Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження методів виявлення аномалій за допомогою відеоаналітики на основі штучного інтелекту у комплексних системах безпеки
(тема)

Виконала:
студентка 2 курсу, групи АМСЗІм-21-2
Семеренська В.В.
(прізвище, ініціали)

Спеціальність групи 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Пшеничних С.В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека .
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Семеренській Вікторії Владиславівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів виявлення аномалій за допомогою відеоаналітики на основі штучного інтелекту у комплексних системах безпеки
затверджена наказом по університету від «23» березня 2023р. №292 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 15.05.2023р.
3. Вихідні дані до роботи: відомі контрольовані та неконтрольовані алгоритми машинного навчання, набір даних з камер відеоспостереження
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз сучасних систем відеоспостереження та методів обробки відеоінформації.
2) Огляд алгоритмів машинного навчання для виявлення аномальної поведінки об'єктів за допомогою камер з інтелектуальною аналітикою.
3) Порівняльний аналіз алгоритмів машинного навчання за своєю ефективністю щодо виявлення аномальної поведінки людини.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: демонстраційний матеріал у вигляді ppt-презентації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Пшеничних Сергій Васильович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2023	Виконано
2	Збір матеріалів для дослідження	30.02.2023	Виконано
3	Розробка 1 розділу	01.03.2023	Виконано
4	Розробка 2 розділу	05.03.2023	Виконано
5	Розробка 3 розділу	15.03.2023	Виконано
6	Розробка 4 розділу	30.03.2023	Виконано
7	Розробка 5 розділу	10.04.2023	Виконано
8	Розробка 6 розділу	20.04.2023	Виконано
9	Оформлення кваліфікаційної роботи	30.04.2023	Виконано

Дата видачі завдання 15 лютого 2023 року

Студентка _____ Семеренська В.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Пшеничних С.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 66 с., 8 рис., 1 додаток, 26 джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ, ВИЯВЛЕННЯ АНОМАЛІЙ, ВІДЕОАНАЛІТИКА, ШТУЧНИЙ ІНТЕЛЕКТ, МАШИННЕ НАВЧАННЯ.

Об’єкт дослідження – процес удосконалення комплексних систем безпеки шляхом використанням відеоаналітики на основі штучного інтелекту.

Предмет дослідження – методи виявлення аномалій в системах відеоспостереження на основі штучного інтелекту.

Мета роботи – аналіз сучасних методів виявлення аномалій в системах відеоспостереження, виявлення їх переваг та недоліків.

Методи досліджень – теоретичний аналіз, формалізація та порівняння.

Дана робота містить огляд алгоритмів машинного навчання для виявлення аномальної поведінки об'єктів за допомогою камер з інтелектуальною аналітикою у сучасних системах відеоспостереження а також порівняльний аналіз ефективності алгоритмів у виявленні аномальної поведінки людини.

У сучасному світі безпека стала одним з головних пріоритетів, а системи відеоспостереження відіграють важливу роль у забезпеченні безпеки різних об’єктів.

Останнім часом відеоаналітика на основі штучного інтелекту набуває все більшої популярності та стає ключовим інструментом для виявлення аномалій у комплексних системах безпеки. В даному дослідженні ми зосередимося на аналізі сучасних систем відеоспостереження та методів обробки відеоінформації, а також на огляді методів детектування аномалій. Вивчення цих методів допоможе розробити нові та ефективні підходи для виявлення аномалій у реальному часі та підвищення ефективності комплексних систем безпеки [1].

ABSTRACT

The report contains: 66 p., 8 fig., 1 application, 26 sources.

INFORMATION SECURITY, VIDEO SURVEILLANCE SYSTEMS, ANOMALY DETECTION, VIDEO ANALYTICS, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING.

The object of the research – integrated security systems using video analytics based on artificial intelligence.

The subject of research – methods of detecting anomalies in video surveillance systems based on artificial intelligence.

The purpose of the work is to analyze modern methods of detecting anomalies in video surveillance systems, to identify their advantages and disadvantages.

Research methods – theoretical analysis, formalization, and comparison.

This paper provides an overview of machine learning algorithms for detecting anomalous behavior of objects using cameras with intelligent analytics in modern video surveillance systems, as well as a comparative analysis of the effectiveness of algorithms in detecting anomalous human behavior.

In the modern world, security has become one of the top priorities, and video surveillance systems play an important role in ensuring the safety of various facilities.

Recently, AI-based video analytics has become increasingly popular and is becoming a key tool for detecting anomalies in complex security systems. In this study, we will focus on analyzing modern video surveillance systems and video information processing methods, as well as reviewing anomaly detection methods. The study of these methods will help to develop new and effective approaches to detect anomalies in real time and improve the efficiency of complex security systems [1].

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

AI – artificial intelligence
BMS – bayesian model selection
CAE – convolutional autoencoder
CBR – case-based reasoning
CCTV – closed-circuit television
CNN – convolutional neural network
C_LOF – cluster-based local outlier factor
CUSUM – cumulative sum control chart
DNN – deep neural network
DSN – deep stacking network
DT – decision tree
EER – equal error rate
FCN – fully convolutional network
FPR – false positive rate
FPS – frames per second
GAN – generative adversarial networks
HTM – hierarchical temporal memory
IoT – internet of things
kNN – k-nearest neighbors
KPI-TSAD – key performance indicator time series anomaly detection
LSAD – least squares anomaly detection
LSTM – long short-term memory
ML – machine learning
RNN – recurrent neural network
ROC-AUC – receiver operating characteristic-area under the curve
SVM – support vector machine
TPR – true positive rate
VAE – variational autoencoder

ВСТУП

Оскільки світ стає все більш взаємопов'язаним завдяки поширенню пристроїв з доступом до Інтернету, кількість даних, що генеруються і передаються, зростає в геометричній прогресії. Однією зі сфер, де це зростання особливо помітне, є камери спостереження, які зараз повсюдно встановлені в громадських місцях, комерційних будівлях і приватних будинках. Однак зі збільшенням обсягу даних зростає ризик порушень безпеки та атак.

Однією з ключових проблем у забезпеченні безпеки даних з камер спостереження є виявлення аномальної поведінки. Аномалії можуть приймати різні форми, від спроб несанкціонованого доступу до підозрілих моделей руху в полі зору камери. Своєчасне і ефективне виявлення і реагування на ці аномалії має вирішальне значення для підтримки цілісності системи відеоспостереження і захисту людей і майна, що знаходяться під її наглядом.

Виявлення аномалій у даних камер спостереження є складним завданням через велику кількість даних, що генеруються, високу мінливість вмісту сцени та освітлення, а також потенційну можливість хибних спрацьовувань. Тому існує потреба в ефективній системі, яка може точно і ефективно виявляти аномалії в даних камер спостереження і попереджати персонал служби безпеки в режимі реального часу.

Мета цієї магістерської роботи – дослідити використання методів машинного навчання для виявлення аномалій у даних камер спостереження. Зокрема, робота буде зосереджена на пошуку, імплементації та тестуванні моделей, які можуть точно ідентифікувати аномальну поведінку людини, з акцентом на мінімізацію помилкових спрацьовувань та оптимізацію обчислювальної ефективності.

Актуальність розглянутої теми полягає в постійному рості потреби у захисті об’єктів, людей та інфраструктури від різноманітних загроз. Розвиток технологій штучного інтелекту та відеоаналітики відкриває нові можливості для вдосконалення комплексних систем безпеки, роблячи їх більш автоматизованими та ефективними. Отже, дослідження методів виявлення аномалій за допомогою відеоаналітики на основі штучного інтелекту є важливим та актуальним напрямком у сфері безпеки.

1 АНАЛІЗ СУЧАСНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ТА МЕТОДІВ ОБРОБКИ ВІДЕОІНФОРМАЦІЇ

1.1 Завдання, що вирішуються системами відеоспостереження в комплексних системах безпеки

Системи відеоспостереження є невід'ємною частиною сучасних комплексних систем безпеки. Вони використовуються для моніторингу різних об'єктів та територій з метою забезпечення безпеки людей, майна, інфраструктури та інформаційних ресурсів. В рамках комплексних систем безпеки, системи відеоспостереження вирішують ряд ключових завдань.

1) Детектування і реєстрація подій. Відеоспостереження дозволяє виявляти та записувати різні події на об'єктах спостереження, такі як входи та виходи людей, рух транспортних засобів, акти вандалізму чи крадіжки.

2) Проактивне виявлення потенційних загроз. Системи відеоспостереження можуть аналізувати відеопотік в реальному часі та виявляти аномальну поведінку, що може свідчити про можливу загрозу або злочин, дозволяючи операторам вжити заходів до ескалації ситуації.

3) Фіксація доказів. Відеозаписи можуть служити важливими доказами у судових справах або розслідуваннях, допомагаючи встановити хід подій та визначити винних сторін.

4) Аналіз та оптимізація. Зібрані відеодані можуть бути використані для аналізу різних аспектів роботи об'єкта, таких як рух людей або транспорту, продуктивність працівників, стан об'єктів та інфраструктури. Це дозволяє виявляти можливі проблеми та працювати над їх оптимізацією.

5) Моніторинг дотримання правил та норм. Відеоспостереження дозволяє контролювати дотримання встановлених правил та норм на об'єктах спостереження. Це може включати перевірку дотримання відстаней між людьми у громадських місцях, дотримання правил дорожнього руху, стандартів праці або вимог до екологічної безпеки.

6) Розпізнавання осіб та об'єктів. Завдяки технологіям штучного інтелекту, системи відеоспостереження можуть розпізнавати осіб, транспортні засоби, номерні знаки, а також різні об'єкти та атрибути. Це може сприяти ефективному контролю доступу на об'єкти, автоматичному розподілу транспорту або виявленню заборонених предметів.

7) Інтеграція з іншими системами безпеки. Відеоспостереження може бути інтегровано з іншими компонентами комплексної системи безпеки, такими як системи контролю доступу, пожежної безпеки, антитерористичних заходів та ін. Це дозволяє створити єдину, централізовану систему контролю та реагування на різні події та загрози.

8) Віддалений моніторинг та контроль. Системи відеоспостереження дозволяють проводити віддалений моніторинг об'єктів та територій через Інтернет або мережі передачі даних. Це забезпечує зручний контроль та оперативне реагування на події з будь-якого місця та в будь-який час [1].

В контексті об'єктів інформаційної діяльності, організацій та установ, де циркулює інформація з обмеженим доступом, системи відеоспостереження виконують додаткові завдання, спрямовані на забезпечення конфіденційності даних та виявлення інсайдерів.

Системи відеоспостереження можуть автоматично визначати осіб, які мають право доступу до певних зон, та контролювати їхній рух, щоб запобігти несанкціонованому доступу до інформації.

Також застосування алгоритмів машинного навчання дозволяє системам відеоспостереження виявляти аномальну поведінку співробітників та інших осіб, які можуть мати намір отримати доступ до конфіденційної інформації або завдати шкоди організації. Відеоаналітика може виявляти підозрілі дії, такі як незвичайний рух співробітника або залишання на робочому місці після закінчення робочого дня, і сповіщати відповідних співробітників про можливі загрози [2].

Інтеграція алгоритмів машинного навчання та відеоаналітики може значно покращити системи відеоспостереження в комплексних системах безпеки. Вони дозволяють автоматично виявляти події, такі як входи та виходи людей, рух транспортних засобів та аномальні дії, зменшуючи залежність від людського оператора і забезпечуючи точніше та оперативніше реагування [3].

Застосування алгоритмів машинного навчання для аналізу відеопотоку дозволяє виявляти аномальну поведінку та потенційні загрози, навіть якщо вони відрізняються від типових сценаріїв, завдяки адаптивності та здатності до самонавчання та дозволяє системам відеоспостереження розпізнавати осіб, транспортні засоби, номерні знаки та інші об'єкти з високою точністю та швидкістю.

Машинне навчання може допомогти у виявленні закономірностей та тенденцій у відеоданих, що може сприяти оптимізації роботи об'єктів, зменшенню проблем з безпекою та покращенню ефективності ресурсів. Алгоритми також можуть допомогти у координації відеоспостереження з іншими компонентами комплексної системи безпеки, такими як системи контролю доступу, пожежної безпеки, антитерористичних заходів та ін. Це дозволяє створити єдину, централізовану систему контролю та реагування на різні події та загрози.

1.2 Огляд сучасних систем відеоспостереження

Сучасні системи відеоспостереження можуть бути розділені на дві основні категорії: традиційні системи, які в основному залежать від людського оператора для моніторингу та аналізу відеоінформації, та інтелектуальні системи, які використовують алгоритми машинного навчання для автоматичної обробки відеоданих та виявлення подій [1].

Традиційні системи відеоспостереження, такі як аналогові камери з закритим телевізійним контуром, мають деякі обмеження, такі як низька якість зображення, відсутність автоматичної обробки даних та залежність від людського оператора. Це може призвести до помилок у виявленні подій, повільного реагування на інциденти та високих витрат на підтримання систем.

Інтелектуальні системи відеоспостереження, засновані на алгоритмах машинного навчання, можуть допомогти у вирішенні деяких з цих проблем. Застосування алгоритмів машинного навчання дозволяє автоматично виявляти та розпізнавати об'єкти на відео, аналізувати їх поведінку та виявляти незвичайні події. Застосування технологій відеоаналітики, таких як виявлення руху, виявлення обличчя та розпізнавання ліцензійних номерів, може допомогти в розслідуванні злочинів та інцидентів [4].

