Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу”

Виконав здобувач вищої освіти
ІІ курсу, групи КІ-25М
ОПП «Комп’ютерна інженерія»
спеціальності F7 «Комп’ютерна інженерія»
_____ Язловецький Б.М.
«____» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнов С.А.
«____» _____ 2026 р.

Нормоконтроль проекту
_____ Коваленко А.С.
«____» _____ 2026 р.

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
Язловецький Богдан Максимович
Сертифікат: 514B5C86A1E5DA110400000044AFE7005D791505
Дійсний з 18.12.2025 16:29:28 по 18.12.2026 16:29:27

Центральноукраїнський національний технічний університет

Факультет *Механіко-технологічний*

Кафедра *Кібербезпеки та програмного забезпечення*

Рівень вищої освіти *магістр*

Галузь знань _F_____*"*Інформаційні технології*"*_____

Спеціальність F7 *"*Комп'ютерна інженерія*"*

Освітньо-професійна (освітньо-наукова) програма _*"*Комп'ютерна інженерія*"*_

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 1 » вересня 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Язловецькому Богдану Максимовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу*

2. Керівник роботи *Смірнов Сергій Анатолійович, кандидат технічних наук, доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 41-13 від 17.08.2026 року

3. Строк подання студентом роботи до захисту *2.12.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи*: Метою розробки є дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.	*5. Впровадження системи в промислову експлуатацію*
2. Перегляд аналогічних існуючих систем.	*6. Наукова новизна*.
3. Опис і обґрунтування проектних рішень.	*7. Заходи з охорони праці та техніки безпеки.*
4. Етапи програмування системи.	*8. Висновки.*

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Наукова новизна	*1 аркуш*
Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи додатку	*2 аркуша*

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Марченко К.М., к.т.н., доцент	06.10.2026	16.11.2026

8. Дата видачі завдання « 1 » вересня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.10.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.10.2026 р.	
3.	Розробка моделі компонента	20.10.2026 р.	
4.	Розробка структур даних	25.10.2026 р.	
5.	Розробка алгоритмів системи	30.10.2026 р.	
6.	Програмування алгоритмів	10.11.2026 р.	
7.	Розрахунки з охорони праці та техніки безпеки	15.11.2026 р.	
8.	Оформлення ПЗ	17.11.2026 р.	
9.	Попередній захист роботи	2.12.2026 р.	

Дата видачі завдання
« 1 » вересня 2026 р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
« 1 » вересня 2026 р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Язловецький Б.М. Дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу. F7 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Метою розробки є дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Об'єктом дослідження є процес апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Предметом дослідження є методи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Методи дослідження базуються на методах теорії кодування, методів теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Python.

Ключові слова: комп’ютерна інженерія, мережа, відеоспостереження, апаратне прискорення, аналіз відеопотоків, режим реального часу

ABSTRACT

Yazlovetskyi B.M. Research and Software Implementation of a Network Video Surveillance System with Hardware-Accelerated Real-Time Video Stream Analysis. F7 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

This master's-level final qualification thesis presents the development of software designed for a network video surveillance system that utilizes hardware acceleration for real-time video stream analysis.

The objective of this project is the research and software implementation of a network video surveillance system featuring hardware-accelerated real-time video stream analysis.

The object of the research is the operation of a network video surveillance system with hardware-accelerated real-time video stream analysis.

The subject of the research consists of the methods employed within a network video surveillance system featuring hardware-accelerated real-time video stream analysis.

The research methodology draws upon coding theory, computer network theory, mathematical statistics, and software development practices.

The outcome of the work is the software implementation of a network video surveillance system with hardware-accelerated real-time video stream analysis.

During the development of the software model, an analysis of existing hardware and software solutions was conducted. All components of the developed software are described in full detail.

A user-friendly interface has been developed. Instructions for using the software tools are provided.

The program can be used on PCs running the Windows 10/11 operating system.

The program was developed using the Python environment.

Keywords: computer engineering, network, video surveillance, hardware acceleration, video stream analysis, real-time mode

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	90	–	
2	А4	Робоча програма	48	–	Додаток А
		Графічні документи			
3	А4	Наукова новизна	1	–	
4	А4	Структурна схема	1	–	
5	А4	Функціональна схема роботи системи	1	–	
6	А4	Діаграма взаємодії процесів	1	–	
7	А4	Блок-схема основної програми	1	–	
8	А4	Блок-схема роботи підпрограми	1	–	

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 10
ВСТУП..... 11
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 14
1.1 Призначення системи..... 14
1.2 Область застосування 15
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 17
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 17
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 23
2.3 Розгорнута постановка завдання 24
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 26
3.1 Опис функціонування системи 26
3.2 Розробка структурної схеми..... 30
3.3 Розробка функціональної схеми 45
3.4 Розробка діаграми процесів 48
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 50
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 50
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 66
6 НАУКОВА НОВИЗНА 70

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 71
7.1 Вступ 71
7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером 72
7.3 Аналіз умов праці на робочому місці фахівця 73
7.4 Розробка заходів з поліпшення охорони праці 77
7.5 Розрахункова частина 78
8 ОСНОВНІ ВИСНОВКИ 81
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 83

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

БПД	–	бездротова передача даних
ПЗ	–	програмне забезпечення
СПД	–	системи передачі даних
ACK	–	повідомлення підтвердження прийому
ARQ	–	протокол повторної передачі даних
BPSK	–	Binary phase-shift keying
FFD	–	повнофункціональний пристрій
GFSK	–	Gaussian frequency-shift keying
MAC	–	шар механізму доступу
NACK	–	повідомлення непідтвердження прийому
OSI	–	мережна модель
P2P	–	однорангові мережі
PAN	–	персональна мережа
PPS	–	Portable Protocol Stack
RFD	–	пристрій з полегшеними функціями
TDMA	–	часовий поділ
Wi-Fi	–	бездротова технологія

ВСТУП

Актуальність теми. Відеоаналітика для спостереження – це програмне забезпечення, яке запускає моделі комп'ютерного зору на зображеннях з камер і перетворює пікселі на події з часовими мітками, які можна знайти: людина в обмеженій зоні, номерний знак біля воріт, залишена сумка. Інтеграція – це робота з передачі цих подій до VMS, інструментів контролю доступу та сповіщень, які оператори вже використовують, щоб сповіщення досягало людини менш ніж за секунду, а не залишалося на окремій панелі інструментів. Аналітики очікують, що ринок відеоаналітики досягне приблизно 37,8 мільярда доларів до 2030 року, зростаючи на 19,5% на рік з 2025 року.

