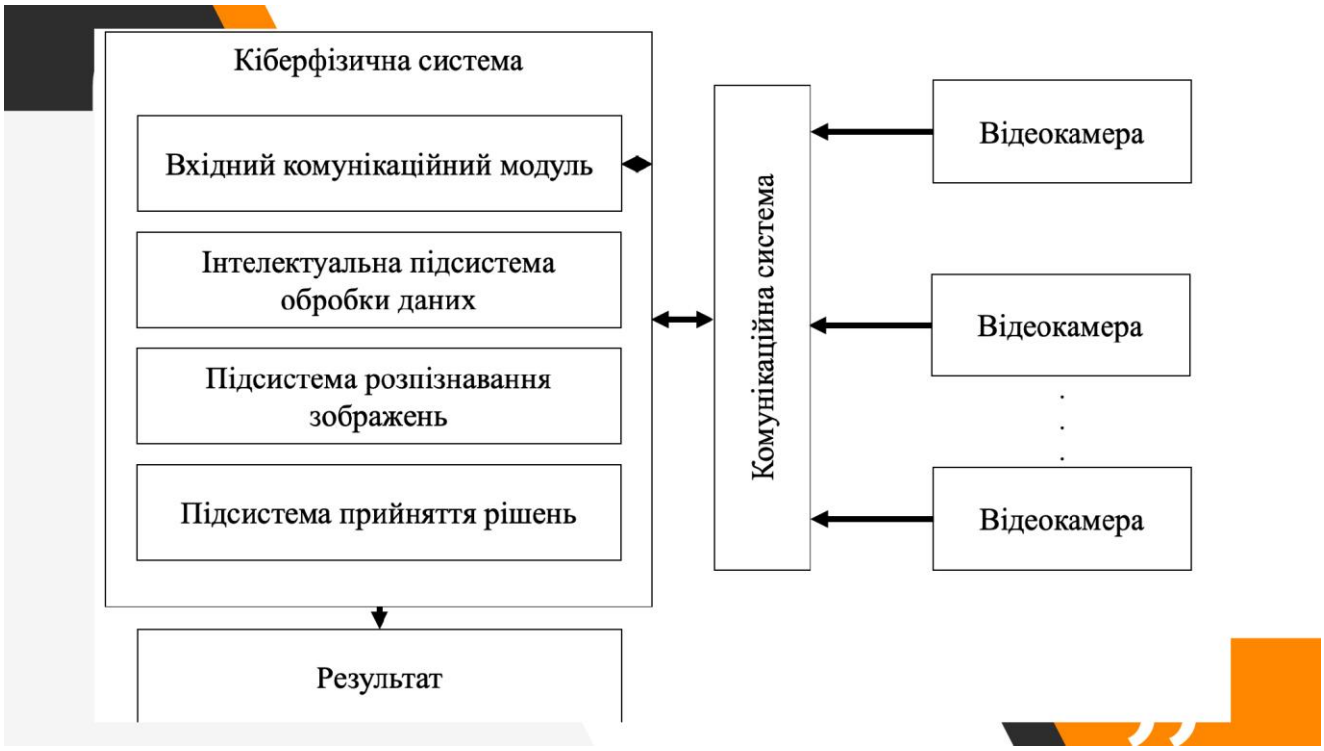
- *Об'єктом дослідження є процес виявлення аномалій в кіберфізичних системах комп'ютерного зору.*
- *Предметом дослідження є методи виявлення аномалій в кіберфізичних системах комп'ютерного зору.*

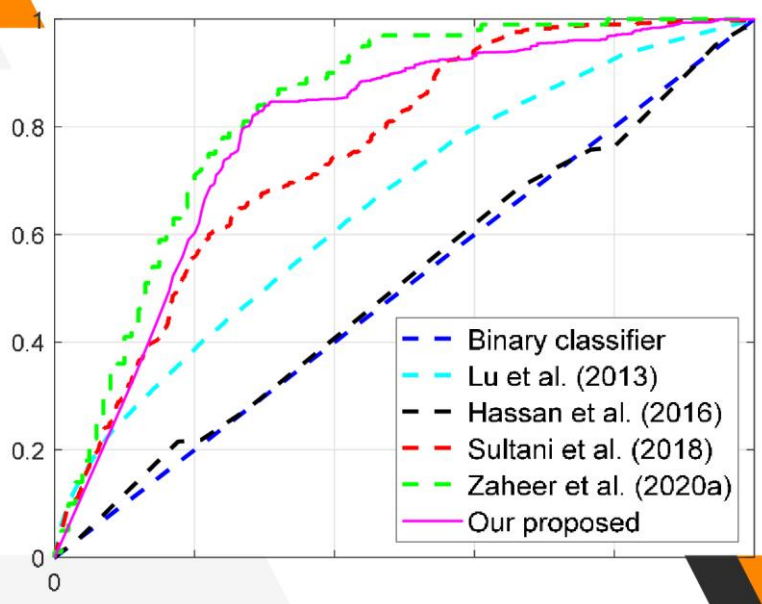
- *Наукова новизна отриманих результатів:*
- *вперше розроблено метод виявлення аномалій в зображеннях кіберфізичними системами комп'ютерного зору;*
- *удосконалено архітектуру кіберфізичних систем комп'ютерного зору.*
- *На основі проведених досліджень розроблена архітектура кіберфізичних систем комп'ютерного зору та метод виявлення аномалій в зображеннях, який імплементовано в обчислювальну підсистему кіберфізичної системи.*
- *Практична значимість отриманих результатів полягає у розробленій архітектурі кіберфізичних систем комп'ютерного зору.*

***Метод** виявлення аномалій в зображеннях кіберфізичними системами комп'ютерного зору **складається з таких трьох кроків:***

- *1) виявлення аномалій статичних зображень;*
- *2) виявлення аномалій дефектів в зображеннях;*
- *3) виявлення аномалій динамічних зображень.*


Кіберфізична система
Обчислювальна підсистема
Комунікаційна частина
Підсистема відеоспостереження


Кіберфізична система
Вхідний комунікаційний модуль
Інтелектуальна підсистема обробки даних
Підсистема розпізнавання зображень
Підсистема прийняття рішень
Результат
Комунікаційна система
Відеокамера
Відеокамера
Відеокамера




10

## Перелік публікацій

За темою кваліфікаційної роботи опубліковано дві публікації у Збірнику наукових праць за матеріалами XIV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2022». (Хмельницький – 2022. – С.139-141) та у матеріалах 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2023, Vol. 3373, Khmelnytskyi, 22-24 March 2023. – Khmelnytskyi, 2023. – P. 401–410.) [80]. [81]

- *Доповідь завершено!*
- *Дякую за увагу!*

**ДОДАТОК Б**
(обов'язковий)

**МАТЕРІАЛИ ПУБЛІКАЦІЇ**

Міністерство освіти і науки України
Хмельницький національний університет


ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XIV Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2022»

*18-19 листопада 2022*

Хмельницький 2022

УДК 004.92

Клейн О.М.