Однак, у систем відеоспостереження, заснованих на алгоритмах машинного навчання, є свої виклики та обмеження. Наприклад, нестача якісних та кількісних даних для тренування моделей, складність налаштування та відладки алгоритмів машинного навчання, відсутність здатності пояснювати прийняті рішення та інші [2].

Отже, аналіз сучасних систем відеоспостереження та методів обробки відеоінформації показує, що інтеграція алгоритмів машинного навчання та відеоаналітики може значно покращити якість та ефективність систем відеоспостереження в комплексних системах безпеки. Проте, необхідно вирішити деякі технічні та технологічні виклики, щоб забезпечити підвищення рівня безпеки та ефективності застосування цих систем.

2 ОГЛЯД АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ КАМЕР З ІНТЕЛЕКТУАЛЬНОЮ АНАЛІТИКОЮ

Метою цього огляду є пошук, оцінка, синтез даних та їх аналіз серед існуючих досліджень, пов'язаних з темою магістерської роботи, для того, щоб оцінити та узагальнити дані в рамках дослідницьких питань.

У цьому огляді буде проаналізовано літературу в галузі виявлення аномалій за допомогою машинного навчання, зокрема, роботи, які розглядають, оцінюють і порівнюють різні методи і техніки машинного навчання. Саме аналіз таких робіт може дати відповідь на дослідницькі питання.

2.1 Вибір бази даних

Для пошуку літератури були використані наступні бази даних:

- IEEE Xplore;
- Semantic Scholar;
- Scopus;
- arXiv;
- Google Scholar.

Розглянуті бази даних були обрані через великий архів наукових праць у відкритому доступі, а також можливість пошуку за ключовими словами та пошуку з використанням штучного інтелекту, що дозволило звузити результати пошуку до праць, які максимально відповідають тематиці дослідження.

2.2 Критерії включення та виключення

У цьому розділі представлено критерії, які були обрані для фільтрації літератури та відбору найбільш пов'язаних статей.

Критерії включення:

– стаття опублікована в рецензованих журналах або матеріалах конференцій;

– дослідження має відношення до питань дослідження та теми огляду;

– дослідження містить кількісні або якісні дані, що мають відношення до теми огляду;

– стаття написана англійською мовою;

– повний текст статті доступний;

– дослідження опубліковане не раніше 2015 року.

Критерії виключення:

– стаття опублікована в нерецензованих джерелах;

– дослідження не має відношення до питань дослідження або теми огляду;

– дослідження не містить кількісних або якісних даних, що мають відношення до теми огляду;

– робота написана не англійською мовою;

– дослідження, які не доступні в повному тексті;

– дослідження, які були опубліковані до 2015 року.

2.3 Стратегія пошуку

Щоб сформулювати успішну стратегію пошуку, необхідно визначити основні поняття, що стосуються теми дослідження. Такими поняттями були визначені наступні:

– виявлення аномалій;

– камери спостереження;

– методи машинного навчання;

– набори даних.

Далі було розроблено список ключових слів для кожного поняття, які можна комбінувати за допомогою булевих операторів (AND, OR, NOT) для формування пошукових рядків.

Знайдені статті, в свою чергу, були відфільтровані відповідно до критеріїв включення та виключення після короткого перегляду назви, опису та змісту статті на основі критеріїв включення та виключення.

Дані, вилучені з відібраних статей після синтезу та аналізу, розміщені у відповідних таблицях результатів і описані в розділі результатів.

2.4 Оцінка якості

Для оцінки якості літератури було створено таблицю з критеріями відбору. Таблиця 2.1 являє собою перелік запитань до кожної статті для оцінки її якості, вона наведена нижче. Відповідь на кожне запитання оцінюється, а потім бали для кожної статті підсумовуються, і стає можливим ранжувати статті відповідно до їх якості для включення в дослідження.

Таблиця 2.1 – Питання якості

№	Питання якості	Релевантно (1 б.)	Частково релевантно (0,5 б.)	Не релевантно (0 б.)
1	2	3	4	5
1	Чи чітко визначені цілі статті?			
2	Чи містить стаття огляд методів машинного навчання?			
3	Чи містить стаття порівняльний аналіз методів машинного навчання?			
4	Чи містить стаття порівняльний аналіз наборів даних?			
5	Чи були набори даних, використані в дослідженнях, репрезентативними для реальних сценаріїв епіднагляду?			

Продовження таблиці 2.1.

1	2	3	4	5
6	Чи проводилися дослідження з використанням загальнодоступних чи запатентованих наборів даних?			
7	Чи використовуються в статті метрики оцінювання методів машинного навчання?			
8	Чи застосовуються розглянуті в статті методи до аномалій поведінки людини?			
9	Чи визначає стаття сильні сторони та обмеження алгоритмів машинного навчання?			
10	Чи чітко сформульовані результати та висновки?			

2.5 Вилучення даних

Цей розділ присвячений вилученню даних, важливому компоненту систематичного огляду літератури. Він передбачає збір і систематизацію відповідних даних з першоджерел. У цьому розділі прагнеться відповісти на дослідницькі питання, пов'язані з використанням алгоритмів машинного навчання для виявлення аномалій у даних камер спостереження. Для цього було проведено пошук в академічних базах даних, в результаті якого було відібрано 20 першоджерел для вилучення даних. Ці джерела включають наукові статті, інформаційні бюлетені та огляди, в яких обговорюються різні аспекти виявлення аномалій у даних камер спостереження. У цьому розділі представлено отримані дані у вигляді таблиці 2.2, класифіковані за такими ключовими критеріями, як методологія дослідження, характеристики наборів даних та ефективність алгоритмів виявлення аномалій.

Таблиця 2.2 – Вилучення даних зі статей

ID Статті	Назва статті	Алгоритми ML	Набори даних	Метрики оцінювання
1	2	3	4	5
5	Deep learning-based methods for anomaly detection in video surveillance: a review	CNN, RNN, LSTM, GAN, Автокодери, 3D ConvNet MIL, SVM, DNN	UCSD, UMN, Subway, CUHK, UCF-crime, Avenue, ShanghaiTech, Ped1, Ped2	ROC-AUC, F1-score, Precision, Recall, Frame-Level Accuracy, RMSE
6	Real-world Anomaly Detection in Surveillance Videos	MIL	UCF-crime, UMN, UCSD Ped 1, Ped 2, CUHK avenue, Subway, BOSS, UCF Crowd	ROC-AUC, EER
7	Taxonomy of Anomaly Detection Techniques in Crowd Scenes	CNN, RNN, LSTM	UCF-crime, PASCAL, VOC, UCSD, UMN, UCD, LV	EER, DR
8	A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data	C_LOF, AutoCloud, TEDA Clustering, KPI-TSAD, HTM, SVM	UCSD, Ped 1, Ped 2, and CUHK Avenue	ACU, EER, TP, TN, FP, FN, AUC

Продовження таблиці 2.2.

1	2	3	4	5
9	Anomaly Detection In Surveillance System Using Machine Learning Techniques- A Review	BMS, HTM, LSAD, LSTM, DNN, CNN, CAD, CUSUM, FCN, SVM	N/A	N/A
10	ANOMALY DETECTION IN SURVEILLANCE VIDEO	LSTM	Subway	N/A
11	Robust anomaly detection in urban environments using sensor and information fusion...	Information fusion, Bayesian Network	Custom dataset	False Alarm Rate, Detection Rate, Time-to-Alarm
12	Multimedia Datasets for Anomaly Detection: A Review	N/A	UCSD, UMN, CUHK, Subway, PETS2009, i-LIDS, VIRAT, UCF-Crime, Abnormal Crowd, ShanghaiTech, Avenue, MEVA, GANet, LSTM-VID-CRIME	N/A

Продовження таблиці 2.2.

1	2	3	4	5
13	Systematic literature review of machine learning based software development effort estimation models	CBR, RNN, and DT	N/A	N/A
14	Unnatural Human Motion Detection using Weakly Supervised Deep Neural Network	DNN	Custom dataset	Accuracy, Precision, Recall, F1-score
16	An overview of deep learning-based methods for unsupervised and semi-supervised...	VAE, GANs, LSTM, CAE	UCSD, UMN, Subway, CUHK, LV	ROC-AUC, AUC-PR.
17	Deep learning for anomaly detection: A survey	Supervised, Unsupervised, Hybrid Models, CNN	N/A	N/A
18	Deep learning-based Anomaly Detection on Surveillance Videos: Recent Advances	Deep learning based methods	UCF-101, UCF-Crime, ActivityNet,	ROC-AUC
20	Abnormal event detection using local sparse representation	Custom model	UCSD, Subway Entrance datasets	ROC-AUC, EER
21	Abnormal event detection in videos using generative adversarial nets	Generative Adversarial Networks (GAN)	UCSD, UMN	ROC-AUC, EER

Продовження таблиці 2.2.

1	2	3	4	5
22	Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes	Fully Convolutional Neural Network (FCN), CNN	UCSD, Subway Dataset	ROC-AUC, EER
23	Quo vadis, action recognition? A new model and the kinetics dataset	Two-Stream Inflated 3D ConvNet (I3D), LSTM, SVM	UCF-101, HMDB-51, ImageNet, PASCAL VOC	Top-1 and Top-5 Accuracy
24	Future frame prediction for anomaly detection—A new baseline	Generative Adversarial Networks (GAN), Convolutional LSTM, CNN	UCSD Pedestrian, CUHK Avenue	ROC-AUC,
25	Learning regularity in skeleton trajectories for anomaly detection in videos	Convolutional Автоенкодери, CNN, RNN	ShanghaiTech	ROC-AUC
26	Deep reinforcement learning for unsupervised video summarization with diversity-representativeness reward	DSN, LSTM	SumMe, TVSum	F1-score, Diversity Score

2.6 Результати систематичного огляду літератури

2.6.1 Алгоритми машинного навчання для виявлення аномалій.

Щоб визначити найбільш ефективні алгоритми ML для цього завдання, було проведено систематичний огляд літератури. У цьому розділі представлено результати систематичного огляду літератури, висвітлюючи найбільш використовувані алгоритми ML для виявлення аномальної поведінки даних, наведені у таблиці 2.3.

Таблиця 2.3 – Алгоритми машинного навчання для виявлення аномалій

Алгоритм ML	Посилання
CNN (Convolutional Neural Network)	[5], [7], [9], [10], [18], [20], [21], [23], [24], [25],[26]
LSTM (Long Short-Term Memory)	[5], [16], [7], [9], [10], [23], [24],[26]
SVM (Support Vector Machine)	[5], [8], [9], [23]
MIL (Multiple-Instance Learning)	[5], [6]
GAN (Generative Adversarial Network)	[5], [16], [21], [24]
HTM (Hierarchical Temporal Memory)	[8], [9]
RNN (Recurrent Neural Network)	[5], [7], [9], [13],[25]
Автоенкодери	[5], [16], [25]

Ці алгоритми були застосовані до різних типів наборів даних і показали ефективні та багатообіцяючі результати у виявленні аномалій у поведінці людей, таких як ненормальні дії, поведінка натовпу та аномальні події. Однак на продуктивність цих алгоритмів може впливати кілька факторів, зокрема якість і розмір набору даних, тип виявленої аномалії та вибрані гіперпараметри. Тому важливо ретельно вибирати та попередньо обробляти набори даних і налаштовувати гіперпараметри для кожного алгоритму, щоб досягти оптимальної продуктивності у виявленні аномалій у поведінці людини.

2.6.2 Характеристики наборів даних.

У цьому розділі представлені результати аналізу даних для дослідницького питання, яке має на меті охарактеризувати набори даних, що використовуються в дослідженнях виявлення аномалій на основі аналізу даних камер спостереження. Процес вилучення даних включав перегляд обраних статей та запис інформації про використані набори даних, включаючи їхній розмір, джерело, формат і маркування. Результати цього процесу, що представлені у таблиці 2.4, дають уявлення про типи набори даних, що використовуються у сфері виявлення аномалій у даних з камер спостереження.

Таблиця 2.4 – Характеристики наборів даних

Набір даних	Тривалість	Кадри	Роздільна здатність	Аномалії	Посилання
UCF-crime	128 годин	~13.8M	320×240	13	[5], [6], [7] [8], [12], [18]
UCSD Ped 1	5 хвилин	14,000	238×158	40	[5], [6], [7] [8], [12], [18], [20], [21], [22], [23], [24], [25]
UCSD Ped 2	5 хвилин	4,560	360×240	12	[5], [6], [7] [8], [12], [18], [20], [21], [22], [23], [24], [25]
Subway entrance	1,5 годин	144,249	512×384	66	[5], [6], [8], [12], [20]
Subway exit	43 хвилин	64,900	512×384	19	[5], [6], [8], [12], [20]
UMN	5 хвилин	~7,700	320×240	11	[5], [6], [7], [12], [21]
CUHK avenue	30 хвилин	35,240	640×360	14	[5], [6], [8], [12],[24]
Shanghai tech	N/A	317,398	856×480	130	[5], [12], [25]
LV	3,93 годин	N/A	декілька	N/A	[7], [12]
UCF Crowd	11 хвилин	~16,320	декілька	N/A	[5], [12]

Усі набори даних, що були розглянуті в цьому розділі, мають мітки для машинного навчання, і багато з них містять немічені відео для тестування алгоритмів на додаток до відеоданих, тому вибір найбільш підходящого набору даних базується на наступних факторах.