«Відеоаналітика» – це насправді десяток окремих продуктів під одним ярликом: виявлення осіб і транспортних засобів, розпізнавання номерних знаків, байдикування та вторгнення, теплові карти, довжина черги, відповідність вимогам ЗІЗ, виявлення зброї, виявлення вогню та диму, судово-медичний пошук природною мовою та оповіщення в режимі реального часу в систему управління відеоспостереженням (VMS). Більшість модернізацій зазнають невдачі, оскільки вони намагаються інтегрувати всі ці функції одночасно в існуючий стек спостереження.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

– Дослідження системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

– Програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Об'єктом дослідження є процес апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Предметом дослідження є методи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Методи дослідження базуються на методах теорії кодування, методів теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

– Розроблено вітчизняний продукт апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними

дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVIII науково-технічній конференції здобувачів вищої освіти «Наука-виробництву», основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №17.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Інтеграція відеоаналітики перетворює пікселі, які вже записує система спостереження, на події з мітками часу («особа увійшла до зони 3 о 14:02:31»), які VMS може вивести на екран оператору, зберегти як метадані, зіставити з контролем доступу та надати доступ до них через пошук. Кожне розгортання вже фіксує відео; саме інтеграція робить його доступним для запитів. У таблиці нижче наведено канонічні типи аналітики, сімейство моделей, на яких базується кожен з них сьогодні, та відповідне робоче навантаження.

На практиці кожна інтеграція виконує ті самі п'ять кроків:

1. Захоплення. Камера надсилає потік запису та легший потік аналітики через RTSP (ONVIF Profile S/T).

2. Декодування та висновок. Прикордонний пристрій або сервер декодує аналітичний потік та запускає детектор плюс трекер, такий як YOLO26 з ByteTrack.

3. Застосовуйте правила. Зони, час перебування та класи об'єктів перетворюють необроблені виявлення на події («людина в зоні 3 протягом 40 с»).

4. Опублікувати. Події та обмежувальні рамки надсилаються до VMS як метадані профілю ONVIF M або через VMS SDK, а до інших систем через MQTT або вебхуки.

5. Дійте та шукайте. Оператор отримує тривогу на тій самій часовій шкалі, що й відео, а метадані стають доступними для пошуку для розслідувань.

1.2 Область застосування

Індустрія відеоспостереження переживає те, що інженери старої школи назвали б «зміною епох». Камери більше не просто записують зображення. Вони стають датчиками, а програмне забезпечення перетворюється на мозок системи безпеки. Глобальний ринок VMS та VSaaS швидко відходить від пасивної моделі запису до архітектур активного інтелекту, де аналітика на основі штучного інтелекту створює основну цінність.

Цей зсув змінює правила конкуренції. Сьогодні важлива не лише стабільність запису та підтримка протоколу, але й здатність системи витягувати сенс з відеопотоків, знижувати загальну вартість володіння та спрощувати щоденну експлуатацію.

Макроекономіка та технологічний вектор ринку

Ринок відеоспостереження зі штучним інтелектом демонструє стабільне двозначне зростання.

У вузькому сенсі, тобто в сегменті штучного інтелекту та інтелектуального відеоспостереження, ринок у 2025 році оцінювався приблизно в 5-6 мільярдів доларів і може досягти 12-18 мільярдів доларів до 2030 року.

У ширшому сенсі, якщо розглядати весь ринок відеоспостереження з функціями штучного інтелекту, вбудованими в загальну екосистему, ринок оцінюється приблизно в 74-84 мільярди доларів у 2025 році та може зрости до 148 мільярдів доларів до 2030 року.

Причини такого зростання очевидні:

– нижчі витрати на графічний процесор та периферійні обчислення;

– зростаючі вимоги безпеки;

– нестача операторів моніторингу;

– тиск бізнесу щодо зменшення збитків;

– розширення хмарних сервісів.

Основну структурну тенденцію можна сформулювати просто: ринок переходить від «відеозапису» до «відеорозвідки».

Згідно з цією логікою, сучасні платформи, включаючи SmartVision, зосереджуються на вбудованій нейромережевій аналітиці та апаратному прискоренні, що відповідає ширшому технологічному напрямку галузі.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

Cisco Meraki

Cisco Meraki пропонує широкий спектр рішень для вашої безпеки, пов'язаних з відеоспостереженням. Усі ці рішення мають спільну рису: найкраще програмне забезпечення. Програмне забезпечення Meraki оснащене потужною відеоаналітикою на базі штучного інтелекту та функціями, які відстежують виявлення руху та пошук за його допомогою.

Усі ваші камери підключені до хмари для віддаленого доступу до відео та мають вбудоване сховище, тому вам не потрібен зовнішній відеореєстратор. Їхнє програмне забезпечення завжди оновлене, а випуски функцій, оновлення прошивки та виправлення помилок завжди публікуються автоматично та без додаткової плати за наявності активної ліцензії.

Meraki також інтегрується з багатьма рішеннями, включаючи Kisi, для створення комплексного рішення безпеки для вашого офісу чи студії, яке включає контроль доступу та відеоспостереження.

Камери Meraki бувають різних форм і цін. На ринку можна знайти дешевші камери, ціна яких починається приблизно від 500 доларів, а ціна може сягати 1000 доларів за камеру. До цієї ціни потрібно додати вартість ліцензії на програмне забезпечення, яка сама по собі може становити близько 1000 доларів, проте це залежить від терміну дії ліцензії та кількості камер. Cisco Meraki пропонує безкоштовну оцінку продукту та індивідуальне ціноутворення.

Rhombus

Подібно до Meraki, Rhombus пропонує комплексне рішення безпеки, яке легко встановити та яке об'єднує всі ваші камери через хмару. Rhombus

постачається з дуже зручною панеллю керування, де ви можете в режимі реального часу відстежувати, що відбувається у вашому просторі. Їхня аналітика включає корисні сповіщення з відфільтрованими кадрами руху, облич, подій датчиків та незвичайної поведінки.

Окрім вбудованого віддаленого доступу та хмарних технологій, Rhombus має багато інноваційних функцій, включаючи розпізнавання облич та номерних знаків. Як і Meraki, вони пропонують датчики навколишнього середовища, а також камери.

Rhombus має перевагу інтеграції з кількома рішеннями, включаючи Kisi, для створення повноцінної інфраструктури безпеки для вашої компанії. Це перетворить ваш офіс на безпечний простір з передовими технологіями.

Verkada

Verkada – це третя хмарна IP-камера в нашій серії, яка постачається з цілим набором супутніх продуктів. Вони пропонують системи контролю доступу та датчики навколишнього середовища з хмарним машинним зором та штучним інтелектом. Їхнє програмне забезпечення для IP-камер Command доступне через мобільні додатки та веб-сайт.

Хоча компанія кілька років тому стала жертвою інциденту безпеки, цей витік призвів до значної перебудови всієї платформи. Відтоді Verkada зробила значні інвестиції у зміцнення своєї системи безпеки, отримавши суворі сертифікати, такі як SOC 2 Type 2 та ISO/IEC 27701, і впровадивши детальні журнали аудиту для аналізу активності користувачів.

Alta Aware (Avigilon Alta)

Хмарна система керування відео Alta Aware від Avigilon – це масштабована, інтелектуальна хмарна система безпеки, яка допомагає вам отримувати видимість та аналітику в режимі реального часу з будь-якого місця. Aware – це потужна хмарна система керування відео на основі штучного інтелекту (VMS), оснащена інтегрованими можливостями машинного навчання.

Функції, доступні в Alta Aware, включають пріоритетні режими перегляду відео, режим карти, функцію розумної присутності для перегляду

певних об’єктів та правила для створення сповіщень на основі певних камер, подій або інших критеріїв.