*Хмельницький національний університет*

# МЕТОД ТА ЗАСОБИ ВИЯВЛЕННЯ АНОМАЛІЙ В СИСТЕМАХ КОМП'ЮТЕРНОГО ЗОРУ

*Розглянуто проблеми в системах комп'ютерного зору, зокрема неточності при здійсненні аналізу. Для вирішення цієї проблеми пропонуються різні методи, які відрізняються точністю. В роботі пропонується вирішення завдання з використанням виявлення аномалій. Було розроблено метод та засоби для виявлення таких аномалій і застосовано ці результати для оцінювання якості друкованих плат.*

*Problems in computer vision systems are considered, in particular, inaccuracies in the analysis. To solve this problem, various methods are proposed, which differ in accuracy. The paper proposes a solution to the problem using anomaly detection. A method and means of detecting such anomalies were developed and these results were applied to evaluate the quality of printed circuit boards.*

Виявлення аномалій в комп'ютерному зорі є актуальним завданням у багатьох застосунках, що вимагають надійних алгоритмів для виявлення аномалій. Характер вхідних даних до цих алгоритмів відіграє значну роль у вирішенні питання про те, який алгоритм використовувати. Тому, є дві проблеми при виявленні аномалій: виявлення зображень та відео потоків. У межах відео потоків вхідні дані можуть з'являтися у вигляді наборів або точок у навчанні точкових шаблонів, що є дуже складним параметром, коли вони мають форму випадкових множин. Роботи з випадковими множинами, які мають випадкову кількість точок, вдалося уникнути, використовуючи різні підходи, які відображають ці вектори розмірності у фіксовані вектори вимірів. Однак ці підходи нехтують неявною інформацією в своїх остаточних рішеннях. Вхідні дані також можуть відображатися як послідовні візуальні дані, такі як відео, де тимчасова інформація містить інформацію про характер події.

Метою роботи є розробка методу і засобу для виявлення аномалій в комп'ютерному зорі.

Класифікацію методів виявлення аномалій можна здійснити за такими загальними категоріями: методи, що базуються на ймовірності; параметричні методи; непараметричні методи; дистанційні методи; методи базовані на реконструкції; методи базовані на випадкових скінчених множинах тощо.

У зв'язку з цим автоматизований візуальний огляд на основі комп'ютерного зору може значно підвищити продуктивність [1]. Різні методи,

керовані даними, засновані на глибокому навчанні, були розроблені для візуального контролю в різних областях застосування, таких як виробництво [2], будівництво [3], транспорт [4] та обчислювальні системи [5]. Загальним підходом до розробки автоматизованого виявлення дефектів є використання різних алгоритмів обробки зображень. Деякі приклади включають фільтр для перевірки поверхні плитки, бінарний шаблон локального порядку для виявлення дефектів тканини, а також масштабно-інваріантні ключові характеристики для друкованих плат.

Через відсутність доступу до дефектних зразків, неконтрольоване виявлення аномалій є кращим варіантом для виявлення дефектів. При такому підході на етапі навчання використовуються тільки нормальні зразки (без дефектів). Аналогічно, виявлення дефектів на основі RFS використовує лише нормальні зразки під час навчання, щоб максимізувати щільність набору RFS, в якій параметри моделі вивчаються за допомогою або оцінювача максимальної ймовірності, або максимізації очікувань.

Використаємо для вирішення поставленого завдання функції точкового шаблону, які різко контрастують із загальновживаною «глобальною ознакою» для виявлення дефектів. Загальний підхід до роботи з функціями точкового шаблону полягає в перетворенні цих функцій у глобальну функцію за допомогою різних методів відображення, таких як множина візуальних слів. На відміну від цього, моделюватимемо особливості точкового шаблону в рамках RFS. Він був використаний для оцінки кардинальності та щільності цих функцій як складний спосіб побудови статистичної моделі, яка найкраще відповідає нормальним зразкам, максимізуючи ймовірність логу. Основна гіпотеза полягає в тому, що при наявності дефекту змінюється кардинальність і щільність особливостей точкового малюнка. Різні ручні та попередньо навчені функції глибокого точкового малюнка були використані як вимірювання набору функцій, щоб перевірити, яка функція точкового малюнка працює краще. Експеримент над великомасштабним набором даних виявлення дефектів був узгоджений. Експериментальні результати показали, що використання вилучення функцій в рамках RFS для виявлення дефектів має найкращу продуктивність (займає перше місце), завдяки своїй здатності фіксувати сильний відгук по краях. Результати свідчать про те, що при наявності дефекту кількість ребер істотно відрізняється. Основним обмеженням використання є необхідність ручного налаштування крайових і пікових порогів, що може сильно вплинути на продуктивність. Але попередньо навчені методи детектування глибоких точок не дають послідовних кращих результатів. Другим найкращим методом виявлення ознак точкового шаблону був R2D2. В основному це пов'язано з тим, що мережа генерує повторювані та надійні дескриптори функцій точкового шаблону. Крім того, він не показав себе добре порівняно з SIFT, бо це пов'язано з тим, що мережа перетворює вхідне зображення в сірий масштаб.

Отже, розроблений метод та програмний засіб для виявлення аномалій в комп'ютерному зорі дають змогу оцінити дефекти друкованих плат. Подальші дослідження спрямовані на деталізацію точок випадкових скінчених множин.