Набори даних, що містять відеозаписи поведінки людей у різних умовах, наприклад, відео з камер спостереження, найкраще підходять для навчання алгоритмів машинного навчання для виявлення аномалій у поведінці людей. Ці набори даних повинні містити достатньо аномалій, щоб алгоритм міг точно виявляти рідкісні події, і в той же час мати достатньо велику кількість нормальної поведінки, щоб забезпечити повне розуміння очікуваних дій. Крім того, набори даних, які є різноманітними з точки зору умов освітлення, кутів нахилу камери та типів аномалій,

допоможуть забезпечити здатність алгоритму узагальнювати реальні сценарії. Набір даних, який відповідає цим критеріям – це UCF-Crime.

2.6.3 Метрики оцінювання.

Метрики оцінки відіграють життєво важливу роль в оцінці ефективності будь-якого методу, що використовується для виявлення аномалій у поведінці людини. У цьому розділі будуть обговорені метрики оцінки, які використовувалися в дослідженнях, розглянутих у цьому систематичному огляді літератури, які можна побачити у таблиці 3.5. Вибір відповідних метрик оцінки має вирішальне значення для забезпечення високих показників виявлення та низького рівня хибнопозитивних результатів запропонованих методів.

Таблиця 3.5 – Метрики оцінювання

Метрики оцінювання	Посилання
ROC-AUC (Receiver Operating Characteristic curve and Area Under the ROC Curve)	[5], [6], [16], [18], [20], [21], [22], [24], [25]
EER (Equal Error Rate)	[5], [6], [7], [8], [20], [21], [22]
F1-оцінка	[5], [14], [26]
Accuracy	[14], [23]
Precision	[5], [14]
Recall	[5], [14]

Метрики оцінки, що використовувалися для оцінки ефективності методів виявлення аномалій, розглянутих у цьому огляді, ґрунтувалися на схожому підході в усіх дослідженнях. У дослідженнях використовувалася комбінація ROC-AUC і EER, які, в свою чергу, базуються на значеннях TPR (True Positive Rate) і FPR (False Positive Rate). Ці показники дають уявлення про те, наскільки добре методи працюють з точки зору правильної ідентифікації аномалій при мінімізації помилкових спрацьовувань.

2.6.4 Переваги та обмеження алгоритмів машинного навчання.

У цьому розділі будуть представлені результати дослідження, метою якого було дослідити сильні та слабкі сторони різних алгоритмів машинного навчання, що використовуються для виявлення аномалій у даних відеоспостереження, які продемонстровано у таблиці 2.6. З літературних джерел було виявилено різноманітний набір алгоритмів, починаючи від традиційних методів машинного навчання, таких як машини опорних векторів SVM, і закінчуючи новітніми підходами до глибокого навчання, такими як згорткові нейронні мережі CNN і мережі з довгою короткочасною пам'яттю LSTM. Вивчаючи сильні та слабкі сторони цих алгоритмів, було надано цінну інформацію для дослідників і практиків, які прагнуть вибрати найбільш підходящі методи для своїх конкретних завдань виявлення аномалій в системах відеоспостереження.

Таблиця 2.6 – Переваги та обмеження алгоритмів машинного навчання

ML Алгоритм	Переваги	Обмеження	Посилання
1	2	3	4
CNN (Convolutional Neural Network)	Чудовий аналіз зображень і відео, виділення локальних ознак, просторових зв'язків, стійкість до шуму та інваріантність перекладу	Велика кількість параметрів, висока обчислювальна вартість, обмежена інтерпретованість	[5], [7], [9], [10], [18], [20], [21], [23], [24], [25],[26]
LSTM (Long Short-Term Memory)	Ефективно фіксує довгострокові залежності, обробляє послідовності змінної довжини, стійкий до проблеми зникаючого/вибухаючого градієнта	Обчислювальна складність, час навчання, обмежена інтерпретованість	[5], [16], [7], [9], [10], [23], [24],[26]
SVM (Support Vector Machine)	Хороші показники узагальнення, стійкість до шуму, здатність обробляти дані високої розмірності	Чутливий до вибору ядра та параметрів, проблеми з масштабуванням, не ідеальний для великих наборів даних	[5], [8], [9], [23]
MIL (Multiple-Instance Learning)	Працює зі слабко маркованими даними, добре навчається на позитивних і негативних пакетах, добре адаптується до незбалансованих наборів даних	Залежить від якості представлення пакетів, чутливий до шуму та викидів	[5], [6]

Продовження таблиці 2.6.

1	2	3	4
GAN (Generative Adversarial Network)	Потужні генеративні моделі, здатні генерувати реалістичні зразки, неконтрольоване навчання	Збій режиму, нестабільність під час тренувань, складність у вимірюванні продуктивності, обмежена інтерпретованість	[5], [16], [21], [24]
HTM (Hierarchical Temporal Memory)	Добре запам'ятовує послідовності, часові патерни та прогнозування, стійкий до шуму	Обмеженість досліджень і застосувань у виявленні аномалій, висока вартість обчислень	[8], [9]
RNN (Recurrent Neural Network)	Добре моделює часові послідовності, обробляє послідовності змінної довжини	Труднощі з фіксацією довгострокових залежностей, проблема зникаючого/вибухового градієнта, високі обчислювальні витрати, обмежена інтерпретованість	[5], [7], [9], [13],[25]
Автоенкодери	Добре вивчає латентні репрезентації, зменшення розмірності, неконтрольоване навчання	Труднощі у визначенні відповідного розміру латентного простору, обмежена інтерпретованість, може не охоплювати всі релевантні ознаки в даних	[5], [16], [25]

Наступні алгоритми ML були обрані як найбільш придатні для порівняння їх ефективності в подальших дослідженнях в контексті виявлення аномалій в поведінці людини.

Контрольовані алгоритми ML розглянуто нижче.

1) CNN (Convolutional Neural Network) – як показано в [3], [15] та [19], CNN широко використовуються для задач виявлення аномалій на основі відео завдяки своїй здатності фіксувати просторові відносини та витягувати локальні особливості із зображень та відеоданих.

2) LSTM (Long Short-Term Memory) – LSTM часто використовуються в задачах відеоаналізу через їхню здатність фіксувати довгострокові залежності в часових даних, як зазначено в [2], [13] і [23]. Це особливо корисно при аналізі відео з камер спостереження для виявлення аномалій.

3) SVM (Support Vector Machine) – SVM, як зазначено в [2] і [5], є популярними моделями керованого навчання, які можна використовувати для виявлення аномалій шляхом максимізації різниці між різними класами в просторі ознак. SVM застосовуються в різних додатках, включаючи виявлення аномалій у відеоспостереженні, за допомогою функцій ядра для обробки нелінійно розділених даних.

4) RNN (Recurrent Neural Network) – RNN, як обговорювалося в [6] і [22], є класом нейронних мереж, які спеціально розроблені для обробки послідовних даних, що робить їх придатними для завдань відеоаналізу. Вони можуть вловлювати часові залежності в даних і були використані в різних додатках для виявлення аномалій у відеоспостереженні.

Ці алгоритми були обрані на основі їхньої поширеності в літературі та придатності для обробки відеоданих, зокрема для набору даних UCF-crime.

3 АНАЛІЗ ТА РЕАЛІЗАЦІЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

У цьому дослідженні були використані методи керованого машинного навчання для розробки моделей, які навчаються на основі маркованих даних з камер спостереження. Для полегшення навчання моделі дані анотуються нормальною та аномальною поведінкою людини. Алгоритми керованого навчання потребують навчального набору даних, який складається з пар вхід-вихід, де вхід – це дані з камер спостереження, а вихід – мітка, що вказує на те, чи є поведінка нормальною чи аномальною. Це дозволяє моделі вивчати взаємозв'язок між вхідними даними і цільовими мітками, що в кінцевому підсумку дозволяє передбачати аномальну поведінку в даних, які не переглядаються [5].

Основна увага в цьому розділі приділена опису деталей реалізації, налаштувань параметрів і архітектури моделі для кожного з цих алгоритмів, що забезпечує їхню придатність для виконання поставлених завдань. Реалізуючи ці алгоритми керованого машинного навчання, буде проаналізована їхня продуктивність і порівняна їхня ефективність у виявленні аномальної людської поведінки, що в кінцевому підсумку дасть відповідь на дослідницькі питання, окреслені раніше в дослідженні.

Реалізація цих алгоритмів здійснюється за допомогою мови програмування Python в середовищі Jupyter Notebook. Jupyter Notebook забезпечує інтерактивний та організований підхід до реалізації та тестування алгоритмів. В процесі реалізації використовується декілька бібліотек та фреймворків, зокрема TensorFlow, Keras та scikit-learn. Ці бібліотеки пропонують багатий набір інструментів та функціональних можливостей, які дозволяють ефективно та зручно реалізовувати обрані алгоритми машинного навчання.

3.1 Попередня обробка даних

У цьому підрозділі описано процес відбору відповідних наборів даних для дослідження та підготовки даних для подальшого аналізу. У цьому дослідженні було обрано загальнодоступний набір даних UCF-crime, який містить відеозаписи різних аномальних і нормальних форм людської поведінки. База даних UCF-Crime – це

масштабний набір даних із 128 годин відеозаписів. Він складається з 1900 довгих і не обрізаних відеозаписів реального спостереження з 13 реалістичними аномаліями, включаючи насильство, арешт, підпал, напад, дорожньо-транспортну пригоду, крадіжку, вибух, бійку, пограбування, стрілянину, крадіжку в магазині та вандалізм. Ці аномалії відібрані тому, що вони мають значний вплив на громадську безпеку [6].

Набір даних розділений на папки з аномальними (наприклад, Abuse, Arrest, Arson тощо) та нормальними (наприклад, Testing_Normal_Videos_Anomaly, Training-Normal-Videos тощо) відеозаписами.

Етапи попередньої обробки включають завантаження набору даних і вилучення фіксованої кількості кадрів (у цьому випадку 5) з кожного відео. Потім ці кадри попередньо обробляються шляхом перетворення їх у відтінки сірого та зміни розміру до фіксованої форми (64x64 пікселів). Результуючий набір даних складається зі списку відеокадрів (X) і відповідних міток, де 1 позначає нормальну поведінку, а 0 – аномальну.

Після завантаження та попередньої обробки набір даних розбивається на навчальний та тестовий набори у співвідношенні 80/20, де 80% даних використовується для навчання, а решта 20% – для тестування. Набір даних додатково обробляється, щоб зробити його придатним для різних алгоритмів машинного навчання. Для моделей CNN, LSTM та RNN значення пікселів кадрів нормалізуються шляхом ділення їх на 255, перетворюючи значення в діапазон [0, 1]. Для SVM-моделі кадри перетворюються в одновимірний формат і масштабуються за допомогою StandardScaler, щоб забезпечити однаковий масштаб ознак.

За допомогою цих кроків попередньої обробки набір даних перетворюється у формат, придатний для навчання та тестування обраних алгоритмів машинного навчання у формальному експерименті.

3.2 Згорткові нейронні мережі

CNN – це клас моделей глибокого навчання, призначених для обробки сіткоподібних даних, таких як зображення або відео. CNN особливо підходять для цього дослідження завдяки їхній здатності автоматично вивчати просторові ієрархії

ознак на основі вхідних даних. Основними структурними елементами CNN є згорнуті шари, об'єднані шари та повністю з'єднані шари.

Методологія використання CNN у цьому дослідженні включає кроки, що описані нижче [5].

3.2.1 Архітектура алгоритму.

Фреймворк CNN складається з двох основних компонентів. По-перше, механізм згортки ідентифікує та розрізняє різні особливості зображення для аналізу за допомогою процедури, відомої як вилучення особливостей. Цей процес включає в себе безліч комбінацій згортки або об'єднання шарів. По-друге, щільно з'єднаний шар приймає результати етапу згортки і прогнозує категорію зображення на основі попередньо вилучених ознак [7].

Метою підходу до вилучення ознак на основі CNN є зменшення кількості ознак у наборі даних при одночасній генерації нових, узагальнених ознак з оригінальної колекції. Схему архітектури CNN зображено на рисунку 3.1, який ілюструє різні рівні, що здіяні в цьому процесі.

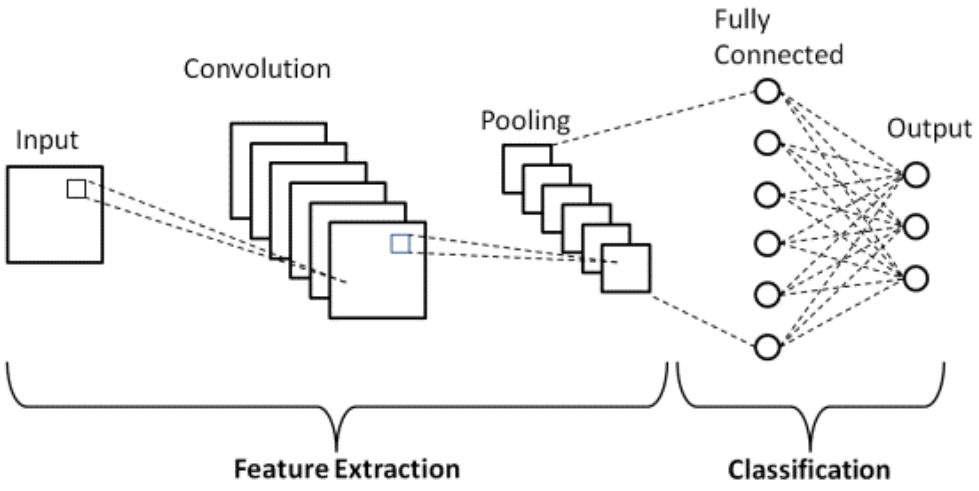

Рисунок 3.1 – Рівні архітектури згорткових нейронних мереж

У розробленій реалізації алгоритму, яка представлена в додатку А, функція визначає архітектуру CNN з використанням послідовної моделі Keras' Sequential.