За допомогою Aware ви також можете швидко шукати за подією, об'єктом та схожістю, щоб знайти певну особу, транспортний засіб або подію, що вас цікавить, серед незліченних годин відео протягом кількох секунд або хвилин.

Eagle Eye

Eagle Eye Networks – американська компанія, що постачає хмарні продукти відеоспостереження для фізичної безпеки та бізнес-операцій.

Eagle Eye Cloud – це відкрита, справжня хмарна платформа, яка зберігає та керує відео. Завдяки спеціальному призначенню, Eagle Eye Cloud є ефективнішою та швидшою для відео, мінімізує затримку та забезпечує економію коштів. Її штучний інтелект навчається на основі даних систем вашого бізнесу та визначає критичні точки даних. Ви також можете отримувати сповіщення про рух у режимі реального часу та створювати персоналізовані зони виявлення для кожної камери.

Eagle Eye також інтегрується з багатьма рішеннями, включаючи Kisi, для створення комплексного рішення безпеки для вашого офісу чи студії, яке включає контроль доступу та відеоспостереження.

Корпоративна система керування відео (VMS)

Videoloft

Багатооб'єктовий відеомоніторинг Videoloft для підприємств дозволяє використовувати необмежену кількість об'єктів, камер та користувачів. Він включає резервне копіювання у хмару поза офісом та сумісний з широким спектром камер та рекордерів. Cloud Adapter Enterprise підтримує до 64 каналів камер та рекордерів для застарілих та нових систем безпеки. Їхнє хмарне рішення для відеоспостереження забезпечує віддалений доступ, аналітику та інші складні функції програмного забезпечення для відеоспостереження.

Рішення використовує жорсткі протоколи безпеки, щоб гарантувати безпечну передачу та зберігання всіх відео у хмарі Videoloft, яка розміщена на

AWS від Amazon. Кінцеві користувачі мають віддалений доступ до своєї хмарної системи відеоспостереження з будь-якого місця та в будь-який час через мобільний додаток або веб-систему управління відео (VMS). Це робить системи безпеки дуже проактивними та персоналізованими, а також миттєво оновлює застарілі системи новими функціями.

Lumana

Lumana – це постачальник рішень безпеки та відеоспостереження на базі штучного інтелекту, який пропонує передові рішення для управління відео та аналітики для підприємств та середовищ з високим рівнем безпеки. Його технологія поєднує обробку відео високої роздільної здатності з інтелектуальною автоматизацією, допомагаючи підприємствам покращити виявлення загроз, скоротити час реагування та покращити загальні операції безпеки.

Рішення Lumana розроблені для безперешкодної інтеграції з існуючою інфраструктурою безпеки, що робить їх привабливим вибором для організацій, які бажають модернізувати свої системи відеоспостереження без капітального ремонту всієї системи.

Основою пропозиції Lumana є VMS+, система керування відео наступного покоління, яка виходить за рамки традиційних можливостей VMS. На відміну від традиційних платформ, що покладаються на пасивний відеозапис, VMS+ використовує штучний інтелект для забезпечення аналітики в режимі реального часу, виявлення аномалій та автоматизованих заходів безпеки.

Система підтримує як хмарне, так і локальне розгортання, пропонуючи організаціям гнучкість в управлінні та масштабуванні своїх операцій спостереження. Завдяки інтелектуальному відстеженню руху, автоматичним сповіщенням та можливостям глибокого навчання, VMS+ перетворює відеоспостереження на проактивний інструмент безпеки, який підвищує ситуаційну обізнаність та операційну ефективність.

Lumana інтегрується із системою контролю доступу Kisi для покращення виявлення несанкціонованих входів, використовуючи відеоаналітику на базі

штучного інтелекту для виявлення несанкціонованих входів та покращення реагування та усунення наслідків безпеки.

Video Insight від i-Pro

Video Insight від i-Pro – це корпоративна система управління відео (VMS), яка використовує платформу контролю доступу MonitorCast. До її функцій входять необмежена кількість клієнтів і користувачів, автоматичне перемикання на резервний комп'ютер і моніторинг справності. Це рішення з відкритою платформою підтримує тисячі різних моделей камер.

Avigilon

Avigilon, компанія Motorola Solutions, проектує, розробляє та виробляє рішення у сфері відеоаналітики, хмарних технологій, камер безпеки, програмного та апаратного забезпечення для керування відео, а також контролю доступу. Avigilon (тепер під брендом Avigilon Unity для своїх локальних та гібридних систем) надає інтегровані рішення для відеобезпеки, контролю доступу та критично важливих комунікацій. Завдяки передовому штучному інтелекту та відеоаналітиці, Avigilon прагне зробити свої технології простими та зручними у використанні, дозволяючи вам зосередитися на найважливішому.

Як обрати найкраще рішення для вашого бізнесу

Перше рішення – чи починаєте ви з нуля, чи додаєте програмне забезпечення до вже існуючих камер, оскільки відповідь виключає половину постачальників зі списку. Хмарні платформи, такі як Verkada та Rhombus, продають свої камери та програмне забезпечення як один пакет, що спрощує розгортання та залишає одну компанію відповідальною за оновлення та підтримку. Компромісом є апаратна прив'язка, тому будь-які камери, які у вас вже є, зазвичай потребуватимуть заміни.

Якщо у вас вже є велика або змішана інсталяція, система управління відео на відкритій платформі, така як Milestone XProtect абоGenetec, дозволяє зберегти наявні камери та додати нові бренди пізніше. Ви візьмете на себе більше роботи з налаштування та часто використовуватимете локальний сервер, але інвестиції в обладнання залишатимуться захищеними в міру зростання вашої

компанії. Програмне забезпечення від виробників камер знаходиться між ними та має найбільший сенс, коли ви стандартизуєтеся на основі одного бренду.

Ціноутворення зазвичай розходиться саме на сховищі та аналітиці. Хмарні плани зазвичай оплачуються за кожну камеру на місяць залежно від того, як довго ви зберігаєте відеозапис, а це означає, що вимоги до зберігання та пропускна здатність завантаження впливатимуть на ваші витрати більше, ніж ліцензія на програмне забезпечення. Функції штучного інтелекту також не потребують нових камер, оскільки аналітичні платформи можуть працювати поверх системи, яка у вас вже є.

Зрештою, зверніть увагу на те, як система управління відеоспостереженням (VMS) підключається до решти вашої будівлі. Система, яка інтегрується з вашою системою контролю доступу, дозволяє вам зіставляти події відкриття дверей із записами, замість того, щоб шукати записи вручну, а якщо ви все ще порівнюєте обладнання, варто звернути увагу на провідні бренди камер безпеки разом із програмним забезпеченням.

Інтеграція відеоспостереження з контролем доступу

Незалежно від того, які відеокамери та програмне забезпечення ви оберете, їх поєднання з контролем доступу пропонує новий рівень безпеки для вашої власності. Така інтеграція дозволяє вам не лише контролювати активність у ваших будівлях та навколо них, але й надавати та скасовувати доступ співробітникам, гостям, відвідувачам та підрядникам.