**Перелік посилань**

1. J.-X. Zhong, N. Li, W. Kong, S. Liu, T. H. Li, and G. Li. Graph Convolutional Label Noise Cleaner: Train a Plug-and-Play Action Classifier for Anomaly Detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pages 1237–1246, 2019a.
2. A. Ziemann, C. X. Ren, and J. Theiler. Multi-sensor anomalous change detection at scale. In Algorithms, Technologies, and Applications for Multispectral and Hyperspectral Imagery XXV, volume 10986, page 1098615. International Society for Optics and Photonics, 2019.
3. B. Zong, Q. Song, M. R. Min, W. Cheng, C. Lumezanu, D. Cho, and H. Chen. Deep autoencoding gaussian mixture model for unsupervised anomaly detection. In International conference on learning representations, 2018.
4. C. Yin, L. Shi, R. Sun, and J. Wang. Improved Collaborative Filtering Recommendation Algorithm based on Differential Privacy Protection. The Journal of Supercomputing, January 2019. ISSN 1573-0484. doi: 10.1007/ s11227-019-02751-7. URL https://doi.org/10.1007/s11227-019-02751-7.
5. X. Yin, Y. Chen, A. Bouferguene, H. Zaman, M. Al-Hussein, and L. Kurach. A deep learning-based framework for an automated defect detection system for sewer pipes. Automation in Construction, 109:102967, 2020.

# Distributed System for Predicting Malicious Activity in Computer Networks

Denys Liubinetskyi[a], Antonina Kashtalian[a], Tomas Sochor[b], Andrii Selskyi[a] and Olexandr Klein[a]

[a] *Khmelnytskyi National University, Institutska str., 11, Khmelnytskyi, 29016, Ukraine*
[b] *Prigo University, Havirov, Czech Republic*

**Abstract**

This article introduce a self-organized that based on deep learning (DL) algorithms. A new self-organized incremental neural network FG-SOINN presented in the Python programming language. This self-organized neural network (SOINN) algorithm generates packets of nodes and edges that are cleaned through fixed, user-defined time intervals. This leads to sudden changes in the network structure. This is due to the fact that large regions of the network are removed with a fixed period before the resumption of the training. Such "oblivion" conflicts with a more gradual oblivion on a large period of time, which is usually observed in natural cognitive systems. In a self-organized incremental algorithm, the removal of nodes and edges is determined by two parameters. These settings should be improved for each existing program through cross-checking. This article proves that FG-SOINN significantly eliminates this shortcoming, considering removal of nodes and edges as a necessary part of the process of study. Three concepts have been developed and implemented to form FG: Time of idle nodes and edges, reliability and utility of a particular node or edges. It is using these concepts that this algorithm and system will remove nodes and fins. The FG technique or node wear technique determines when and after which node of the period it will be removed. But if they are not updated in the specified time, they are simply deleted. These characteristics make it attractive for the dynamics of the environment, which requires long-term training. To ensure system scalability, the network will be guided by the n parameter. The algorithm starts its work and initiates the network with empty sets of nodes.Next, the nodes are added to the weight vectors. After that, the winner vector (nearest node) and the second winner vector will be searched. Distance measurement formulas will be used to determine the distance.
The structure and results of the system demonstrate that this proposition can be adapted to the dynamic profile of network data for both normal and attack classes. The algorithm uses less resources, is faster, and has a higher detection rate than the teaching-teacher method than the traditional SOINN.

**Keywords**

DS, traffic analysis, DL, neural networks, harmful/malicious activity, self-organized system

## 1. Introduction

With the continuous growth of threats and attacks, it is quite a difficult task to accurately and timely detect malicious activity in computer networks. To date, many principles, methods, and systems for detecting network intrusions have been proposed. However, they face critical challenges due to the constant increase in new threats that current systems do not understand. Network activity refers to the interaction of different computers to achieve certain goals.

IntelITSIS'2023: 4th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 22–24, 2023, Khmelnytskyi, Ukraine
EMAIL: kiberplayer@gmail.com (D. Liubinetskyi); yantonina@ukr.net (A. Kashtalian); tomas.sochor@osu.cz; (T. Sochor); andriy.saa@gmail.com (A. Selskyi); oleksanderklein@gmail.com (O. Klein);
ORCID: 0000-0003-1575-4457 (D. Liubinetskyi); 0000-0002-4925-9713 (A. Kashtalian); 0000-0002-1704-1883 (T. Sochor); 0000-0002-7373-0472 (A. Selskyi); 0000-0002-1896-943X (O. Klein)

Internet traffic prediction is very important for tasks such as resource allocation, network planning, and detection of network anomalies caused by attacks [1]. An accurate prediction model can be used to detect security attacks in computer networks by comparing predicted traffic with actual traffic. [2] Additionally, predicting future traffic on a computer network based on current traffic allows the network manager to take action against attacks, congestion, disconnections, or downtime. Similar predictions can be made by modeling network input and output traffic as time series. Currently, there are several studies in this field [3, 4].

Studies of benign activity help establish a baseline [5] or characterize its growth. Unfortunately, it is difficult to understand the extent of these potential threats due to the decentralization of the Internet, so detecting malicious activity in computer networks becomes a rather important task. In addition, due to frequent cyberattacks, one can observe a tendency that they become more and more qualitative and skilled. Failure to prevent or detect such intrusions can have serious consequences for users of such a network. Preventing exposure to malicious activity requires a system that will recognize network connectivity patterns to classify known and unknown intrusions, but also requires periodic retraining to maintain high performance.

## 2. Statement of the problem in a general form and its connection with important scientific or practical tasks

Malicious cyber-attacks are creating serious security challenges that require a new, flexible and more robust intrusion detection system (IDS). An IDS is a proactive intrusion detection tool that is used to automatically detect and classify intrusions, attacks, or violations of security policies. Most of the methods for detecting malicious actions proposed in the literature are rule-based methods (signature matching) and predictive modeling methods (anomaly detection) [6], [7]. Rule-based methods typically use known malicious behavior as a baseline to compare against new behaviors known to indicate security breaches [6]. This is usually achieved by embedding heuristics to search for known patterns (signatures) in the network and/or audit data [8-11]. However, developing malicious activity scenarios that cover all patterns and/or invisible patterns (i.e., zero-day attacks) is quite difficult. This task is complicated by the presence of polymorphism techniques [12]. In addition, attackers may be aware of detection heuristics already in use by the engine and attempt to avoid them. Therefore, there is a need for more reliable methods that can be adapted during operation to prevent malicious activity.