1) Згорткові шари додаються до моделі за допомогою класу Conv2D. У скрипті послідовно додаються три шари Conv2D з 32, 64 і 128 фільтрами, відповідно, і розміром ядра 3x3, за якими слідують функції активації ReLU.

2) Шари об'єднання додаються за допомогою класу MaxPooling2D. Існує три шари MaxPooling2D, кожен з яких слідує за шаром Conv2D з розміром пулу 2x2.

3) Повністю з'єднані шари реалізовані за допомогою класу Dense. Спочатку карти об'єктів сплющуються за допомогою шару Flatten, а потім додається повністю зв'язаний шар зі 128 вузлами. Крім того, є вихідний шар Dense з одним вузлом для бінарної класифікації.

4) Шар, що відсівається, додається за допомогою класу Dropout з коефіцієнтом відсівання 0.5 для зменшення перенавчання.

5) Функції активації вказуються як аргументи в шарах Conv2D і Dense. У скрипті функції активації ReLU використовуються у згортковому та повністю зв'язаному шарах.

6) Для вихідного шару використовується сигмоїдна функція активації, оскільки вона підходить для бінарної класифікації.

3.2.2 Тренування моделі.

CNN навчається на попередньо обробленому та доповненому наборі даних з відповідною функцією втрат та алгоритмом оптимізації. Під час навчання гіперпараметри, такі як швидкість навчання та розмір партії, налаштовуються для досягнення оптимальної продуктивності.

Модель компілюється за допомогою оптимізатора Adam зі швидкістю навчання 0,001, двійковою перехресною втратою ентропії та точністю як метрикою оцінювання. Вхідні дані змінюються шляхом додавання додаткового виміру, щоб відповідати необхідній формі вхідних даних моделі CNN. Потім модель навчається протягом 20 епох з розміром партії 32 і 20%-им валідаційним розбиттям.

Після навчання модель оцінюється на тестовому наборі даних і генеруються прогнози. Нарешті, обчислюється площа під ROC-кривою AUC і коефіцієнт однакових помилок EER та будуються графіки для візуалізації роботи моделі.

Ця реалізація забезпечує базову модель CNN для виявлення аномалій у даних камер спостереження.

3.3 Мережі з довготривалою та короткочасною пам'яттю

LSTM – це тип архітектури рекурентних нейронних мереж RNN, що спеціально розроблені для обробки довготривалих залежностей у послідовних даних. LSTM-мережі підходять для аналізу даних з камер спостереження, оскільки вони можуть фіксувати часові патерни та залежності у відеопослідовності, які є важливими для виявлення аномальної поведінки людини [7].

3.3.1 Архітектура алгоритму.

LSTM працює як з довготривалою пам'яттю LTM (Long Term Memory), так і з короткотривалою пам'яттю STM (Short Term Memory), використовуючи концепцію вентилів для спрощення і прискорення обчислень, як показано на рисунку 3.2.

1) Ворота забуття (Forget Gate) – отримує LTM і відкидає несуттєву інформацію.

2) Ворота вивчення (Learn Gate) – поточний вхід (подія) і STM об'єднуються, що дозволяє застосувати останні знання з STM до поточного входу.

3) Ворота запам'ятовування (Remember Gate) – об'єднує збережену інформацію LTM з STM і подією для створення оновленого LTM.

4) Використання воріт (Use Gate) – LTM, STM і подія використовуються цими воротами для прогнозування результатів поточної події, в результаті чого створюється оновлена STM.

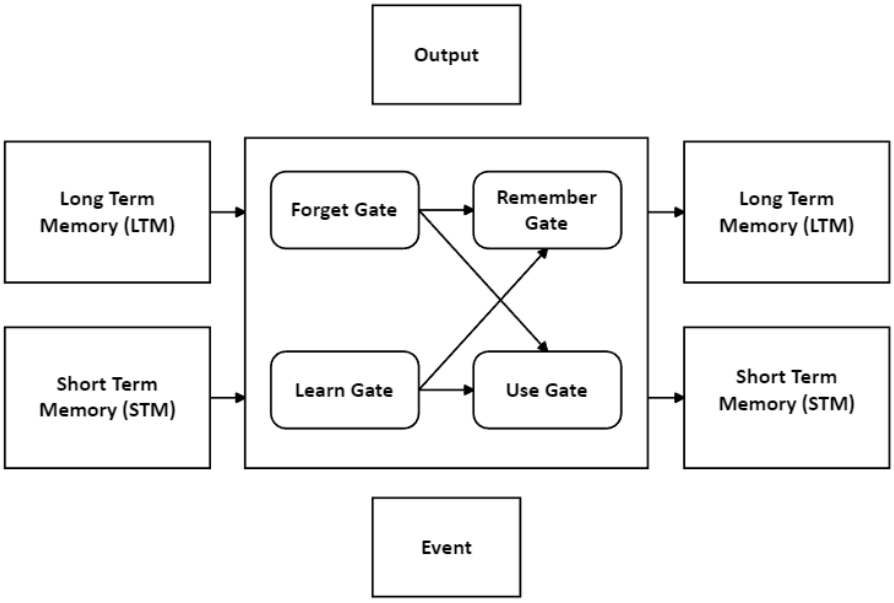

Рисунок 3.2 – Структура архітектури мереж з довготривалою та короткочасною пам'яттю

Для реалізації алгоритму, який представлено в додатку А, розробляється відповідна LSTM архітектура, що складається з одного або декількох LSTM-шарів, за якими слідують повністю з'єднані шари. Вихідний шар використовує відповідну функцію активації (наприклад, сигмоїд для бінарної класифікації), щоб передбачити, чи є поведінка вхідної послідовності нормальною чи аномальною.

Створена реалізація визначає LSTM-модель з двома LSTM-шарами, шарами відсіву та щільним вихідним шаром для бінарної класифікації. LSTM шари в Keras автоматично включають всі необхідні вентилі (forget, learn, remember і use gate) як частину своєї внутрішньої архітектури.

LSTM модель побудована за допомогою Sequential API від TensorFlow. Архітектура складається з наступних шарів.

1) Шар LSTM з 128 прихованими одиницями, форма входу, яка вказує на те, що цей шар повинен виводити послідовність прихованих станів для обробки наступним шаром.

2) Шар відсіву з коефіцієнтом відсіву 0,5 для запобігання перенавчання.

3) LSTM-шар з 64 прихованими одиницями, що означає, що цей шар виводитиме лише кінцевий прихований стан.

4) Ще один шар Dropout з коефіцієнтом відсіву 0,5.

5) Щільний шар з одним вихідним елементом і сигмоїдною функцією активації, що використовується для бінарної класифікації.

3.3.2 Тренування моделі.

LSTM навчається за допомогою попередньо обробленого та виокремленого набору даних з відповідною функцією втрат та алгоритмом оптимізації. Як і у випадку з підходом CNN, гіперпараметри, такі як швидкість навчання та розмір партії даних, налаштовуються для досягнення оптимальної продуктивності.

Модель компілюється за допомогою оптимізатора Adam зі швидкістю навчання 0,001, втратами binary_crossentropy та точністю як метрикою. Потім модель навчається протягом 20 епох з розміром партії 32 і валідаційним розбиттям 0.2. Параметр verbose встановлено в 1, що означає, що прогрес навчання буде виведено у консоль.

Після навчання модель оцінюється на тестовому наборі для отримання прогнозованих оцінок. На завершення обчислюється площа під ROC-кривою AUC та середньоквадратична помилка EER.

3.4 Машина опорних векторів

SVM – це потужний метод машинного навчання, відомий своєю ефективністю у вирішенні проблем класифікації. Він спрямований на пошук оптимальної гіперплощини, яка максимізує відстань між різними класами в просторі ознак, тим самим забезпечуючи надійну границю рішення. Реалізація алгоритму SVM передбачає визначення функції ядра, налаштування гіперпараметрів та тонке налаштування моделі для досягнення найкращої продуктивності. У контексті дослідження SVM-модель буде використовуватися для класифікації відеоданих на нормальну та аномальну поведінку, використовуючи попередньо оброблені ознаки, отримані з наборів даних камер спостереження [8].

3.4.1 Архітектура алгоритму.

Архітектура SVM складається з декількох компонентів, як показано на рисунку 3.3.

1) Вхідні дані. Вхідні дані для SVM включають попередньо оброблені ознаки, витягнуті з наборів даних. Кожна точка даних на вході представлена у вигляді вектора ознак у багатовимірному просторі ознак.

2) Функція ядра. Функція ядра відіграє вирішальну роль в архітектурі SVM. Це математична функція, яка відображає точки вхідних даних у простір вищої розмірності, що полегшує пошук розділяючої гіперплощини, навіть якщо дані не піддаються лінійному розділенню у вихідному просторі. Деякі поширені функції ядра включають лінійну, поліноміальну, радіально-базисну функцію RBF та сигмоїдну.

3) Опорні вектори. Вектори підтримки – це точки даних, які лежать найближче до межі рішення або гіперплощини. Вони сприяють визначенню положення оптимальної гіперплощини і є критично важливими для визначення межі між різними класами.

4) Маржа. Маржа – це відстань між розділювальною гіперплощиною та найближчими точками даних з кожного класу (опорними векторами). SVM намагається максимізувати цю відстань, щоб створити надійну границю рішення, яка допомагає мінімізувати помилку класифікації.

5) Кордон рішення або гіперплощина. Межа рішення або гіперплощина - це підпростір (лінія, площина або гіперплощина, залежно від розмірності вхідних даних), який розділяє точки даних на різні класи. Оптимальна гіперплощина - це та, яка найкраще розділяє класи, максимізуючи при цьому маржу.

6) Регуляризація. Регуляризація – це метод, який використовується в SVM для контролю компромісу між максимізацією маржі та мінімізацією помилки класифікації. Вона допомагає запобігти надмірному пристосуванню, вводячи штрафний член в задачу оптимізації. Параметр регуляризації, який часто позначають як «C», визначає баланс між максимізацією маржі та мінімізацією помилки класифікації [9].

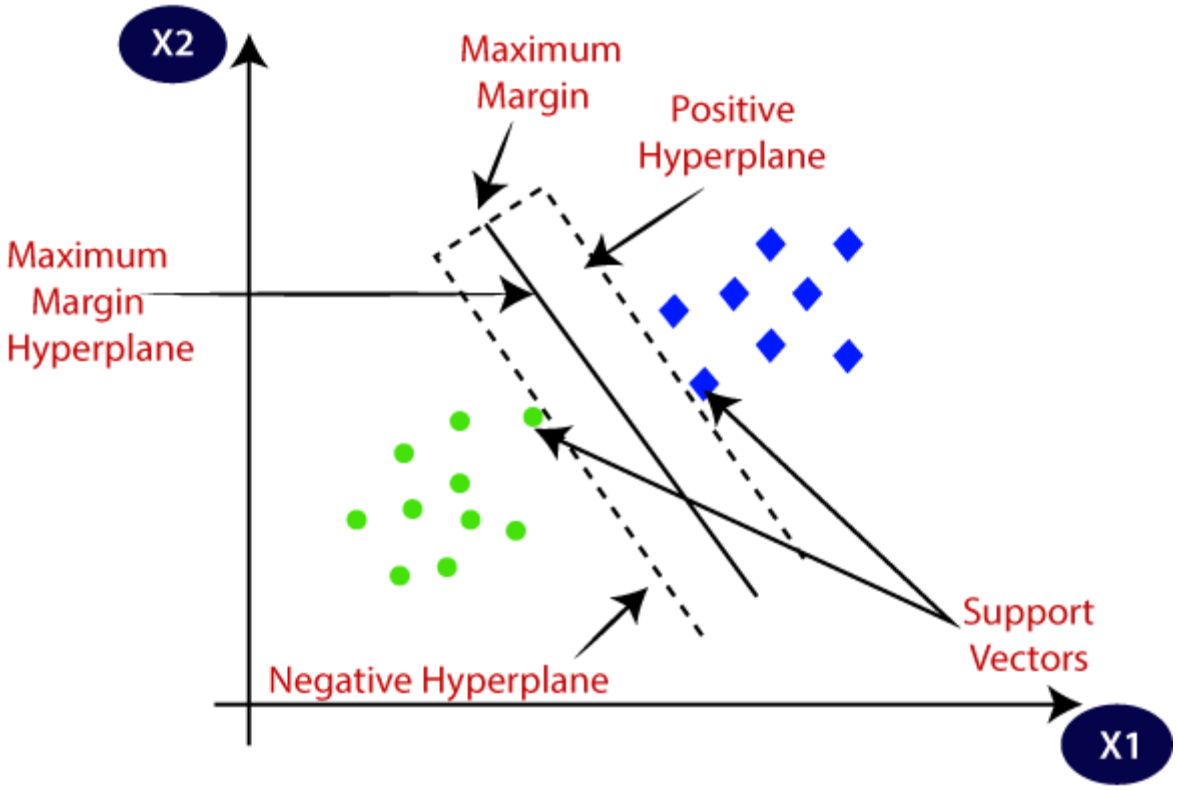

Рисунок 3.3 – Структура архітектури машини опорних векторів

У реалізації алгоритму, яка представлена в додатку А, SVM-модель визначається за допомогою класу «SVC» з модуля «sklearn.svm». Конструктор отримує наступні параметри.