Інші речі, які ви можете зробити, інтегрувавши свої камери з контролем доступу, включають:

– Перегляньте відеозапис на наявність подій доступу, таких як спроба проникнення з використанням зловмисника

– Аналізуйте поведінку співробітників, таку як відвідуваність

– Позначайте вразливості, які можуть призвести до порушень безпеки, таких як несанкціонований доступ відвідувачів

– Запобігання злочинній діяльності, такій як вандалізм та крадіжки зі зломом

Kisi можна інтегрувати з багатьма провідними постачальниками відеобезпеки, включаючи Rhombus, Cisco Meraki та Eagle Eye Networks, для створення комплексного рішення для відеоспостереження.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Для розробки керуючої логіки, інтеграції модулів та реалізації алгоритмів комп'ютерного зору в апаратно-програмних комплексах мережевого відеоспостереження обрано мову програмування Python. Це об'єктно-орієнтована мова високого рівня загального призначення з відкритим вихідним кодом. Її архітектурні особливості та розгалужена екосистема роблять її ефективним інструментом для швидкого прототипування і розробки програмного забезпечення.

Ключові переваги мови:

– Висока продуктивність розробки: лаконічний синтаксис та інтуїтивно зрозуміла структура дозволяють мінімізувати час на написання коду порівняно з низькорівневими мовами (наприклад, C/C++).

– Інтерпретований характер: поетапне виконання коду спрощує процес відлагодження та пошуку логічних помилок.

– Динамічна типізація: забезпечує гнучкість при маніпулюванні структурами даних під час виконання програми.

– Портативність: кросплатформність забезпечує можливість запуску написаних модулів на різних операційних системах.

– Екосистема бібліотек: наявність потужних стандартних та спеціалізованих пакетів дозволяє зосередитися на бізнес-логіці системи без необхідності реалізації базових алгоритмів з нуля.

Обмеження мови у реальному часі:

– Швидкість виконання та пам'ять: оскільки Python є інтерпретованою мовою з динамічною типізацією, «чистий» код може поступатися за швидкістю

та ефективністю використання пам'яті компільованим мовам. У задачах мережевого відеоспостереження високої інтенсивності цей чинник нівелюється шляхом винесення ресурсомістких операцій (обробка відеокадрів, детекція об'єктів) у суміжні оптимізовані бібліотеки (наприклад, OpenCV, написані на C/C++), із задіянням апаратного прискорення GPU.

Сфери застосування Python у комплексах відеоспостереження:

1. Аналіз та обробка відеоданих (Machine Learning & Computer Vision): використання нейромережевих моделей для детекції об'єктів, розпізнавання руху, класифікації подій та аналізу відеопотоків у реальному часі за допомогою бібліотек OpenCV, NumPy, PyTorch або TensorFlow.

2. Візуалізація та моніторинг: побудова графічних інтерфейсів (GUI), вебпанелей оператора та інструментів візуалізації статистики роботи комплексів за допомогою бібліотек на кшталт Matplotlib або вебфреймворків.

3. Розробка серверної частини (Backend): створення API-шлюзів для зв'язку між камерами, серверами обробки та кліентськими робочими місцями.

4. Автоматизація і скриптинг: написання сценаріїв для автоматизованого тестування, керування архівами відеозаписів, моніторингу працездатності обладнання та розгортання оновлень.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних

і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Еталонна архітектура: камера – периферія, система керування відеоспостереженням (VMS) та оператор

Кожна серйозна інтеграція використовує той самий скелет: пристрої змінюють постачальника, а протоколи залишаються на місці. Вибирайте кожен пристрій за його достовірністю, замість того, щоб купувати пакет одного постачальника, який блокує решту.

Рівень камери та гігієна RTSP

Аналітика непомітно дає збій на поганих каналах. Зафіксуйте основні параметри: NTP, синхронізований з секундою на кожній камері та сервері; ONVIF Profile S/T для потокової передачі, Profile M для метаданих; основний потік 1080p/4K для запису плюс вторинний потік 360p–720p для аналітики, щоб зменшити навантаження на графічний процесор у 3–5 разів. Вибирайте камери з вбудованим нейронним процесором або SoC на базі відеопроцесора (Axis ARTPEC-8/9, Hanwha Wisenet, Bosch INTEOX або камера Hailo-15 VPU), коли конфіденційність або затримка вимагають внутрішньокамерного виводу даних. Якщо профілі ONVIF для вас новачок, наш посібник із профілів ONVIF у системах безпеки – це простою мовою.

Вузол виведення ребер

Один або декілька периферійних серверів на сайт: NVIDIA DeepStream на Jetson Orin, прискорювач Hailo-8 M.2 (26 TOPS), розміщений в периферійному сервері з обмеженим енергоспоживанням, або сервер Intel OpenVINO для робочих навантажень лише на процесор. Конвеєр DeepStream об'єднує декодування → виявлення → відстеження → фільтр ROI → видавець подій в один графік, ефективний з використанням графічного процесора, тому ви сплачуєте вартість декодування один раз.

VMS та шина метаданих

Події повертаються до VMS як закладки або власні метадані. Milestone MIP,Genetec Security Center SDK, Avigilon Unity Video SDK (раніше ACC), Nx Witness Metadata SDK та BriefCam надають еквівалентні перехоплювачі. MQTT або вебхуки з'єднують системи сторонніх розробників: контроль доступу, панелі вторгнення, VoIP-пейджинг, оповіщення Slack або Teams. Щоб ознайомитися з самими платформами з точки зору покупця, перегляньте наш огляд систем керування відеоспостереженням.

Робоче місце оператора та склад судово-медичної експертизи

Оператор бачить події на тій самій часовій шкалі, що й запис, з можливістю відтворення одним клацанням миші та підтвердженням. Окреме сховище судово-медичної інформації (об'єктно-адресоване, з тегами зберігання, криптографічно підписане) зберігає відеозаписи доказів для слідчих. Для роботи судового рівня ми підписуємо відеозаписи токеном позначення часу та авторизації, щоб ланцюг зберігання залишався доступним для перевірки.

Edge vs. cloud vs. hybrid: рішення щодо розгортання

Три схеми розгортання охоплюють майже кожен проєкт, який ми бачимо. Правильна схема відповідає вашій пропускній здатності, бюджету затримки та конфіденційності, а не бажаному SKU постачальника.

Звертайтеся до гібридного варіанту edge + cloud, коли: у вас використовується більше кількох камер і вам потрібні як сповіщення в реальному часі менше 150 мс, так і інтенсивний судово-медичний пошук. Залишайте виявлення, відстеження та сповіщення на периферії; надсилайте до хмари лише метадані та короткі кліпи для пошуку VLM та міжсайтового зберігання.

Гібрид перемагає на практиці: периферійне обчислення обробляє виявлення, відстеження та сповіщення в реальному часі; хмара обробляє довгий хвіст, який великий VLM або величезний індекс Face ID роблять економічно вигідним у великих масштабах. Щодо інженерії затримки, що лежить в основі цього розподілу, дивіться наш посібник з периферійних обчислень.