In order to ensure the protection of the system's network, three important problems related to network security must be solved.

1. The first problem is related to the rapid increase in the amount of network data. This growth is due to the use of the Internet of Things (IoT) [13], cloud services and the rapid growth of the network of devices. Improving the methods of data analysis includes increasing the speed and reliability of the analysis process.

2. The second problem is that more accurate tracking and interpretation significantly increases the quality of the findings. NIDS (Network Instruction Detection System) analysis requires more context-specific observations that emphasize more abstract and higher-level observations. All behavior changes should be traceable to a specific user, operating system version, or application specific protocols.

3. The third threat of modern networks is the variety of protocols and massive data transfer in modern networks. In this case, there is an extremely high level of complexity when trying to distinguish between abnormal and normal behavior. This increases the likelihood of unreliable and inconsistent data and increases the potential for exposure to zero-day vulnerabilities.

Intrusion detection systems can be classified based on the used detection mechanism. Detection methodologies are divided into two types: Signature-based and anomaly-based. Signature-based detection uses pre-defined templates associated with known attacks and is distributed as a set of signatures. The following signatures are compared to network traffic patterns to detect potential attacks. Despite its effectiveness against known threats, this method cannot detect or prevent unknown attacks, nor can it maintain or update signatures for known or recently discovered threats.

You can decide that anomaly-based detection sets the baseline/normal level using statistically significant traffic.

Research on improving classification methods for intrusion detection systems has focused on evaluating alternative solutions to fundamental analysis, including neural networks [14], fuzzy logic [9, 15], genetic algorithms [16] and vector support machines [17]. As pointed out by previous studies, SOINN and incremental learning are indeed very effective approaches to the problem of malicious activity detection. The development of intrusion detection systems has shown that hybrid detection methods are more effective due to their ability to distinguish different types of network attacks. If the detection engine determines that the traffic is malicious or part of an attack, the packet may be logged or rejected and only partially forwarded to the intended recipient.

## 3. Statement of the problem

As the amount and size of data increases, learning algorithms are needed to efficiently handle large amounts of signals. Furthermore, a much more challenging task for unsupervised learning is to efficiently and robustly learn data from distributions in which noisy data exist. The main difficulty is that the learning algorithms have no prior knowledge about the distribution of the data as a whole. Thus, when the first few data of a particular distribution are received, the amount of data is insufficient to represent the entire distribution. Currently, learning algorithms cannot determine whether this data is noisy or normal. Therefore, for each iteration, existing methods (such as self-organizing map (SOM) [19], neural gas (NG) [20], etc.) must respond to new data and update the weight vectors of the corresponding neurons, which usually causes a critical deviation of the resulting topology mapping. Another problem is that in most self-organizing "growing-type" neural networks, such as the growing neural gas (GNG) [21], the number of neurons will constantly increase due to the growth of the strategy for identifying them. A large number of neurons increases the computational cost of finding the winning neurons at each iteration, which makes the training procedure inefficient. Therefore, solving such problems requires an algorithm that will avoid these problems, which will greatly improve the efficiency of the self-organized system.

A Self-Organizing and Incremental Neural Network (SOINN) is an unsupervised learning mechanism for unlabeled data. SOINN has already been used in other studies as a clustering method that processes controlled data [22]. SOINN offers unsupervised training for an incremental clustering method with relatively high processing speed at low computational cost. In addition, the complexity and size of the SOINN network is controlled and stabilized through "garbage" or the discovery of unnecessary nodes (neurons).

The technique of the collector or the method of wear of the node, determines when and after which node of the period it will be removed. But if they are not updated at the specified time, they are simply deleted. This property makes it attractive for the dynamics of any environment where continuous learning is required.

The task of the research is to create a distributed self-organized system for predicting malicious activity, namely an intrusion detection system based on artificial intelligence and a module based on the modified SOINN algorithm. Such a module should use a "garbage-forgetting" architecture based on the concepts of downtime, reliability, and utility.

Incremental learning algorithms allow the classifier to improve and expand its capabilities over time (as it processes more data), unlike an autonomous or batch learning algorithm, which provides that the classifier is subject to one group of input data. The dynamics of network data are constantly changing, and using static models will negatively affect detection, as in the case of teacher-trained algorithms.

Implementation of the set task will allow to determine, design and implement the system of prediction of malicious activity by using neural networks and SOINN methods.

## 4. The architecture of the self-organized prediction system

For the correct functioning of the work system aimed at detecting malicious activity, it is necessary to determine its architecture.

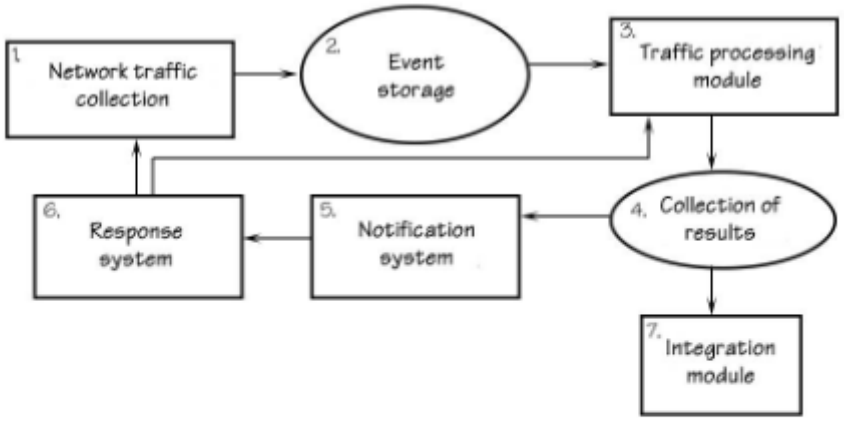



**Figure 1:** Architecture of the IDS system based on FG-SOINN

This system will consist of the following components:

1. Collection of network traffic, which is necessary to use all available information about devices used in the network. In addition, it will perform the function of converting the original network traffic in the required form (for calculating the necessary parameters) and recording data in the event store.