1) Функція ядра має значення «linear», що вказує на використання лінійного ядра для SVM-моделі. Лінійні ядра підходять для даних високої розмірності або коли дані лінійно розділяються. Вони спрощують модель і зменшують обчислювальні витрати порівняно з іншими функціями ядра, такими як радіально-базисна функція (RBF) або поліном.

2) Параметр «probability» встановлено на «True», щоб увімкнути оцінки ймовірностей для SVM моделі. Це дозволяє моделі виводити ймовірнісні оцінки для кожного класу замість просто прогнозованих міток класів.

3) Параметр «C» встановлено на 1, що є значенням за замовчуванням. Цей параметр контролює компроміс між досягненням низької помилки навчання та низької помилки тестування. Менше значення C створює ширший запас, що може призвести до деяких помилкових класифікацій у навчальних даних, але може краще узагальнювати тестові дані. Більше значення C створює вужчу межу, що має на меті

мінімізувати помилкові класифікації в навчальних даних, але може призвести до надмірного припасування.

4) Параметр «random_state» має значення 42, що забезпечує відтворюваність результатів за допомогою генератора випадкових чисел, який використовується в моделі SVM.

3.4.2 Тренування моделі.

Процес навчання SVM моделі включає наступні кроки.

1) Масштабування даних. Навчальні та тестові дані стандартизуються за допомогою класу «StandardScaler» з модуля «sklearn.preprocessing». Масштабувальник накладається на навчальні дані, а потім використовується для перетворення як навчальних, так і тестових даних. Цей крок є важливим, оскільки SVM-моделі чутливі до масштабу вхідних ознак, а стандартизація даних гарантує, що всі ознаки мають однаковий масштаб.

2) Навчіть SVM-модель. SVM-модель навчається на масштабованих навчальних даних (X_train_scaled) та відповідних мітках (y_train) за допомогою методу «fit» класу «SVC».

3) Прогнозування за допомогою SVM-моделі. Після навчання SVM-моделі робиться прогноз на масштабованих даних тестування (X_test_scaled) за допомогою методу «predict» класу «SVC». Додатково використовується метод «predict_proba» для отримання ймовірнісних оцінок для класу позитивних відповідей.

3.4 Рекурентна нейронна мережа

RNN – це тип архітектури нейронної мережі, спеціально розроблений для обробки послідовних даних. Вона складається з взаємопов'язаних шарів нейронів, кожен з яких має прихований стан, здатний фіксувати інформацію з попередніх часових кроків. Основним структурним елементом RNN є рекурентний нейрон, який зберігає свій прихований стан на всіх часових кроках під час обробки вхідної послідовності [7].

3.4.1 Архітектура алгоритму.

У рекурентній нейронній мережі RNN кожен вхідний елемент пов'язаний між собою. Спочатку RNN обробляє перший вхід, X(0), і генерує вихід, h(0). Згодом h(0) і X(1) об'єднуються як вхідні дані для наступного кроку. Таким же чином, h(1) і X(2) використовуються як вхідні дані для наступного кроку, і так далі. Такий підхід гарантує, що RNN зберігає контекстну інформацію протягом усього процесу навчання, як показано на рисунку 3.4.

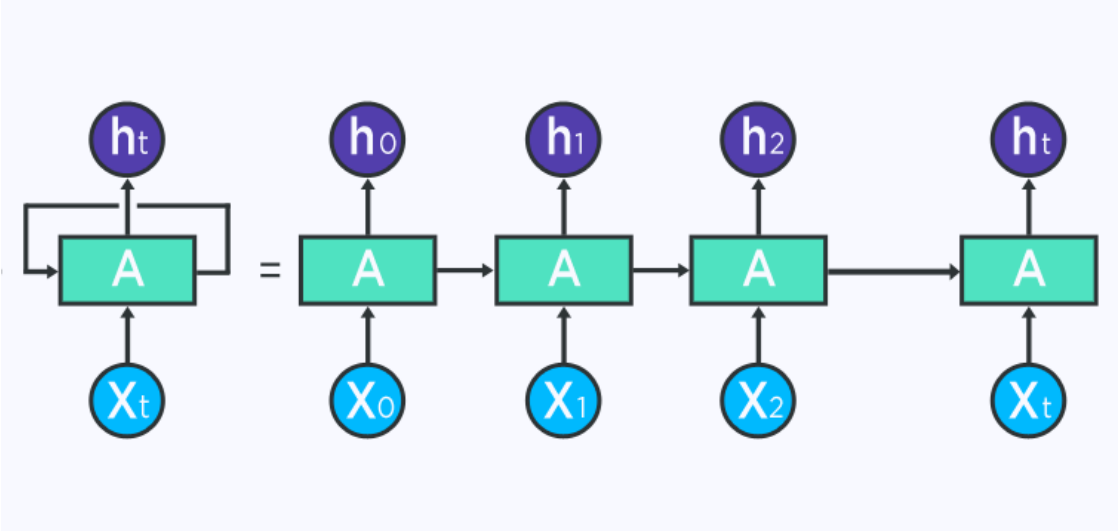

Рисунок 3.3 – Структура архітектури рекурентної нейронної мережі

У реалізації, яка представлена в додатку А, RNN-модель побудована з використанням шарів довготривалої короткочасної пам'яті LSTM, які є різновидом RNN-шару, що може обробляти довготривалі залежності в послідовностях. Архітектура моделі RNN виглядає наступним чином:

1) Перший LSTM шар. Перший LSTM-шар складається з 64 одиниць і має параметр return_sequences, встановлений у True. Це дозволяє шару виводити послідовності, а не лише кінцевий прихований стан, що робить можливим підключення цього шару до іншого LSTM-шару. Параметр input_shape задає форму вхідних даних, яка в даному випадку дорівнює (5, 64 * 64), де 5 – кількість відібраних кадрів, а 64 * 64 - розмір сплющеного кадру.

2) Другий шар LSTM. Другий LSTM-шар має 128 одиниць і також має параметр return_sequences, встановлений у True. Цей шар отримує вихідні послідовності від

першого LSTM-шару і виробляє іншу послідовність, яка може бути передана наступному LSTM-шару.

3) Третій рівень LSTM. Третій рівень LSTM має 256 одиниць, але параметр return_sequences не встановлений, тобто за замовчуванням він дорівнює False. Цей шар отримує вихідну послідовність від другого LSTM-шару і виводить лише кінцевий прихований стан. Це дозволяє моделі зосередитися на найбільш релевантній інформації для задачі класифікації.

4) Шар з відсівом. Після третього шару LSTM додається шар відсіву з коефіцієнтом відсіву 0,5. Цей шар випадковим чином встановлює частину вхідних одиниць в 0 під час навчання, що допомагає запобігти надмірному пристосуванню, змушуючи модель вивчати більш надійні ознаки.

5) Вихідний шар. До моделі додається щільний вихідний шар з одним нейроном і сигмоїдною функцією активації. Сигмоїдна функція активації відображає вхідні дані у значення від 0 до 1, забезпечуючи ймовірнісний вихід для бінарної класифікації.

3.4.2 Тренування моделі.

Функція train_rnn_model приймає попередньо оброблені навчальні дані (X_train), відповідні мітки (y_train) та форму вхідних даних як вхідні аргументи. Всередині функції створюється RNN-модель за допомогою функції create_rnn_model, а потім компілюється за допомогою наступних компонентів: оптимізатора Адама та функції бінарних перехресних ентропійних втрат.

Після компіляції модель навчається на змінених навчальних даних для 20 епох з розміром партії 32 і валідаційним розбиттям 20%. Валідаційний розбиття використовується для того, щоб затримати частину навчальних даних для моніторингу роботи моделі на невидимих даних під час навчання, що допомагає виявити надмірне пристосування і відповідно скоригувати модель. Функція повертає навчену RNN-модель та історію її навчання, яку можна використовувати для подальшого аналізу або оптимізації.

4 МЕТРИКИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ АНОМАЛІЙ АЛГОРИТМАМИ МАШИННОГО НАВЧАННЯ

ROC-AUC (Receiver Operating Characteristic – Area Under the Curve) і EER (Equal Error Rate) – це метрики оцінки, які часто використовуються в задачах бінарної класифікації, таких як виявлення аномалій. Вони можуть допомогти оцінити ефективність алгоритмів машинного навчання у виявленні аномальної поведінки людини.

4.1 Робоча характеристика приймача – площа під кривою

ROC-крива – це графік співвідношення частоти правильних спрацьовувань TPR і частоти помилкових спрацьовувань FPR при різних порогових рівнях класифікації. AUC – це площа під ROC-кривою, яка надає єдине скалярне значення для узагальнення продуктивності класифікатора [5].

Частота правильних спрацьовувань TPR або чутливість може бути описана формулою (4.1).

$$\mathrm{TPR} = \mathrm{TP}/\ (\mathrm{TP}+\ \mathrm{FN}) \tag{4.1}$$

Частота хибнопозитивних спрацьовувань FPR або 1 - специфічність може бути описана формулою (4.2).

$$\mathrm{FPR} = \mathrm{FP}/\ (\mathrm{FP}+\ \mathrm{TN}) \tag{4.2}$$

Де TP (True Positives) – аномальні події, правильно ідентифіковані як аномалії, FN (False Negatives) – аномальні події, помилково ідентифіковані як нормальні, FP (False Positives) – нормальні події, помилково ідентифіковані як аномалії, TN (True Negatives) – нормальні події, правильно ідентифіковані як нормальні.

ROC-AUC є ефективною метрикою для порівняння продуктивності різних алгоритмів ML, оскільки вона враховує компроміс між TPR і FPR на різних порогових

рівнях, надаючи єдине значення для для оцінки загальної продуктивності. Вище значення ROC-AUC вказує на кращу ефективність класифікації.

4.2 Рівна частота помилок

EER – це точка на ROC-кривій, де частота хибнопозитивних спрацьовувань FPR дорівнює частоті хибнонегативних спрацьовувань FNR. Іншими словами, це точка, в якій кількість хибнопозитивних і хибнонегативних результатів дорівнює. EER можна використовувати для визначення оптимального порогу класифікації, який збалансовує компроміс між хибнопозитивними та хибнонегативними результатами [5].

Для розрахунку AUC можна використовувати різні методи чисельного інтегрування, такі як правило трапецій, яке оцінює площу під ROC-кривою шляхом обчислення суми площ трапецій, утворених кривою і віссю x. EER – це значення FPR (або FNR), коли FPR = FNR.

EER корисний для порівняння алгоритмів ML, оскільки він надає єдине скалярне значення, яке представляє оптимальний компроміс між хибнопозитивними та хибнонегативними результатами [20]. Нижчий EER вказує на кращу ефективність класифікації. Порівнюючи значення EER протестованих алгоритмів можна визначити, який алгоритм має кращий баланс між помилковими спрацьовуваннями і помилковими негативами, що робить його більш ефективним у виявленні аномальної поведінки людини.

5 РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ ТА ОЦІНКА РЕАЛІЗОВАНИХ АЛГОРИТМІВ

У цьому розділі представлено комплексну оцінку впроваджених алгоритмів машинного навчання, а саме згорткових нейронних мереж CNN, мереж з довгою та короткою пам'яттю LSTM, машин опорних векторів SVM та рекурентних нейронних мереж RNN, для виявлення аномалій у даних з камер спостереження. Основна мета експерименту – визначити ефективність цих алгоритмів у виявленні аномальної поведінки людини. Буде оцінена їхня ефективність за допомогою різних оціночних метрик, включаючи ROC-AUC та EER. Ці метрики дозволять порівняти алгоритми та зрозуміти їхні сильні та слабкі сторони в контексті виявлення аномалій.

Щоб забезпечити справедливе порівняння, було використано однакові набори даних, методи попередньої обробки та методи доповнення даних для всіх алгоритмів. Крім того, були оптимізовані їхні конфігурації та гіперпараметри, щоб досягти найкращої продуктивності в кожному конкретному випадку.

У наступних розділах буде детально розглянуто результати, отримані для кожного алгоритму, а потім проведено порівняльний аналіз, який проллє світло на найефективніший підхід до виявлення аномальної поведінки людини в даних з камер спостереження. Ця оцінка надасть цінну інформацію для дослідників і практиків, які прагнуть впровадити ефективні рішення для виявлення аномалій у реальних системах відеоспостереження.

5.1 Результати моделювання з використанням алгоритму згорткових нейронних мереж

Модель CNN досягла показника AUC 0,8346, що свідчить про високу ефективність класифікації. Це значення свідчить про те, що модель здатна ефективно розрізняти аномальну і нормальну поведінку, з високим показником істинних позитивних результатів і відносно низьким показником хибних позитивних результатів на різних порогових рівнях. Значення AUC ближче до 1 означає ідеальний класифікатор, тоді як значення 0,5 - випадковий класифікатор. Таким чином, отримане

значення AUC 0,8346 демонструє здатність моделі ідентифікувати аномалії зі значною точністю.

З точки зору метрики EER, модель CNN дала значення 0,2439, що свідчить про те, що при оптимальному порозі класифікації приблизно 24,39% класифікацій будуть помилковими, або хибнопозитивними, або хибнонегативними. Нижче значення EER вказує на кращий баланс між хибними спрацьовуваннями та хибними неспрацьовуваннями, що призводить до покращення ефективності класифікації. Отримане значення EER демонструє, що модель CNN демонструє розумний компроміс між хибнопозитивними та хибнонегативними результатами, хоча все ще є місце для вдосконалення. Візуалізація оцінок ROC-AUC та EER для алгоритму CNN наведена на рисунку 5.1.