Протоколи інтеграції та API VMS: ONVIF, RTSP, MQTT, SDK

ONVIF – це найменший спільний знаменник, що «клеїть» («клей»). Профіль S – це потокова передача, Профіль T – розширена потокова передача з H.265 та подіями обробки зображень, ПрофільG – це сховище на периферії, а Профіль M, який тут має значення, – це стандартна схема для метаданих (обмежувальні рамки, класифікації, зони). Потоки подій використовують службу подій ONVIF; багато сучасних VMS використовують Профіль M без спеціального коду.

RTSP передає відео, на якому працює аналітика; RTMP призначений лише для застарілого отримання даних.

MQTT – це шина подій для гетерогенних парків пристроїв Інтернету речей та відеоспостереження – легка, зручна для автентифікації та з урахуванням QoS.

Вебхуки – це найшвидший шлях до систем контролю доступу та пейджингу.

VMS SDK. Milestone MIP є найбагатшим: архітектура плагінів, точки розширення інтерфейсу користувача, метадані на часовій шкалі, перехоплення агентів запису.Genetec Security Center SDK посідає друге місце завдяки тісній інтеграції єдиної безпеки. Avigilon Unity Video SDK (раніше ACC), Nx Witness Metadata SDK, BriefCam API, Hanwha Wisenet SDK та Dahua DSS API покривають решту.

Як інтегрувати API із системою керування відео? Ви надсилаєте кожне виявлення аналітики до VMS як подію, яку VMS вже розуміє, а потім зіставляєте цю подію з тривогою або закладкою на часовій шкалі камери. Кожна велика VMS має задокументований спосіб зробити це; таблиця показує, де аналітичні події потрапляють у кожну з них, як задокументовано постачальниками у 2026 році.

Які постачальники мають найширшу інтеграцію зі сторонніми розробниками? Milestone таGenetec мають найбільші партнерські екосистеми для аналітичних плагінів; Nx Witness є найбільш відкритим для користувацьких

плагінів за нижчою вартістю ліцензії. Хмарні продукти VMS інтегруються найшвидше, але дають вам найменший контроль над тим, де зберігається відео. Спочатку виберіть VMS, а потім створіть рівень аналітики навколо її найсильнішої поверхні інтеграції; якщо вам потрібно написати та підтримувати цей рівень, наша команда розробників програмного забезпечення для розпізнавання відео на основі штучного інтелекту створює плагіни виявлення, відстеження та VMS на YOLO26, RT-DETR, ByteTrack та Jetson.

Зовнішні джерела, які варто додати до закладок: специфікації профілю ONVIF для схеми метаданих та документація Ultralytics YOLO11 для детектора, з якого починається більшість граничних конвеєрів.

Стек моделей штучного інтелекту 2026 року для спостереження

Виявлення об'єктів. YOLO26 (Ultralytics; попередній перегляд у вересні 2025 р., випуск 14 січня 2026 р.) – це поточний стандарт, орієнтований на периферію: комплексний редизайн без NMS, який працює до ~43% швидше на процесорі, ніж YOLO11, який досі є найпоширенішим детектором у цій галузі. RT-DETR – це альтернатива трансформатору, коли важлива точність виявлення малих об'єктів.Grounding DINO додає виявлення з відкритим словником («знайти людей у синіх капелюхах») без спеціального навчання.

Відстеження. ByteTrack та BoT-SORT – це налаштування за замовчуванням у 2026 році; DeepSORT все ще підходить там, де простота переважає точність; StrongSORT додає функції зовнішнього вигляду для переповнених сцен.

Повторна ідентифікація. OSNet та TransReID вбудовують особу у вектор, який витримує переходи між камерами, що є основою робочих процесів «знайти цю людину по всьому кампусу».

Семантичний та судово-медичний пошук. Вбудовування CLIP плюс векторне сховище (pgvector, Weaviate, Pinecone) дозволяють шукати кліпи простою мовою. Додайте VLM (GPT-класу Vision,Gemini, Claude Vision) для перевірки людиною в циклі, яка пояснює, чому кліп збігається.

Перевірка сповіщень VLM (нова версія 2026 року). Найшвидше розвивається цей рік, і між детектором та оператором розташований шар: модель візуальної мови спостерігає за кліпом за кожним сповіщенням і позначає його як реальне або хибне, перш ніж людина його побачить. План 3.1 для пошуку та підсумовування відео NVIDIA (документація оновлена в липні 2026 року) постачає службу перевірки сповіщень, яка позначає сповіщення вище за течією як підтверджені, відхилені або неперевірені за допомогою Cosmos Reason або Qwen3-VL, а Milestone додала відеозведення на основі Cosmos Reason до XProtect у 2026 році. Залиште детектор як тригер і використовуйте VLM як другу думку; це занадто повільно та занадто дорого для запуску на кожному кадрі.

Сегментація. SAM 3 (Meta, листопад 2025 р.) – це стандартна версія, коли маски на рівні пікселів мають значення (підрахунок покинутих об'єктів, транспортних засобів); вона додає сегментацію концепцій з підказками та відстеження об'єктів у відео, тому текстова підказка повертає кожен відповідний екземпляр. Поєднайте її з детектором, а не запускайте її на кожному кадрі.

3.2 Розробка структурної схеми

Сегментація ринку VMS та VSaaS

Глобальний ринок програмного забезпечення для відеоспостереження можна умовно розділити на три основні кластери, кожен з яких має свою економіку, аудиторію та технологічні компроміси.

Сегмент SOHO, SMB та DIY

Цей сегмент обслуговує:

- приватні будинки;
- малий бізнес;
- технічно кваліфіковані користувачі.

Блакитний ірис історично вважався фактичним стандартом серед рішень для самостійного ремонту.

Сильні сторони сегмента

Платформи для самостійного виготовлення популярні з очевидних причин:

- низька вартість входу;
- висока гнучкість;
- велика спільнота користувачів;
- детальне ручне налаштування.

Вони добре підходять для ентузіастів, які готові витрачати час на налаштування.

Обмеження самостійного підходу

Однак, зі зростанням бізнес-вимог починають проявлятися системні слабкі місця:

- високе навантаження на процесор;
- складне налаштування ШІ за допомогою плагінів;
- нестабільність при масштабуванні;
- необхідність ручного переадресації портів;
- обмежені хмарні можливості.

Сегмент корпоративних VMS

Це найважча класова система в галузі. Ці системи були розроблені для:

- аеропорти;
- загальноміські системи;
- промислові об'єкти;
- критична інфраструктура.

Сильні сторони корпоративних рішень

Платформи корпоративних VMS залишаються стандартом де-юре у великомасштабних проектах завдяки:

- масштабованість;
- зріла екосистема;
- розгалужену партнерську мережу;
- сертифікації та відповідність вимогам;

- глибока інтеграція обладнання.

Обмеження корпоративного підходу

Але класичне підприємництво має свою ціну, і не малу:

- висока сукупна вартість володіння;
- дороге ліцензування на канал;
- складність розгортання;
- довгі цикли продажів;
- надмірна функціональність для середнього бізнесу.

У багатьох сценаріях малого та середнього бізнесу такі системи виглядають як поїзд, побудований для перевезення однієї сумки.