2. Event storage this system defines as a place to save information, which is then analyzed by the system for the presence of malicious traffic and network attacks. Each point of records in the storage will store information about data flows according to the parameters required by the traffic processing module.

3. The traffic processing module is needed as a system working on the FG-SOINN algorithm (forgetting garbage of self-organized incremental neural networks). This module will perform traffic analysis of all flow records that will be stored in the output event database using algorithms that are based on machine learning methods. At the end, for each record, the module determines the type of connection: normal or malicious, as well as the type of attack if it is detected.

4. The results of the data analysis will be recorded in the results database. The location of the results collection is presented as a separate database, which is used to save the anomalies detected.

5. The data should be used by the notification system as well as the compatibility module to extract and further use the analysis results.

6. The response system will act as a "garbage collector". Each record that was determined by the system as malicious will be destroyed, undefined records, that is, such records that are neither normal nor malicious, will be returned to the traffic processing module. This information will then be used for further reprocessing. After that, the system returns to the network traffic collection module, which continues the work cycle.

7. The integration module is an API for the ability to integrate with response systems, an interface for system interaction using http requests.

## 5. The main part

Self-organized incremental neural network (SOINN) is a mechanism of uncontrolled learning (or teaching without a teacher) for unmarked data. Unsupervised training (without a teacher) has two main objectives: clustering and studying of data topology. The purpose of clustering is to divide this dataset into multiple clusters, where each data pair in one cluster is more similar than two different clusters [23]. On the other hand, data topology learning can be described as follows: given a high-dimensional data distribution, it is necessary to project the input data into a topological structure, in which the topological contiguous units of the data in the input space are projected. Recently this

technique is widely used for intellectual analysis of data, vector quantization, image recognition, computer vision and many other related industries [24].

SOINN initiates a network with an empty set of nodes, then adds the first two nodes to the list using vector weights as two input vectors [25]. After the initializations, the neural network finds the winning or nearest node and the same second closest winning node. The distance S1 and S2 from each input to each node is measured by means of the equations (1) and (2). This formula is a general formula for measuring the distance between the layers.

$$s_1 = argmin_{c \in A} dist(x, w_c) \quad (1)$$

$$s_2 = argmin_{c \in A - (s_1)} dist(x, w_c) \quad (2)$$

If the input vector corresponds to the same cluster as the winning nodes, SOINN updates the weight vector of the node and its neighbors with the input weight vector and connects it to the rebromine node. If no matching vector is found in the input vector definition, a new node is added to the network.

The original SOINN is most often used for unsupervised learning. SOINN is used to learn the topological structure of the input data, it is able to grow gradually and take into account input patterns of non-stationary data distribution. It can separate low-density overlapping classes and detect the underlying structure of clusters that are contaminated with noise. It automatically learns the number of nodes and network structure, reports the number of clusters, and provides typical prototypes of each cluster.

Self-organizing incremental neural networks include a family of neural networks, common for which is that they find a topological reflection of incoming data in the network structure by means of competitive training [26].

That understand that SOINN reflects $p$ - measurable input $x = x_1 x_2 \dots x_p$ where $x_i$ $is$ $i^{-M}$ meaning of signs for a separate node in a non-oriented graph. The display corresponds to the point in $p$ - three-dimensional space of sign. Training in SOINN means adaptation of the topology map: Nodes can move, join with other nodes, remain single or be removed, and the edges between nodes can be created or deleted. The node should be considered as a microcluster of incoming cases, which are about one to one. Edges can be considered as consolidated links between associated nodes, such as nodes belonging to one (macro)cluster.

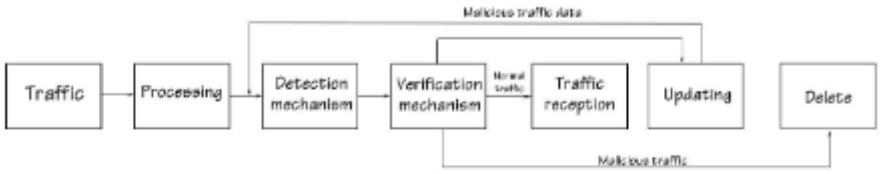



**Figure 2**: System information flows based on FG-SOINN

Figure 2 shows how information flows are processed in the system, where traffic is checked for classification in the system. The system starts with the fact that the incoming traffic collected by the system during the work cycle is fed to the pre-processing module. It is this module that captures and processes incoming traffic in real time. The defined and identified connections are processed to extract and further use the functions. These functions will be the input vector of the detection mechanism - FG-SOINN. The NSL-KDD dataset was performed for the study, and all attribute information is available in [27]. The information is then fed to the malicious activity detection engine, which, after processing, transmits the traffic information to the data validation engine module. The validation module then determines how the system is improved and improved by confirming the expected label. It is at this stage that traffic is divided into harmful and normal traffic. After confirming that the traffic is normal, it is transferred to the user for further work. However, if the system has confirmed that a malicious traffic has been detected, the data validation module will forward forecasts to the update module and remove the traffic from the data set. The system update

module operates in two phases: the active phase and the update phase. In the real-time phase, he makes decisions based on what his capabilities were at the time. In the active phase, the module makes decisions using the data it possesses at the time. In the system update phase, the module updates data with failed predictions that will improve its capabilities in the future. The phases will be executed simultaneously, when necessary, or alternate according to the data of the network traffic.

The basic concept of the proposed algorithm is the gradual creation of the mechanism of network protection. The initial stage of network training uses a relatively small sample containing attributes that are necessary for further correct detection of attacks by the system. Further, after the first cycles of work, the system is re-plenished with definite, undefined and unknown data. Thanks to the last two, the system can be re-learned and improved to improve the security mechanism. To enhance its capabilities, the underlying detection engine must be able to classify network data into multiple classes, not only as to whether it is associated with an attack or not, but also as to the type of attack.

The main part of the system consists of Clustering and Classifier. The clustering block contains a pair of nSOINN [28], which are understood and used by the algorithm classes to compress the data received by the preprocessing module. The classification part takes the output of n-SOINNs, creates the input data for the SVM classifier for each class of the classification pre-run.