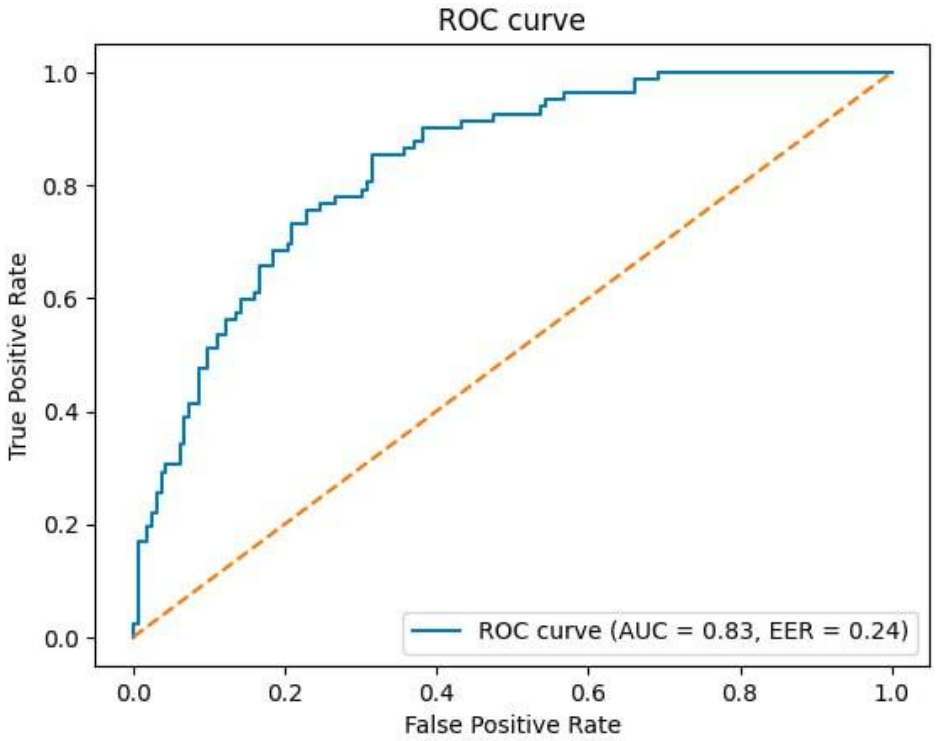

Рисунок 5.1 – Візуалізація оцінки ефективності алгоритму згорткових нейронних мереж

Реалізація CNN для виявлення аномалій у даних камер спостереження показала обнадійливі результати. Ці результати свідчать про те, що CNN може бути ефективним для виявлення аномальної поведінки людини в цьому контексті, але

подальша оптимізація або порівняння з іншими алгоритмами машинного навчання може призвести до ще кращої продуктивності.

5.2 Результати моделювання з використанням алгоритму довготривалої та короткочасної пам’яті

Мережі з довгою короткочасною пам'яттю LSTM, застосовані до задачі виявлення аномалій у даних з камер спостереження, продемонстрували досить ефективну роботу.

З показником ROC-AUC 0,7797 модель LSTM демонструє свою здатність успішно класифікувати аномальні та нормальні випадки. Хоча цей показник не досягає рівня моделі CNN, він все ж вказує на адекватну ефективність у розпізнаванні аномалій. Моделі вдається підтримувати баланс між помірно високим показником істинних спрацьовувань і контрольованим показником хибних спрацьовувань у діапазоні порогових рівнів. EER моделі LSTM є вищим, що свідчить про те, що компроміс між хибнопозитивними і хибнонегативними результатами може бути ще більше оптимізований. Візуалізація оцінок ROC-AUC та EER для алгоритму CNN наведена на рисунку 5.2.

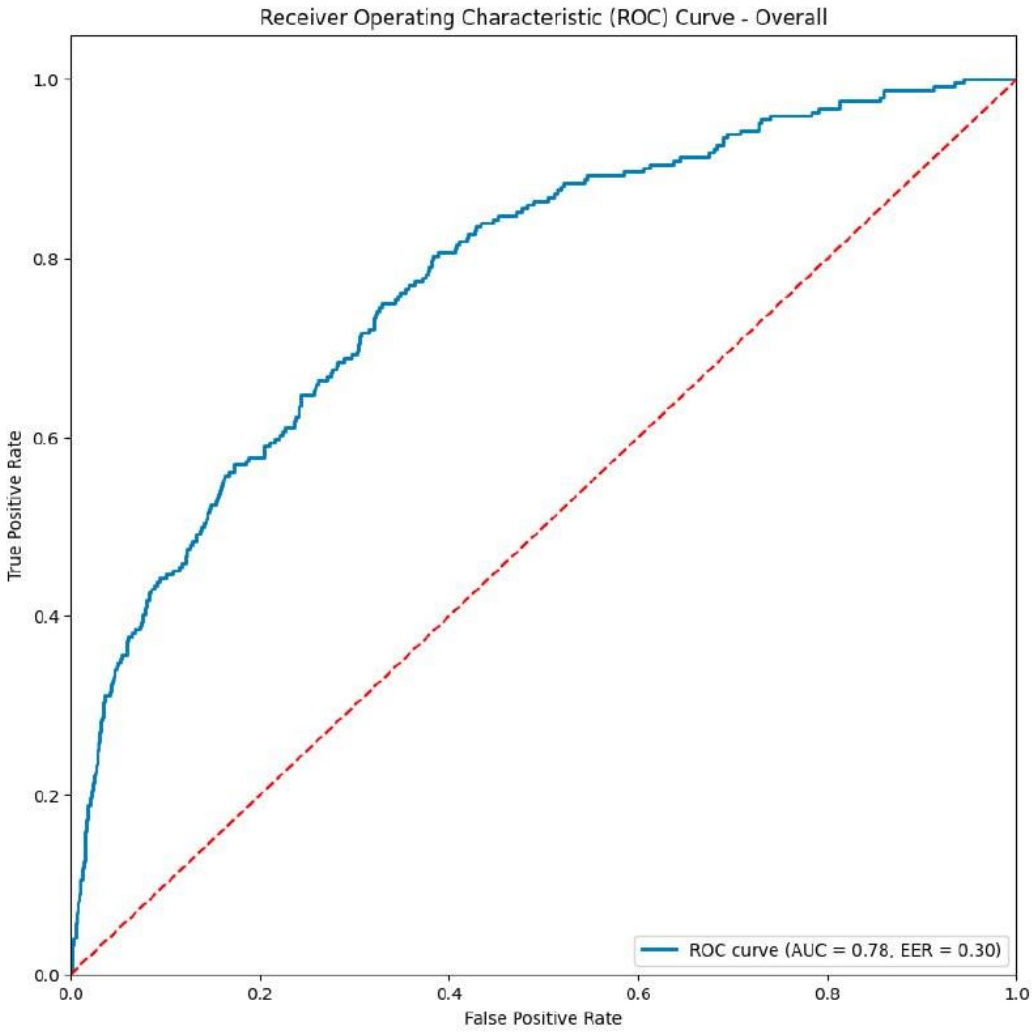

Рисунок 5.2 – Візуалізація оцінки ефектиівності для алгоритму довготривалої та короткочасної пам’яті

Таким чином, мережі LSTM демонструють відносно ефективну роботу у виявленні аномальної поведінки людини за допомогою даних з камер спостереження. Хоча результати не є оптимальними, підхід LSTM залишається життєздатним варіантом для задач виявлення аномалій.

5.3 Результати моделювання з використанням алгоритму машини опорних векторів

Показник ROC-AUC для алгоритму SVM склав 0,7281, що вказує на помірний рівень продуктивності в розрізненні аномальних і нормальних подій. Показник AUC нашої SVM-моделі свідчить про те, що її ще можна вдосконалити.

У контексті нашого дослідження EER 0,3780 означає, що SVM-модель може правильно класифікувати приблизно 62,2% випадків, коли частота хибнопозитивних і хибнонегативних спрацьовувань однакова. Візуалізація оцінок ROC-AUC та EER для алгоритму SVM наведена на рисунку 5.3.

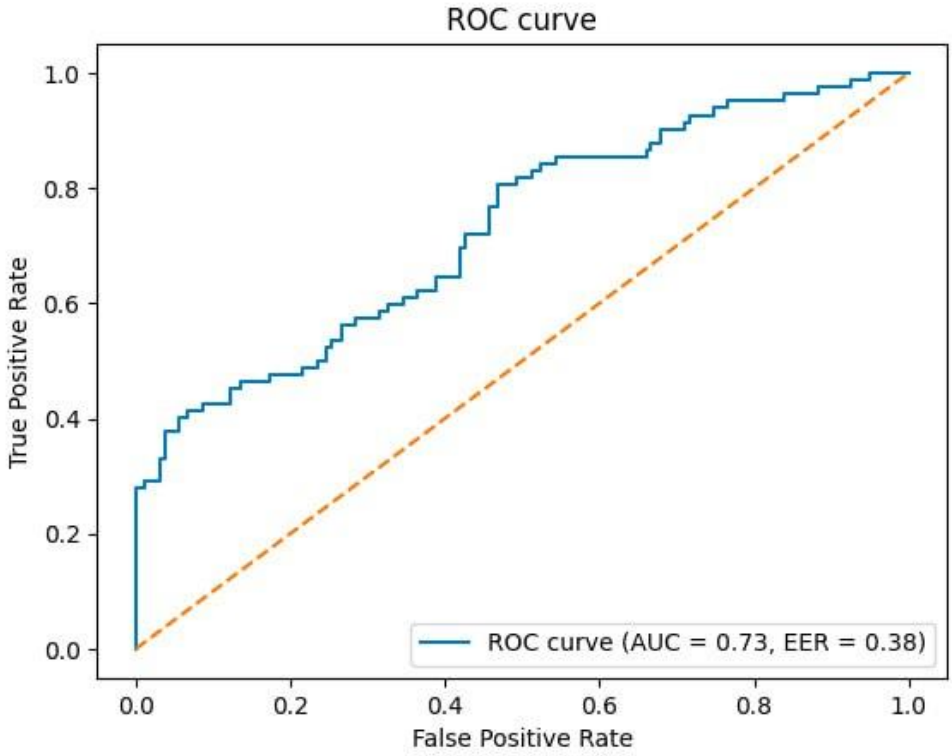

Рисунок 5.3 – Візуалізація оцінки ефективності для алгоритму машини опорних векторів

Цей результат демонструє потенціал алгоритму SVM для задач класифікації відео, але також підкреслює необхідність подальшої оптимізації та вивчення інших методів машинного навчання для підвищення ефективності класифікації.

5.4 Результати моделювання з використанням алгоритму рекурентної нейронної мережі

Ефективність RNN-моделі, виміряна за допомогою ROC-AUC, склала 0,7602. Цей результат показує, що RNN-модель перевершила алгоритм SVM, але алгоритми LSTM і CNN все ще перевершують його в розрізненні аномальних і нормальних подій.

Що стосується метрики EER, то модель RNN досягла значення 0,3292, що є кращим показником, ніж EER моделі SVM (0,3780). При меншому значенні EER RNN модель може правильно класифікувати близько 67,08% випадків. Візуалізація оцінок ROC-AUC та EER для алгоритму RNN наведена на рисунку 5.4.

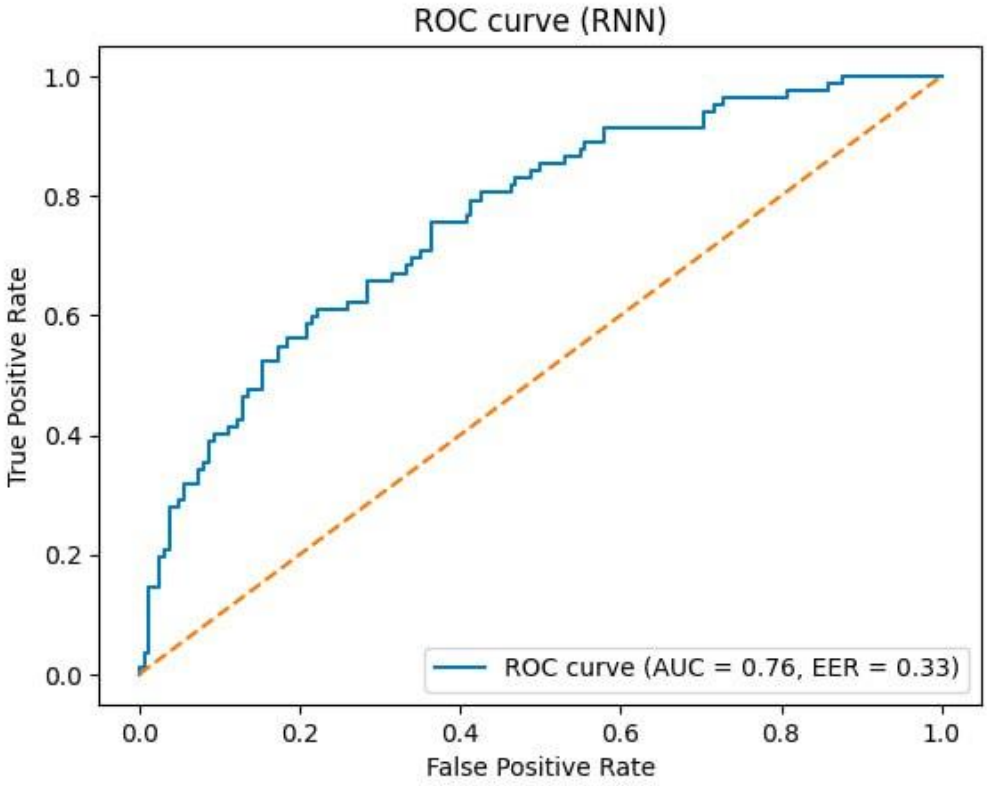

Рисунок 5.3 – Візуалізація оцінки ефективності для алгоритму рекурентної нейронної мережі

Загалом, продуктивність моделі RNN, про що свідчать ROC-AUC 0,7602 та EER 0,3292, демонструє досить добру роботу в задачі класифікації відео.