Водночас, корпоративні платформи залишаються сильнішими у масштабних інтеграційних проектах та глобальних партнерських екосистемах.

Сегмент хмарного VSaaS

Це найшвидше зростаючий сегмент ринку завдяки низькому порогу входу.

Чому бізнес любить хмарні технології

Причини легко зрозуміти:

- швидкий старт;
- не потрібна місцева інфраструктура;
- віддалений доступ;
- модель передплати;
- мінімальне налаштування.

Для малого бізнесу це часто найпростіший шлях.

Системні обмеження хмарної моделі

Однак, у міру масштабування розгортань починають виникати проблеми:

- велике навантаження на інтернет-канал;
- зростання вартості трафіку;
- залежність від хмарного провайдера;
- проблеми конфіденційності;
- прив'язка до постачальника.

Технологічні тенденції, що формують ринок

Штучний інтелект стає базовою функцією

Якщо раніше відеоаналітика була преміум-опцією, то сьогодні вона стає мінімальною вимогою.

Ринок зараз очікує, що сучасна система управління відеоспостереженням (VMS) забезпечить:

- виявлення об'єктів;
- розпізнавання обличчя;
- класифікація транспортних засобів;
- поведінкова аналітика;
- аудіо аналітика.

Перехід до гібридних архітектур

Чиста хмара виявилася не універсальним рішенням. Бізнеси все частіше обирають гібридні моделі.

Причини такі:

- контроль даних;
- менше споживання трафіку;
- краща стійкість до невдач;
- передбачувана загальна вартість володіння (TCO).

Гібридна модель SmartVision добре вписується в цю макротенденцію та відображає загальні зміни в галузі.

Зростаюча роль графічного процесора та апаратного прискорення

Вища роздільна здатність, більша кількість камер та складніші робочі навантаження штучного інтелекту роблять підходи, що базуються виключно на процесорі, все менш ефективними.

Сучасні платформи VMS все частіше використовують:

- апаратне декодування;
- висновок на графічному процесорі;
- обробка країв.

Спрощення віддаленого доступу

В останні роки вимога користувачів звучала однаково в кожній країні: «зробіть так, щоб це працювало без гімнастики NAT».

Безперебійний віддалений доступ без переадресації портів зараз розглядається як критично важлива функція для масового ринку.

Рішення, що потребують ручної налаштування мережі, поступово втрачають позиції.

Моделі ціноутворення на ринку VMS зазнають не меншої трансформації, ніж сама технологія.

Традиційна модель підприємства:

- ліцензування для кожного каналу;
- окремі платні модулі;
- платні оновлення;
- дорога підтримка.

Натомість новіші гравці використовують пакетні ціни.

Типовий приклад позиціонування:

- безкоштовний рівень для однієї камери;
- фіксовані пакети для кількох камер;
- розширені функції в планах вищого рівня.

Ця модель часто є привабливішою, ніж ліцензування на канал, особливо для клієнтів малого та середнього бізнесу.

Глобальний ринок програмного забезпечення для відеоспостереження переходить від ери пасивного запису до ери інтелектуальної аналітики. Зростаюче робоче навантаження на штучний інтелект, зростання вартості хмарного трафіку та тиск бізнесу щодо зниження загальної вартості володіння створюють попит на нові архітектурні підходи.

У кожному з ключових сегментів все ще є сильні гравці:

- Саморобні рішення домінують завдяки інерції встановленої бази.
- Корпоративні платформи зберігають великі проекти.
- Хмарний VSaaS продовжує зростати завдяки простоті.

Однак, водночас, з'являється новий клас гібридних платформ VMS наступного покоління.

Технологія розумної аналітики на основі штучного інтелекту перетворює відеоматеріали на великі дані

Використання штучного інтелекту є одним із трендів відеобезпеки 2026 року. ШІ дозволяє перетворювати години раніше надлишкових відеоматеріалів на дані, які потім можна аналізувати на предмет тенденцій та закономірностей відеобезпеки. Раніше команди безпеки навчалися на інцидентах, ідентифікованих вручну. Тепер вони можуть дізнатися більше з годин невикористаного відео, яке раніше пропускали. Завдяки цій цінній інформації все більше компаній бачать необхідність впровадження відеоаналітики на основі штучного інтелекту та відповідно складають бюджет.

Однією з найважливіших тенденцій цього року в галузі комерційних камер безпеки є використання технології відеоаналітики для створення великих даних. Нижче наведено деякі фактори, що сприяють її зростанню.

Глибоке навчання та аналітика

Глибоке навчання – це відносно нова технологія камер безпеки та одна з останніх тенденцій у сфері камер безпеки, яку впроваджують основні виробники в галузі комерційних камер безпеки.

Відеоаналітика на основі штучного інтелекту використовує передове програмне забезпечення для розуміння того, що відбувається на відеоматеріалах. Вона може автоматично ідентифікувати людей, об'єкти та транспортні засоби в режимі реального часу, подібно до того, як наш мозок розпізнає знайомі об'єкти. Ця технологія дозволяє сучасним камерам безпеки не просто записувати відео; вони тепер можуть аналізувати його, щоб виявляти потенційні проблеми та надавати цінну інформацію.

Завдяки можливостям глибокого навчання технологія відеоспостереження може поступово покращувати виявлення стимулів у певних місцях. Чим довше система аналізує цільову область, тим більше вона звикає до звичайної активності та тим послідовніше може виявляти аномалії.

Щоб зрозуміти, чому глибоке навчання та відеоаналітика є основними трендами відеобезпеки у 2026 році, може бути корисним визначити їхні ключові переваги:

– Покращене прийняття рішень: дані, отримані за допомогою технології глибокого навчання та відеоспостереження, можуть допомогти командам підтвердити або спростувати теорії щодо подій безпеки, виступаючи в якості підкріпленого даними довідника для інформування про ефективність реагування на події та вдосконалення системи.

– Підвищена ефективність: програмне забезпечення для глибокого навчання може безперервно контролювати цільову область необмежений час без зниження точності виявлення, що дозволяє командам зосередитися на складніших проблемах та ефективніше використовувати ресурси.

– Підвищена точність виявлення: оскільки інструменти аналітики на основі штучного інтелекту розпізнають загрози на основі достовірних даних та моделей поведінки, які можна довести, на їхню точність не впливають відволікаючі фактори чи непереконливі докази, що дозволяє постійно точно виконувати операції безпеки.

– Можливості інтеграції та автоматизації: технологію камер безпеки на базі штучного інтелекту можна інтегрувати з пристроями безпеки, такими як датчики, сигналізації та зчитувачі доступу, для підтримки автоматизованих реакцій. Це дозволяє всім системам безпеки отримувати вигоду від технології глибокого навчання.

Хоча передові технології відеоспостереження у 2026 році виграють від таких тенденцій, як глибоке навчання та аналітика штучного інтелекту, фахівці з безпеки та моніторинг відеоспостереження навряд чи будуть замінені такими інструментами. Штучний інтелект доречніше розглядати як допоміжну технологію, що надає командам людей додаткову можливість точно аналізувати та отримувати інформацію про події безпеки.