In SOINN, node and edge removal is defined by two parameters that must be optimized for each available program using cross-validation or similar resampling approaches. FG-SOINN overcomes this drawback by treating node and edge removal as an integral part of the learning process. Unlike simple SOINN, FG-SOINN has a unique function that tries to bind the nodes that are likely to represent the signal rather than the noise. Binding depends on the reliability of the node.

## 6. Experimental research

The evaluation of the received structure was carried out on NSL-KDD data set [29], which is an improved version of the well-known data set KDD'99. Despite its age, the data set is still a de facto alternative to methods and tools of comparative analysis aimed at providing effective systems of intrusion detection. The training of the system begins with the study of 125,972 traffic instances of the NSL-KDD data set. As can be seen in the figure, the time of initial training and first acquisition of knowledge of the neural network, which will use the FG-SOINN algorithm, is 18 min 57 sec. The number of nodes defined by the network is 819, the number of edges is 2308. With these data, the system will continue to work.

```
Learning time: 18 min 57 sec
Input data processed: 125972
Number of nodes: 819
Number of edges: 2308
```

**Figure 3:** First training phase

Due to the fact that the input data set includes a large sample of data, five binary classes were created four for attacks and one for normal traffic:

- Normal traffic.
- DoS attacks - denial of service attack.
- Probing attack is a starting phase of attack on web resources and web applications. During this attack, the attacker collects information about the structural features of the web application (pages, settings, etc.) and an additional supporting infrastructure (operating system, databases, etc.).
- Remote to user (R2L) — an R2L attack occurs when an attacker tries to send packets to a machine over a network that does not have an account [30].
- User to Root (U2R): The main attack in U2R is a buffer overflow, which copies too much data to a static buffer without checking that the data is written exactly to the program [31, 32].

Several system assessment metrics were used to further compare the results of the study:

- True TPR or Detection Ratio (DR): The ratio between the number of correctly predicted attacks and the total number of attacks, also called Detection Ratio (DR) (3).

$$TPR = TP / (TP + FN) \quad (3)$$

- Level of false positive results (FPR): Ratio between the number of common cases misclassified as attacks and the total number of common cases (4).

$$FPR = FP / (FP + TN) \quad (4)$$

- Negative indicator (FNR): The anomaly could not be identified and classified as normal traffic (5).

$$FNR = FN / (FN + TP) \quad (5)$$

- Positive predictive value (PPV): Probability of intrusion detection if IDS gives alarm (6).

$$PPV = TP / (TP + FP) \quad (6)$$

- Negative predicted value (NPV): Probability of no invasion when IDS does not give alarm (7).

$$NPV = TN / (TN + FN) \quad (7)$$

- The classification coefficient (CR) or accuracy: The percentage of all these correctly predicted cases to all cases, also known as accuracy (8).

$$CR = (TP + TN) / (TP + TN + FP + FN) \quad (8)$$

- Base rate (B): The probability that input data is an attack (9).

$$B = (TP + FN) / (TP + TN + FP + FN) \quad (9)$$

- Intrusion Detection capability (CID): The ratio of common information between input and output and input entropy (10).

$$CID = (H(X) - H(X \mid Y)) / H(X) \quad (10)$$

- Complicated formula for defining the entropy using PPV and NPV (11).

$$h_{x_y} = -b * (1 - fnr) * math.\log(ppv) - b * fnr * math.log(1 - npv) - (1 - b) * (1 - fpr) * math.log(npv) - (1 - b) * fpr * math.log(1 - ppv) \quad (11)$$

The first phase of the update showed the following results (fig. 4). Accuracy 96.44%, detection rate 97.7%, classification as attack 4.65%, error rate 2.3%, possibility of invasion detection 78%. For comparison, also pay attention to the eighth update (fig. 5) and the twelfth update (fig. 6).

```
update_phase(model=s, data=train_1, labels=y_train_1)
```

```
Time for the upgrade phase: 1 min  9 sec
Accuracy (percentage of correctly predicted cases): 96.45%
Detection percentage (TPR): 97.7%
Ability to detect intrusions (CID): 78.31 %
False positive rate (FPR - normally classified as seizures): 4.65%
False negative rate (FNR) - attacks are classified as normal): 2.3%
```

**Figure 4:** First update phase

```
update_phase(model=s, data=train_8, labels=y_train_8)
```

```
Time for the upgrade phase: 1 min 20 sec
Accuracy (percentage of correctly predicted cases): 97.5 %
Detection percentage (TPR): 97.93%
Ability to detect intrusions (CID): 83.23%
False positive rate (FPR - normally classified as seizures): 2.88%
False negative rate (FNR) - attacks are classified as normal): 2.07%
```

**Figure 5:** Eighth update phase

```
update_phase(model=s, data=train_12, labels=y_train_12)

Time for the upgrade phase: 1 min 19 sec
Accuracy (percentage of correctly predicted cases): 98.23%
Detection percentage (TPR): 98.31%
Ability to detect intrusions (CID): 87.15%
False positive rate (FPR - normally classified as seizures): 1.83%
False negative rate (FNR) - attacks are classified as normal): 1.69%
```

**Figure 6:** The Phase of the twelfth update

**Table 1.** Results of testing the results of the implemented system based on FG-SOINN

| № | Time, sec | Accuracy,% | TPR,% | FPR,% | FNR,% | CID,% |
|---|---|---|---|---|---|---|
| 1 | 69 | 96.45 | 97.7 | 4.65 | 2.3 | 78.31 |
| 2 | 72 | 96.73 | 97.4 | 4.6 | 2.26 | 79.02 |
| 3 | 150 | 96.83 | 97.47 | 3.72 | 2.53 | 79.88 |
| 4 | 75 | 97.66 | 98.1 | 2.72 | 2.49 | 84.09 |
| 5 | 80 | 97.67 | 97.55 | 2.23 | 2.45 | 84.1 |
| 6 | 79 | 97.7 | 97.61 | 2.71 | 2.39 | 82.83 |
| 7 | 77 | 97.67 | 97.62 | 1.91 | 2.81 | 83.99 |
| 8 | 80 | 97.5 | 97.93 | 2.88 | 2.07 | 83.23 |
| 9 | 84 | 97.52 | 97.96 | 2.87 | 2.24 | 83.77 |
| 10 | 87 | 97.92 | 98.24 | 2.35 | 1.76 | 85.47 |
| 11 | 80 | 98.06 | 97.65 | 1.57 | 2.15 | 86.19 |
| 12 | 79 | 98.23 | 98.31 | 1.83 | 1.69 | 87.15 |

If compare the data from the first, eighth and twelfth updates, the difference in the improvement of attack detection becomes clear. In the first, unknown threats were 2.3%, while in the twelfth they became 1.69%. The results of all twelve updates are shown in Table 1. According to Table 1, the CID intrusion detection result has been continuously increased during twelve update cycles, and the error level has been constantly changed and the system has achieved the best results for twelve updates.