5.5 Зведення метрик продуктивності для алгоритмів

У цьому підрозділі представлено короткий огляд метрик продуктивності, отриманих в результаті реалізації різних алгоритмів машинного навчання, включаючи згорткові нейронні мережі CNN, мережі з довгою і короткою пам'яттю LSTM, машини опорних векторів SVM і рекурентні нейронні мережі RNN. Ці показники дають цінну інформацію про ефективність кожного алгоритму у виявленні аномалій у системах відеоспостереження. У таблиці 5.1 нижче наведено порівняння продуктивності кожного методу.

Таблиця 5.1 – Зведення метрик продуктивності для алгоритмів

	ROC-AUC	EER
CNN	0.8346	0.2439
LSTM	0.7797	0.3039
SVM	0.7281	0.3780
RNN	0,7602	0,3292

5.6 Переваги та обмеження кожного алгоритму

У цьому підрозділі обговорені компроміси та обмеження кожного алгоритму машинного навчання, що використовується для виявлення аномалій у системах відеоспостереження. У таблиці 5.2 нижче наведено переваги та обмеження, пов'язані з кожним методом.

Таблиця 5.2 – Переваги та обмеження кожного алгоритму

Алгоритм	Переваги	Обмеження
CNN	Висока точність і продуктивність. Ефективний в роботі з просторовими об'єктами.	Потребує великих наборів даних для навчання. Дорогий в обчислювальному плані
LSTM	Добре фіксує часові залежності. Підходить для часових рядів даних.	Довший час навчання. Труднощі з розпаралелюванням
SVM	Добре працює з невеликими наборами даних. Ефективний для даних високої розмірності.	Проблеми масштабування з великими наборами даних. Чутливий до вибору ядра та налаштування параметрів.
RNN	Може фіксувати послідовну інформацію. Застосовується для різних послідовних завдань.	Проблема зникаючого градієнта. Обмежений обсяг пам'яті.

Розуміючи ці фактори, можна краще оцінити їхню придатність для конкретних застосувань і визначити сфери для вдосконалення.

На основі переваг і обмежень кожного алгоритму машинного навчання, можна зробити висновок, що CNN та LSTM можуть бути найбільш ефективними для виявлення аномалій поведінки, у тому числі таких, як виявлення інсайдерів, та аномальних ситуацій, як пожежа, задимлення, проникнення у приміщення сторонніх осіб у неробочий час, пронесення на контрольовану територію підозрілих предметів, тощо. Це пояснюється тим, що CNN володіє високою точністю в роботі з просторовими об'єктами, а LSTM здатний фіксувати часові залежності і підходить для часових рядів даних.

Для подальшого поліпшення якості виявлення аномалій та забезпечення більш точної реакції на аномальні події, можна розробити систему, що буде включати алгоритми машинного навчання, які працюють у співпраці. Це дозволить комбінувати переваги різних алгоритмів для досягнення більш високої точності та надійності виявлення аномалій.

6 ІМПЛЕМЕНТАЦІЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ У КОМПЛЕКСНУ СИСТЕМУ БЕЗПЕКИ

У даному розділі досліджується процес імплементації алгоритмів машинного навчання, у комплексну систему безпеки.

Впровадження алгоритмів машинного навчання у системи відеоспостереження та безпеки дозволяє значно підвищити ефективність та точність виявлення аномальних ситуацій, що забезпечує більш надійний захист об'єктів та поліпшення якості контролю. Розглянуті в даному розділі практичні аспекти впровадження допоможуть забезпечити успішну інтеграцію алгоритмів машинного навчання в існуючі системи та забезпечити їхнє ефективне функціонування [24].

6.1 Процес інтеграції алгоритму машинного навчання у систему відеоспостереження з інтелектуальною відеоаналітикою

У даному підрозділі буде розглянуто процес інтеграції алгоритму згорткових нейронних мереж CNN у систему відеоспостереження з інтелектуальною відеоаналітикою. Згорткові нейронні мережі були визначені як найефективніший алгоритм для виявлення аномалій на основі результатів, отриманих у попедерньому розділі, дозволить значно покращити здатність системи виявляти аномальні явища та поведінку об'єктів у реальному часі.

Метою даного підрозділу є опис інтеграційного процесу, включаючи адаптацію алгоритму CNN до потреб системи відеоспостереження, налаштування параметрів та взаємодію з існуючими компонентами системи. Також будуть розглянуті можливі технічні та алгоритмічні виклики, пов'язані з інтеграцією алгоритму згорткових нейронних мереж у систему відеоспостереження, та способи їх подолання.

Інтеграційний процес алгоритму CNN у систему відеоспостереження з інтелектуальною відеоаналітикою може бути поділений на кілька ключових етапів, наведених у таблиці 6.1.

Таблиця 6.1 – Етапи інтеграційного процес алгоритму

Назва етапу	Опис етапу
1	2
Адаптація алгоритму CNN до потреб системи відеоспостереження	На цьому етапі необхідно внести зміни до архітектури та параметрів CNN таким чином, щоб вони відповідали специфікаціям системи відеоспостереження. Це може включати оптимізацію розміру вхідного зображення, кількості шарів та параметрів самої мережі.
Налаштування параметрів та гіперпараметрів	Відповідні параметри та гіперпараметри CNN, такі як швидкість навчання, кількість епох, розмір партії та коефіцієнти регуляризації, повинні бути налаштовані для досягнення оптимальної продуктивності та ефективності на відеоданих, які отримуються від системи відеоспостереження.
Інтеграція алгоритму CNN з існуючими компонентами системи відеоспостереження	Алгоритм CNN повинен бути інтегрований з існуючими компонентами системи відеоспостереження, такими як модулі зберігання відеоданих, обробки відеопотоку та передачі сигналів. Це включає розробку інтерфейсів для обміну даними між CNN та цими компонентами.
Розгортання алгоритму CNN на апаратному рівні	Для оптимальної роботи алгоритму CNN у реальному часі, його слід розгорнути на відповідному апаратному рівні. Це може включати використання спеціалізованих пристроїв, таких як граф фічні процесори GPU або спеціалізовані апаратні прискорювачі для операцій згортки, що підвищить продуктивність та ефективність обробки відеоданих у режимі реального часу.

Продовження таблиці 6.1.

1	2
Тестування та налагодження інтегрованої системи	Після інтеграції алгоритму CNN у систему відеоспостереження необхідно провести ряд тестів, щоб перевірити стабільність та ефективність системи у різних умовах. На основі результатів тестування можуть бути внесені корективи в параметри та налаштування алгоритму та системи відеоспостереження.
Моніторинг та оновлення моделі	З метою підтримки оптимальної ефективності алгоритму CNN, необхідно регулярно моніторити його роботу та проводити оновлення моделі на основі нових даних та відгуків. Це може включати збір та аналіз даних про реальні аномалії, а також оновлення навчальних даних та параметрів моделі.

Цей процес дозволить впровадити алгоритм CNN у систему відеоспостереження з інтелектуальною відеоаналітикою та забезпечити високу продуктивність та ефективність виявлення аномалій у комплексній системі безпеки.

Інтеграція алгоритму CNN у систему відеоспостереження може мати деякі технічні та алгоритмічні виклики, які потребують уваги та рішень. Нижче наведені деякі з них.

1) Обмеження обчислювальних ресурсів. CNN вимагає значних обчислювальних потужностей для ефективної роботи. Інтеграція CNN у систему відеоспостереження може виявитися обмеженою через недостатні обчислювальні ресурси. Можливим рішенням є використання апаратних прискорювачів, таких як GPU, або оптимізація архітектури CNN для зменшення обчислювальних вимог.

2) Відгук у реальному часі. Для забезпечення відгуку у реальному часі необхідно оптимізувати алгоритм CNN та процес обробки відео. Це можна досягти шляхом використання ефективних алгоритмів стиснення відео, паралельної обробки даних та використання спеціалізованих апаратних рішень.

3) Робастність моделі до змін умов освітлення, перешкод та інших факторів. Модель CNN повинна бути стійкою до змінних умов освітлення, погодних умов,

перешкод на сцені та інших зовнішніх факторів. Розвиток та використання методів переднавчання, аугментації даних та адаптивних архітектур можуть допомогти забезпечити робастність моделі та підвищити її ефективність в різних умовах.

4) Конфіденційність та безпека даних. Інтеграція алгоритму CNN у систему відеоспостереження може викликати питання конфіденційності та безпеки даних. Застосування методів шифрування, аутентифікації та контролю доступу є важливими для забезпечення безпеки даних у системі.

5) Сумісність з існуючим обладнанням та програмним забезпеченням. Інтеграція CNN у систему відеоспостереження може вимагати сумісності з наявним обладнанням та програмним забезпеченням. Розробка адаптерів, API та інтерфейсів для забезпечення безперебійної інтеграції є важливою частиною процесу імплементації.

6) Складність розгортання та обслуговування. Інтеграція CNN може збільшити складність розгортання та обслуговування системи відеоспостереження. Організація підтримки та створення належної документації для спрощення розгортання та обслуговування є критично важливими [25].

Розглянувши ці виклики та потенційні рішення, можна підготувати систему відеоспостереження до успішної інтеграції з алгоритмами машинного навчання.

6.2 Інтеграція системи відеоспостереження з інтелектуальною відеоаналітикою у комплексну систему безпеки

Інтеграція системи відеоспостереження з інтелектуальною відеоаналітикою, зокрема алгоритму згорткових нейронних мереж CNN, у комплексну систему безпеки важлива для забезпечення оптимального рівня захисту об'єктів та персоналу, ефективного моніторингу та виявлення аномалій та різних загроз.

У цьому підрозділі будуть розглянуті основні аспекти інтеграції, такі як взаємодія інтелектуальної системи відеоспостереження з іншими компонентами комплексної системи безпеки, налаштування спільних каналів комунікації та передачі даних, а також налагодження роботи системи відеоспостереження з різними сенсорами та пристроями безпеки для забезпечення комплексного захисту, які можна побачити у таблиці 6.2.

Таблиця 6.2 – Основні аспекти інтеграції системи відеоспостереження з інтелектуальною відеоаналітикою у комплексну систему безпеки.

Аспект інтеграції	Опис аспекту	Запропоноване технічне рішення
1	2	3
Взаємодія з іншими компонентами комплексної системи безпеки	Необхідність співпраці системи відеоспостереження з іншими елементами системи безпеки для ефективного реагування на аномалії та загрози.	Розробка спільного протоколу комунікації та інтерфейсів для обміну даними між різними компонентами системи.
Канали комунікації та передачі даних	Встановлення зв'язку між системою відеоспостереження та іншими компонентами комплексної системи безпеки для передачі інформації про аномалії та загрози.	Використання стандартних мережевих протоколів (наприклад, TCP/IP) та шифрування даних для безпечної передачі.
Робота з різними сенсорами та пристроями безпеки	Інтеграція системи відеоспостереження з різними типами сенсорів та пристроїв безпеки для забезпечення комплексного контролю об'єктів.	Розробка модульної архітектури для підключення та управління різними сенсорами та пристроями через єдиний інтерфейс.
Адаптація до специфіки об'єктів	Необхідність адаптації системи відеоспостереження та алгоритмів виявлення аномалій до специфіки окремих об'єктів та їх особливостей.	Розробка параметричної моделі алгоритмів виявлення аномалій, що дозволяє налаштовувати їх відповідно до потреб об'єкта.

Продовження таблиці 6.2.

1	2	3
Моніторинг та аналіз результатів імплементації	Систематичний контроль та збір даних про роботу системи відеоспостереження з інтелектуальною відеоаналітикою для оцінки її ефективності та виявлення проблем.	Розробка модуля для моніторингу, який дозволить відслідковувати показники роботи системи та збирати статистичні дані.
Оновлення алгоритмів та покращення системи	Постійний розвиток та покращення алгоритмів машинного навчання та системи відеоспостереження для підвищення ефективності виявлення аномалій.	Використання модульної архітектури для забезпечення можливості оновлення алгоритмів та компонентів без втрати роботи системи.
Реагування на аномальні явища	Організація оперативного реагування на аномальні явища, виявлені системою відеоспостереження з інтелектуальною відеоаналітикою.	Розробка процедур та сценаріїв реагування, які включають автоматичне виклик оперативних служб або включення сигналізації.
Приватність та захист даних	Забезпечення захисту та конфіденційності даних, що обробляються системою відеоспостереження з інтелектуальною відеоаналітикою.	Використання сучасних методів шифрування даних, регулярний аудит системи безпеки та дотримання нормативно-правових актів з приватності даних.

6.3 Оповіщення та реагування на аномальні явища на об'єкті

Важливим елементом успішної реалізації комплексної системи безпеки є своєчасне оповіщення відповідних служб або відповідальних осіб про потенційно небезпечні ситуації та забезпечення ефективного реагування на подібні події. У цьому підрозділі розглядається організація оповіщення та реагування на аномальні явища в рамках комплексної системи безпеки.