Периферійні обчислення

Зростання периферійних обчислень є важливим технологічним зрушенням у галузі камер безпеки та ключовим трендом відеоспостереження 2026 року. Периферійні обчислення стосуються систем, які виконують функції на пристрої, а не на окремому сервері, що дозволяє генерувати високоякісну аналітику з меншою затримкою.

Що стосується технології камер спостереження, периферійні системи використовують аналітику відеокамер для обробки відеоданих у момент запису, що дозволяє співробітникам служби безпеки краще розуміти події в режимі реального часу завдяки передовій аналітичній обробці швидко, точно та надійно.

Нижче наведено деякі ключові переваги цієї останньої тенденції в технології відеоспостереження :

– Зменшена затримка: периферійні системи обробляють відео на камері, використовуючи інструменти аналітики для виявлення кадрів, які можуть потребувати перевірки людиною. Такий робочий процес означає, що менше даних потрібно надсилати до окремих систем, що покращує швидкість передачі даних і зменшує затримку.

– Підвищена ефективність використання пропускної здатності: оскільки технологія периферійного відеоспостереження обробляє дані локально, передавані дані упаковуються ефективніше, що допомагає зменшити використання пропускної здатності.

– Швидше реагування на інциденти: аналіз на пристрої за допомогою периферійних обчислень дозволяє набагато швидше запускати сповіщення та автоматизовані відповіді, що покращує час реагування.

– Покращена конфіденційність даних: чим більше даних обробляється на пристрої, тим менше їх потрібно надсилати кудись ще, що усуває можливості перехоплення конфіденційної інформації.

Периферійні обчислення знаходяться на передовій новітніх тенденцій у технології камер відеоспостереження, а переваги обробки даних на пристрої підтримують інновації в ширших технологіях спостереження. Як видно з ролі

відеоспостереження у зниженні злочинності у Великій Британії, периферійний аналіз, ймовірно, вплине на майбутні інновації у сфері відеоспостереження, оскільки він стане більш поширеним.

Хмарні технології змінюють те, як компанії керують відеобезпекою

Однією з тенденцій у сфері камер безпеки у 2026 році є зростання хмарних технологій у сфері безпеки, зокрема у відеоспостереженні. Перехід до хмарних технологій дає підприємствам можливість гнучко та масштабовано розвиватися майже в усіх сферах, включаючи фінанси, найм та дистрибуцію. Що стосується комерційної безпеки, то тенденції у сфері камер також сильно залежать від хмарних технологій.

Хмарні сервери та« Програмне забезпечення як послуга»

Перенесення послуг відеоспостереження в хмару продовжує бути популярною тенденцією в індустрії камер безпеки, що дозволяє компаніям розробляти гнучку, надійну та доступну IT- інфраструктуру. Зі зростанням популярності хмарних сервісів зростає і модель «Як послуга» (AaS), яка дозволяє організаціям передавати трудомісткі процеси на аутсорсинг перевіреним та надійним постачальникам послуг.

Як хмарні сервіси та моделі AaS враховують останні тенденції в технології відеоспостереження та нові технології камер спостереження? Відповіді криються в ключових перевагах цих рішень:

– Підвищена гнучкість: пакети AaS можна вільно налаштовувати в будь-який час, щоб найкращим чином відповідати мінливим бізнес-потребам, що дозволяє командам посилювати або скорочувати різні ключові аспекти систем спостереження у відповідь на поточні потреби та відповідні дані.

– Спрощене масштабування: Фактичний процес масштабування інфраструктури технологій відеоспостереження також спрощується в рамках хмарних моделей AaS, оскільки постачальники послуг можуть налаштовувати параметри активних систем відповідно до потреб бізнесу.

– Автоматичні оновлення: Завдяки автоматичним оновленням, що виконуються постачальниками послуг, компанії можуть забезпечити

використання найновіших технологій камер відеоспостереження та кібербезпеки у своїх робочих процесах, що зменшує навантаження на внутрішні команди.

– Оптимізовані витрати: За моделлю AaS компанії платять лише за те, що їм потрібно, а поточні витрати, пов’язані з оновленнями та обслуговуванням, включені в основну плату за підписку.

Мережі Інтернету речей

Інсталяції Інтернету речей (IoT), мережі фізичних пристроїв, підключених через Інтернет, були задіяні в багатьох тенденціях систем безпеки та технологій відеоспостереження в останні роки, однією з останніх є міграція операцій безпеки до Wi-Fi та хмарних сервісів.

Усунувши деякі обмеження, пов'язані з дротовою інфраструктурою безпеки, команди можуть швидко та ефективно встановлювати камери в ширшому діапазоні місць, що забезпечує такі ключові переваги, як:

– Оптимізоване управління: технології відеоспостереження, встановлені на кількох об'єктах, можна переглядати та аналізувати з централізованої хмарної платформи управління, що забезпечує цілісне уявлення про події безпеки в усій мережі безпеки бізнесу.

– Віддалений доступ: Сучасні мережі Інтернету речей підтримують швидку передачу HD- даних через Інтернет, причому багато постачальників послуг пропонують спеціальні мобільні додатки, які дозволяють користувачам переглядати та налаштовувати активні пристрої дистанційно в будь-який час.

– Аналітика в режимі реального часу: Можливість доступу до потоків даних камер через хмару підтримує збір та аналіз даних у режимі реального часу, а також налаштовувані сповіщення безпеки надсилаються на смарт-пристрої користувачів, щоб забезпечити оперативне реагування на інциденти цілодобово.

Інтегруючи технології безпеки, управління будівлями та відеоспостереження в рамках спеціально розробленої інсталяції Інтернету речей, керівники підприємств можуть допомогти забезпечити відповідним

зацікавленим сторонам послідовний, надійний та безпечний доступ до загальнокорпоративного огляду ключових операцій безпеки.

Конвергенція фізичної безпеки та кібербезпеки

Хоча міграція до хмарних сервісів може принести кілька переваг, об'єднання важливих систем безпеки може виявити нові вразливості. Якщо хмарна інфраструктура не надійно захищена, порушення в одній системі може поширитися на кілька мереж. Щоб зменшити цей ризик, багато компаній надають пріоритет практикам конвергенції фізичної безпеки та кібербезпеки.

Деякі основні переваги конвергенції фізичної та кібербезпеки у 2026 році включають:

– Краща хмарна безпека: Завдяки об'єднанню фізичних систем та систем кібербезпеки, команди можуть краще захистити технологію фізичних камер безпеки від кібератак, що здійснюються через хмару, зменшуючи ризик віддаленого злому камер.

– Посилена безпека даних: Забезпечення фізичного та кіберзахисту всіх систем допомагає компаніям усунути вектори витоків даних, причому ця практика особливо важлива в системах, де дані регулярно передаються між пристроями.

– Надійні оновлення системи: Поєднання практик фізичної та кібербезпеки надає IT- командам чіткіше уявлення про поточний стан усіх пристроїв безпеки, що дозволяє їм забезпечити регулярне оновлення всіх рішень для боротьби з новими загрозами безпеці.