It should be noted that after the initial training for each round of renewal the subset is checked on the training FG-SOINN, and only soon forecasts return to the system. For visualization the data received after the training were presented on the linear graph, which is shown in Figure 7. The blue color represents the percentage value of the system results, which is learned with the FG-SOINN algorithm, and the red one is SOINN.

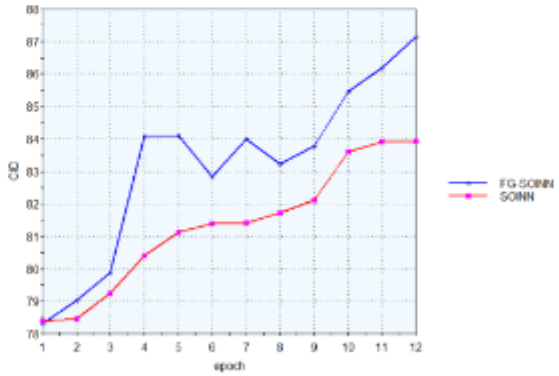



**Figure 7:** Comparison of systems based on algorithms FG-SOINN and SOINN

These indicators show that the accuracy of the FG-SOINN algorithm is greater than SOINN. The quality of intrusion detection by IDS is improved with each new phase, which confirms the efficiency of the proposed algorithm modification.

## 7. Conclusion

The paper proposes a self-organized system for predicting malicious activity based on incremental learning. It is performed with the help of an intrusion detection system that learns with the help of neural networks. The structure of the developed system and its results show that this proposal is confidently adaptable with the nature of the dynamic network data profile. This system uses fewer resources, runs faster and has a higher detection level than teacher training or simple SOINN. Analysis of the proposed FG-SOINN algorithm, which will be used in the distributed intrusion detection system, showed that the efficiency of each subsequent phase of updating and developing the system increases by 1-4%, which gives a good result on huge volumes of data. If we provide this system with many unsuccessful predictions, we not only achieve incremental learning with great and promising accuracy, but also create an effective structure. It will simply not be necessary to add a full set of data to the system. By providing the system with failed predictions, we not only achieve incremental learning with promising accuracy, but also an efficient framework, i.e., instead of feeding it the full dataset. Although system learning time increases with the increase in update input, system update and operating modes can either work concurrently (simultaneously), or update mode can switch when the operational phase is inactive (i.e. no input for detection). In this way, it acquires abilities by learning new input data or failed classifications.

## 8. References


[1] W. Jiang and L. Jiayun Graph neural network for traffic forecasting: A survey. Expert Systems with Applications (2022) 117921.

[2] J. Bao, H. Bechir W. Weng-Keen Iot device type identification using hybrid deep learning approach for increased iot security 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2020.

[3] A.H. Gandomi, C. Fang and A. Laith Machine learning technologies for big data analytics Electronics 11.3 (2022) 421.

[4] S.S. Lin, S. Shui-Long and Z. Annan Real-time analysis and prediction of shield cutterhead torque using optimized gated recurrent unit neural network. Journal of Rock Mechanics and Geotechnical Engineering 14.4 (2022) 1232-1240.

[5] Q. Gong, and G. Chenwei A Baseline modeling algorithm for internet port scanning radiation flows. 2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP). IEEE, 2021.

[6] J. Snehi et al. Global intrusion detection environments and platform for anomaly-based intrusion detection systems //Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020. – Springer Singapore (2021) 817-831.

[7] M. Alsoufi, et al. Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. Applied sciences 11.18 (2021) 8383.

[8] S. Lysenko, O. Savenko, K. Bobrovnikova, A. Kryshchuk, B. Savenko. Information technology for botnets detection based on their behaviour in the corporate area network, Communications in Computer and Information Science 718 (2017) 166–181

[9] O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic, Communications in Computer and Information Science 370 (2013) 243-254

[10] B. Savenko, S. Lysenko, K. Bobrovnikova, O. Savenko, G. Markowsky, Detection DNS Tunneling Botnets, Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, September 22-25.- 2021. pp. 64-69