Процес організації оповіщення та реагування на аномальні явища в рамках комплексної системи безпеки може бути реалізований наступним чином.

Система відеоспостереження з інтелектуальною відеоаналітикою, яка використовує алгоритм згорткових нейронних мереж CNN, виявляє аномальну подію або поведінку на відеозображенні. Алгоритм CNN аналізує деталі аномальної події, визначає її характеристики та класифікує її за ступенем ризику або важливості.

На основі аналізу аномалії система генерує оповіщення з детальною інформацією про подію, її місцезнаходження, час виникнення та іншими релевантними даними. Система надсилає оповіщення до відповідних служб або відповідальних осіб через налаштовані канали зв'язку, такі як електронна пошта, SMS, мобільні додатки або спеціалізовані системи сповіщення.

Отримавши оповіщення, відповідальні особи або служби оцінюють ситуацію та вживають необхідних дій для реагування на аномальну подію. Це може включати перевірку події на місці, виклик поліції, пожежних чи медичних служб, активацію аварійних процедур та координацію з іншими компонентами комплексної системи безпеки.

Після реагування на аномальну подію збирається зворотний зв'язок від відповідальних осіб або служб, який включає результати їх дій та можливі пропозиції щодо поліпшення системи. Зібрані дані можуть використовуватися для оптимізації алгоритму CNN, налаштування параметрів системи оповіщення та реагування, а також для розробки навчальних програм для співробітників, щоб краще реагувати на подібні аномальні явища у майбутньому [26].

Для ефективного реагування на аномальні явища, система відеоспостереження з інтелектуальною відеоаналітикою повинна бути інтегрована з іншими компонентами комплексної системи безпеки, такими як системи контролю доступу,

пожежної безпеки, персонального відслідковання тощо. Це дозволить координувати дії між різними системами та забезпечити швидке та ефективне реагування на аномальні явища.

Організація процесу оповіщення та реагування на аномальні явища в рамках комплексної системи безпеки вимагає взаємодії та координації різних компонентів безпеки, а також забезпечення постійного аналізу та оптимізації системи для підвищення її ефективності та адаптивності.

6.4 Розробка сценаріїв співпраці системи відеоспостереження з іншими компонентами комплексної системи безпеки

Для ефективної роботи комплексної системи безпеки важливо розробити сценарії співпраці між системою відеоспостереження з інтелектуальною відеоаналітикою та іншими компонентами. Це дозволить забезпечити координовану реакцію на різні аномальні події та зменшити ймовірність ложних спрацьовувань або неправильного реагування. Розглянемо декілька прикладів сценаріїв співпраці, що представлено в таблиці 6.3.

Таблиця 6.3 – Сценарії співпраці системи відеоспостереження з іншими компонентами комплексної системи безпеки

Сценарій співпраці з системою	Опис сценарію
1	2
Система контролю доступу	У разі виявлення неавторизованого входу на територію об'єкта система відеоспостереження може передавати інформацію про подію системі контролю доступу. Це дозволить останній заблокувати доступ до внутрішніх приміщень та відправити оповіщення відповідальним особам або охороні.

Продовження таблиці 6.3.

1	2
Система пожежної безпеки	У разі виявлення пожежі або задимлення система відеоспостереження може передавати інформацію про подію системі пожежної безпеки, яка в свою чергу активує пожежну сигналізацію та систему пожежогасіння.
Система персонального відслідковання	У разі виявлення аномальної поведінки працівника або відвідувача, система відеоспостереження може передавати дані про подію системі персонального відслідковання. Це дозволить відслідковувати рух особи по території об'єкта та підтримувати контакт з ним у разі потреби.
Система евакуації	У разі виявлення екстрених ситуацій, таких як пожежа, землетрус або терористична загроза, система відеоспостереження може передавати дані про подію системі евакуації. Це дозволить швидко розподілити потік евакуємого персоналу та відвідувачів, враховуючи стан коридорів, виходів та інших маршрутів, а також забезпечити контроль за евакуацією через відеоспостереження.
Система зв'язку і оповіщення	У разі виявлення аномальних подій система відеоспостереження може передавати інформацію системі зв'язку і оповіщення. Це дозволить оперативно інформувати відповідальних осіб, охорону та служби порятунку про виявлені проблеми та забезпечити їх оперативне реагування.
Система автоматичного відключення енергопостачання	У разі виявлення витоку струму, короткого замикання або інших електротехнічних проблем система відеоспостереження може передавати інформацію про подію системі автоматичного відключення енергопостачання. Це дозволить вчасно відключити електропостачання у зоні проблеми, запобігти подальшому розвитку аварійної ситуації та забезпечити безпеку персоналу та відвідувачів.

Ці та інші сценарії співпраці системи відеоспостереження з іншими компонентами комплексної системи безпеки дозволяють забезпечити гнучкість, ефективність та автоматизацію процесів реагування на різні аномальні події, що можуть виникнути на об'єкті.

ВИСНОВКИ

У ході виконання даної магістерської роботи було проаналізовано сучасні методи виявлення аномалій в системах відеоспостереження. Основними методами, що вивчалися, були згорткові нейронні мережі CNN, мережі з довгою короткочасною пам'яттю LSTM, машини опорних векторів SVM та рекурентні нейронні мережі RNN.

Показники ефективності алгоритмів, такі як ROC-AUC і EER, демонструють, що деякі алгоритми перевершують інші у виявленні аномалій в системах відеоспостереження. Згорткові нейронні мережі CNN показали найкращі результати: ROC-AUC – 0,8346, EER – 0,2439. Це можна пояснити їхньою здатністю ефективно фіксувати просторові особливості в даних зображень, що має вирішальне значення для виявлення аномальної поведінки людини на відеокадрах. Методи на основі LSTM також показали хороші результати, досягнувши ROC-AUC 0,7797 і EER 0,3039, завдяки своїй здатності фіксувати часові залежності в даних часових рядів.

З іншого боку, машини опорних векторів SVM та рекурентні нейронні мережі (RNN) досягли нижчих показників ефективності: ROC-AUC – 0,7281 та 0,7602, а EER – 0,3780 та 0,3292 відповідно. Ці результати свідчать про те, що ці алгоритми менш ефективні для виявлення аномальної поведінки в системах відеоспостереження порівняно з CNN та LSTM.

Відмінності в показниках ефективності між алгоритмами можна пояснити компромісами та обмеженнями кожного методу, як було обговорено в попередньому розділі. Наприклад, проблеми масштабування SVM на великих наборах даних і чутливість до вибору ядра та налаштування параметрів можуть обмежити ефективність виявлення певних типів аномальної поведінки. Аналогічно, проблема зникаючого градієнта та обмежений об'єм пам'яті RNN також можуть вплинути на його продуктивність у задачах виявлення аномалій.

Враховуючи переваги та обмеження кожного алгоритму машинного навчання, можна стверджувати, що CNN та LSTM мають великі перспективи для ефективного виявлення аномалій у поведінці, включаючи виявлення інсайдерів та ситуаційних аномалій, таких як пожежі, задимлення, неповноважене проникнення в приміщення

поза робочим часом, перевезення сумнівних предметів на контрольованій території та ін.

Інтеграція алгоритму машинного навчання у систему відеоспостереження з інтелектуальною відеоаналітикою дозволяє покращити виявлення аномалій та зменшити кількість ложних тривог, завдяки точному та швидкому аналізу відеоданих. Успішне поєднання системи відеоспостереження з інтелектуальною відеоаналітикою у комплексній системі безпеки сприяє забезпеченню надійного виявлення аномальних подій та оперативного реагування на них, підвищуючи рівень безпеки об'єкта. Розробка сценаріїв співпраці системи відеоспостереження з іншими компонентами комплексної системи безпеки дозволяє оптимізувати роботу системи в цілому, забезпечуючи її більш ефективне функціонування. Впровадження оповіщення та реагування на аномальні явища в рамках комплексної системи безпеки дозволяє оперативно повідомляти відповідні служби про виникнення аномалій, що сприяє своєчасному реагуванню на потенційні загрози безпеці.

Завершуючи, можна сказати, що дана магістерська робота створює міцну основу для подальшого дослідження та розвитку систем відеоаналітики на основі штучного інтелекту для виявлення аномалій у комплексних системах безпеки. Вивчення та реалізація передових методів та алгоритмів машинного навчання сприятиме створенню більш ефективних, надійних та інтелектуальних систем безпеки в різних галузях, таких як промисловість, транспорт, міське планування та охорона довкілля.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Семеренська В. В. Можливості інтегрованих систем відеоспостереження. *Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті* : матеріали Всеукраїнської науково-практичної Internet-конференції, м. Харків, 15 – 16 лист. 2022 р. Харків : ХНАДУ, 2022. С. 78–80.
2. Семеренська В. В. Виявлення аномалій у поведінці людини за даними камер спостереження з використанням методів машинного навчання. *Експериментальні та теоретичні дослідження в контексті сучасної науки* : матеріали II Всеукраїнської студентської наукової конференції, м. Івано-Франківськ, 24 берез. 2023 р. Вінниця : ГО «Європейська наукова платформа», 2023. С. 53–54.
3. Семеренська В. В. Аналіз ефективності інтегрованої системи безпеки. *Пріоритетні напрямки та вектори розвитку світової науки* : матеріали III Всеукраїнської студентської наукової конференції, м. Черкаси, 31 берез. 2023 р. Вінниця : ГО «Європейська наукова платформа» 2023. С. 148 –149.
4. Video analytics and artificial intelligence. About machine learning and deep learning based analytics tools deep learning URL: https://www.axis.com/files/whitepaper/wp_AI_in_video_analytics_ru_2103.pdf (дата звернення: 01.04.2023).
5. Berroukham A. Deep learning-based methods for anomaly detection in video surveillance: a review. *Bulletin of Electrical Engineering and Informatics*. 2023. Vol. 12, No. 1. P. 314–327.
6. Sultani W., Chen C., Shah M. Real-World Anomaly Detection in Surveillance Videos. *CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Salt Lake City, UT, 18–23 June 2018. 2018. P. 6479.
7. Aldayri A., Albattah W. Taxonomy of Anomaly Detection Techniques in Crowd Scenes. *Sensors*. 2022. Vol. 22, No. 16. P. 6080.
8. Al-amri R. A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. *Applied Sciences*. 2021. Vol. 11, No.12. P. 5320.
9. Rohit Kumar K., Gandhewar N. Anomaly Detection in Surveillance System Using Machine Learning Techniques – A Review. *SSRN Electronic Journal*. 2022.

10. Thakkar K., Kadiya K., Chauhan J. Anomaly detection in surveillance video. 2021.

11. Andersson M., Hemström F., Molin S. Robust anomaly detection in urban environments using sensor and information fusion and a camera network. *Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies*, Berlin, Germany, 10–13 September 2018. P. 356.

12. Kumari P., Bedi A. K., Saini M. Multimedia Datasets for Anomaly Detection: A Survey. 2022.

13. Wen J. Systematic literature review of machine learning based software development effort estimation models. *Information and Software Technology*. 2012. Vol. 54, No. 1. P. 41–59.

14. Miki D., Chen S., Demachi K. Unnatural Human Motion Detection using Weakly Supervised Deep Neural Network. *2020 Third International Conference on Artificial Intelligence for Industries (AI4I)*, Irvine, CA, USA, 21–23 September 2020. P. 4051.

15. Семеренська В. В. Моделювання системи відеоспостереження. *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій* : матеріали 25-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті», м. Харків, 20 – 21 квіт. 2021 р. Харків : ХНУРЕ, 2021. С. 54–55.

16. Kiran B., Thomas D., Parakkal R. An Overview of Deep Learning Based Methods for Unsupervised and Semi-Supervised Anomaly Detection in Videos. *Journal of Imaging*. 2018. Vol. 4, No. 2. P. 36.

17. Chawla S., Raghavendra C. Deep Learning for Anomaly Detection: A Survey. 2019.

18. Abbas Z. K., Al-Ani A. A. A Comprehensive Review for Video Anomaly Detection on Videos. *2022 International Conference on Computer Science and Software Engineering (CSASE)*, Duhok, Iraq, 15–17 March 2022. 2022. P.2055

19. Marsiano A. F. D., Soesanti I., Ardiyanto I. Deep learning-based Anomaly Detection on Surveillance Videos: Recent Advances. *2019 International Conference of Advanced Informatics: Concepts, Theory and Applications (ICAICTA)*, Yogyakarta, Indonesia, 20–21 September 2019. P.157

20. Ren H., Moeslund T. B. Abnormal event detection using local sparse representation. *2014 International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, Seoul, South Korea, 26–29 August 2014. P. 160

21. Ravanbakhsh M. Abnormal event detection in videos using generative adversarial nets. *2017 IEEE International Conference on Image Processing (ICIP)*, Beijing, 17–20 September 2017. P. 47

22. Sabokrou M. Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes. *Computer Vision and Image Understanding*. 2018. Vol. 172. P. 88–97.

23. Carreira J., Zisserman A. Quo Vadis, Action Recognition? A New Model and the Kinetics Dataset. *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, 21–26 July 2017. P. 391

24. Liu W. Future Frame Prediction for Anomaly Detection - A New Baseline. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Salt Lake City, UT, 18–23 June 2018. P. 58

25. Morais R. Learning Regularity in Skeleton Trajectories for Anomaly Detection in Videos. *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Long Beach, CA, USA, 15–20 June 2019.

26. Zhou K., Qiao Y., Xiang T. Deep Reinforcement Learning for Unsupervised Video Summarization with Diversity-Representativeness Reward. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2018. Vol. 32, No. 1.