[11] O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, A. Nicheporuk, A Technique for detection of bots which are using polymorphic code, Communications in Computer and Information Science 431 (2014) 265-276.
[12] O. Pomorova, O. Savenko, S. Lysenko, A. Nicheporuk, Metamorphic Viruses Detection Technique based on the the Modified Emulators. CEUR-WS 1614 (2016) 375-383
[13] Y. Otoum, N.Amiya, As-ids: Anomaly and signature based ids for the internet of things. Journal of Network and Systems Management 29 (2021) 1-26.
[14] MA Khan, HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. Processes 9.5 (2021) 834.
[15] M. Almseidin, A.-S. Jamil and A. Mouhammd Anomaly-based intrusion detection system using fuzzy logic. 2021 International Conference on Information Technology (ICIT). IEEE, 2021.
[16] Z. Halim, et al. An effective genetic algorithm-based feature selection method for intrusion detection systems. Computers & Security 110 (2021) 102448.
[17] M. Mohammadi, et al. A comprehensive survey and taxonomy of the SVM-based intrusion detection systems. Journal of Network and Computer Applications 178 (2021) 102983.
[18] Z. Wang, et al. An efficient network intrusion detection approach based on deep learning. Wireless Networks (2021) 1-14.
[19] X. Qu, et al. A survey on the development of self-organizing maps for unsupervised intrusion detection. Mobile networks and applications 26 (2021) 808-829.
[20] MS Al-Daweri, A. Salwani and AZ Khairul, A homogeneous ensemble based dynamic artificial neural network for solving the intrusion detection problem. International Journal of Critical Infrastructure Protection 34 (2021) 100449.
[21] F. Ardilla, AS Azhar and K. Naoyuki Batch Learning Growing Neural Gas for Sequential Point Cloud Processing. 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, 2022.
[22] M Zhu, et al. Attention-based federated incremental learning for traffic classification in the Internet of Things. Computer Communications 185 (2022) 168-175.
[23] S Comert, et al, Hopfield neural network based on clustering algorithms for solving green vehicle routing problem. International Journal of Industrial Engineering Computations 13.4 (2022) 573-586.
[24] A. Protogerou, et al. A graph neural network method for distributed anomaly detection in IoT. Evolving Systems 12 (2021) 19-36.
[25] RW Ng, et al. An improved self-organizing incremental neural network model for short-term time-series load prediction. Applied Energy 292 (2021) 116912.
[26] J.D Nunes, et al. Spiking neural networks: A survey. IEEE Access 10 (2022) 60738-60764.
[27] F. Masoodi, Machine learning for classification analysis of intrusion detection on NSL-KDD dataset. Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.10 (2021) 2286-2293.
[28] Z. Chiba, et al. A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks. Procedia Computer Science 210 (2022) 94-103.
[29] A. Devarakonda, et al. Network intrusion detection: a comparative study of four classifiers using the NSL-KDD and KDD'99 datasets. Journal of Physics: Conference Series. 2161 1. (2022).
[30] Beulah J. R. et al. Enhancing Detection of R2L Attacks by Multistage Clustering Based Outlier Detection //Wireless Personal Communications. – 2022. – Т. 124. – №. 3. – С. 2637-2659.
[31] A. Sachenko, V. Kochan, V. Turchenko, V. Tymchyshyn and N. Vasylkiv, "Intelligent nodes for distributed sensor network," IMTC/99. Proceedings of the 16th IEEE Instrumentation and Measurement Technology Conference (Cat. No.99CH36309), Venice, Italy, 1999, pp. 1479-1484 vol.3, doi: 10.1109/IMTC.1999.776072
[32] V. Sreerag, et al. Reinforce NIDS Using GAN to Detect U2R and R2L Attacks. Ubiquitous Intelligent Systems: Proceedings of ICUIS 2021. Springer Singapore, 2022.

UNICHECK

Ім'я користувача:
**Кафедра КІ**

ID перевірки:
**1014800628**

Дата перевірки:
**25.04.2023 18:22:34 EEST**

Тип перевірки:
**Doc vs Internet + Library**

Дата звіту:
**25.04.2023 18:25:44 EEST**

ID користувача:
**100005591**

Назва документа: **Клейн_Метод та засоби виявлення аномалій в кіберфізичних системах комп'ютерного зору**

Кількість сторінок: **84** Кількість слів: **20189** Кількість символів: **158826** Розмір файлу: **440.82 KB** ID файлу: **1014504833**

## 3.36% Схожість

Найбільша схожість: **1.62%** з Інтернет-джерелом (https://web.posibnyky.vntu.edu.ua/firen/3zlepko_osnovy_biomedychno

| | | |
|---|---|---|
| 2.56% Джерела з Інтернету | 79 | Сторінка 86 |
| 1.55% Джерела з Бібліотеки | 116 | Сторінка 86 |

## 0% Цитат

| | | |
|---|---|---|
| Цитати | 2 | Сторінка 87 |
| Посилання | 1 | Сторінка 87 |

## 0% Вилучень

Немає вилучених джерел

## Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

| | |
|---|---|
| Замінені символи | 3 |

# Anti-Plagiarism v-15.257

**Максимальне співпадіння з одним документом 2.0%**

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

| ID: 112571<br>Назва: МКР Метод та засоби виявлення аномалій в кіберфізичних системах комп'ютерного зору<br>Додано в БД: 2023-04-25<br>Автора: О.Клейн<br>Керівники: Д.М. Медзатий<br>Консультанти:<br>Опоненти: | Документ | | Сумарний збіг по Базі Даних | |
|---|---|---|---|---|
| | Символи | Лексеми | Символи | Лексеми |
| | 143953 | 1173 | 3323 (2%) | 28 (2%) |

Джерело плагіату

| ID | Опис | Наявність плагіату в документі | |
|---|---|---|---|
| | | Символи | Лексеми |

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Олександр КЛЕЙН

Тема: Метод та засоби виявлення аномалій в кіберфізичних системах комп'ютерного зору

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг дипломної роботи:

Кількість сторінок записки 104 с.

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано систему профілювання вразливостей при керуванні розумним будинком

2. Висновок про відповідність роботи дипломному завданню
Дипломна робота відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз методів обробки зображень та систем комп'ютерного зору. Досліджено відомі рішення та засоби в цій сфері. У другому розділі розроблено концепцію методу виявлення аномалій на зображеннях кіберфізичними системами комп'ютерного зору. У третьому розділі запропоновано виявлення аномалій за допомогою даних зображення. У четвертому розділі запропоновано виявлення аномалій у відеозображеннях. У Висновках підведено підсумки виконаної роботи.

4. Позитивні сторони роботи: Запропонована метод виявлення аномалій на зображеннях кіберфізичними системами комп'ютерного зору.

5. Негативні сторони роботи: немає.

6. Оцінка графічного оформлення та пояснювальної записки роботи: _–_

7. Відгук про роботу в цілому: Робота виконана на належному рівні.

8. Інші зауваження: _–_

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої дипломної роботи вважаю, що робота заслуговує оцінки «відмінно» 4,75 (B)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Мартинюк Валерій Володимирович, д.т.н., професор, завідувач кафедри АКІТР ХНУ

"24" 04 2023р.

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Клейна Олександра Миколайовича
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-21-1

ЗАЯВА

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

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

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

22 квітня 2023 року

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Метод та засоби виявлення аномалій в кіберфізичних системах комп'ютерного зору

Автор: Клейн Олександр Миколайович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: к.т.н., доцент Медзатий Д.М.

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки усі запозичення фрагментарні, або мають належним чином оформленні посилання;

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 2% і адресується до першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Д.М. Медзатий

Гарант ОП _____ О. С. Савенко

Завідувач кафедри КІСч _____ Т. О. Говорущенко