– Цілісне реагування на загрози: Поєднання фізичної інформації та інформації про кібербезпеку в рамках конвергентної інфраструктури дозволяє командам аналізувати результати обох практик, покращуючи свої можливості виявлення аномалій в одній системі, які згодом можуть вплинути на інші.

Конвергенція фізичної та кібербезпеки, ймовірно, залишатиметься основною тенденцією відеоспостереження у 2026 році та надалі, особливо для організацій, які впроваджують IP- пристрої безпеки. Пристрої з віддаленим доступом, такі як IP-камери, потребують як фізичного, так і кіберзахисту для

безпечної та ефективної роботи, а це означає, що конвергентні команди повинні контролювати їх.

Постійний попит на IP- камери порівняно з аналоговими

Оскільки компанії в галузі камер безпеки та технологій відеоспостереження переносять свою діяльність у хмару та інвестують у нові технології, такі як штучний інтелект, логічно, що вони оберуть пристрої, які вписуються в цю нову екосистему. Аналогові камери, які передають необроблені відеосигнали через коаксіальний кабель, не пропонують такої ж простоти інтеграції. Хоча можна покращити застарілі аналогові камери за допомогою новіших технологій відеоаналітики, багато компаній переходять на мережеві IP-камери.

При порівнянні переваги IP над аналоговими стають очевидними. Наприклад, якість відео набагато вища. Роздільна здатність зображення в IP-камері може бути від шести до 20 разів вищою, ніж у аналогової камери, що забезпечує ширші зони огляду та набагато більше деталей під час збільшення.

IP- камери передають відео у цифровому форматі, який зазвичай має кращу якість. Ризик погіршення якості на великих відстанях значно зменшується, якщо сигнал передається через Wi-Fi, а не через кабелі. Найновіші технології камер відеоспостереження зосереджені на вдосконаленні камер відеоспостереження, таких як IP- камери з поворотом, нахилом та масштабуванням, щоб зробити їх ще розумнішими в різних аспектах.

5G у технології відеоспостереження

Впровадження камер із підтримкою 5G стає помітною тенденцією в галузі безпеки. Завдяки можливості надсилати аудіо- та відеодані через високошвидкісні мережі Wi-Fi, ці стільникові пристрої обіцяють більшу ємність, вищу якість відео та надійніший сигнал, ніж аналогічні застарілі технології.

Очікується, що технологія 5G у відеоспостереженні дедалі більше впроваджуватиметься, частково завдяки таким перевагам:

– Швидша швидкість передачі даних: стрибок у швидкості завантаження та вивантаження між мережами 4G та 5G є значним, причому перша до 100 разів

швидша, а друга – до 30 %, що дозволяє службам безпеки ефективніше обмінюватися відеозаписами та аналізувати їх.

– Покращена якість відео: швидше та стабільніше з’єднання 5G забезпечує плавну потокову передачу відео з низькою затримкою на кількох пристроях віддаленого доступу.

– Більша пропускна здатність мережі: мережі 5G можуть підтримувати до 100 разів більше трафіку, ніж мережі 4G, що дозволяє стабільніше забезпечувати стабільні з'єднання.

– Розширені функції безпеки: Оскільки мережі 5G є найновішим поколінням бездротових технологій, пристрої з підтримкою 5G отримують вигоду від найновіших функцій та оновлень безпеки.

Зі зростанням доступності 5G буде розроблено більший вибір камер відеоспостереження, інтеграцій та додатків з підтримкою 5G для комерційних установок. Оскільки новітні технології камер відеоспостереження адаптовані для підтримки сумісності з 5G, також дуже ймовірно, що камери та мобільні додатки 5G стануть ще ефективнішими та зручнішими для користувачів.

Нова енергоефективна технологія камер спостереження

Найновіші технології відеоспостереження, особливо ті, що використовують зображення високої роздільної здатності та відеоаналітику за допомогою штучного інтелекту, споживають велику кількість енергії для роботи. Оскільки енергоефективність, зелені технології та зниження витрат є ключовими пріоритетами для бізнесу, очікується, що однією з тенденцій відеоспостереження на 2026 рік стане прагнення до екологічно чистих рішень для відеоспостереження.

За даними Міжнародного енергетичного агентства, між 2023 і 2026 роками світовий попит на енергію зростатиме прискореними темпами порівняно з попередніми роками. Тому організації звертаються до:

– Відеонагляд на сонячних батареях: для зменшення залежності від традиційних джерел енергії

– Енергозберігаючі датчики: які запускають запис за потреби

– Екологічні матеріали: використовуються для створення обладнання для відеоспостереження

– Бездротові рішення: для мінімізації монтажних та матеріальних відходів

Такі рішення не лише дозволяють значно заощадити кошти, але й доповнюють ініціативи щодо сталого розвитку, які окреслили багато організацій, використовуючи вуглецево чисту енергію для забезпечення своїх операцій.

Інтеграція камер безпеки з IT- інфраструктурою

Нові технології спостереження та тенденції камер безпеки 2026 року свідчать про те, що багато організацій зараз надають пріоритет багатофункціональним системам безпеки, які пропонують підвищену гнучкість, віддалений доступ та зручне керування. Оскільки кілька компаній переводять більше основних операцій в онлайн, команди безпеки також звертаються до програмних та апаратних систем з хмарною синергією.

Для ефективної підтримки цих цілей здійснюється інтеграція між ключовими пристроями безпеки, такими як камери, зчитувачі доступу та сигналізації, що вимагає безперешкодної інтеграції IT- інфраструктури з установками відеоспостереження. Якщо установники комерційних камер безпеки приділять час плануванню та впровадженню інтегрованих систем безпеки, можна отримати значні організаційні переваги:

– Оптимізовані операції: Інтеграція між камерами безпеки та ширшими системами дозволяє обмінюватися даними між різними практиками, допомагаючи командам оптимізувати операції, спрямувавши інформацію в режимі реального часу на єдину централізовану платформу управління безпекою.

– Спрощені налаштування: Коли системи безпеки та управління будівлями налаштовані для підтримки інтегрованих операцій, додавання нових технологій та робочих процесів до базової інфраструктури може бути спрощено, що дозволяє гнучко коригувати їх відповідно до потреб, що змінюються.

– Розширені системні можливості: ключові функції камер безпеки можна автоматизувати та розширити завдяки інтеграції з ширшими технологіями. Наприклад, камери можна запрограмувати на автоматичний запис та позначення відеоматеріалів залежно від спрацьованих датчиків.

– Ефективне управління будівлею: Системи відеоспостереження можуть запропонувати ширші переваги управління будівлею як частина інтегрованого рішення, завдяки відеоаналітиці, яка аналізує такі показники, як заповнюваність, для інформування про роботу освітлення та систем опалення, вентиляції та кондиціонування повітря.

Оскільки компанії продовжують випробовувати різні типи та комбінації технологій відповідно до тенденцій безпеки та відеоспостереження у 2026 році, інтегровані системи, ймовірно, стануть більш поширеними, а можливість інтеграції різних технологій стане безцінним заняттям.



Рисунок 3.1 – Структурна схема системи

Сумісна технологія відеоспостереження

В останні роки такі країни, як США, заборонили використання технологій деякими китайськими виробниками в системах безпеки для державних органів та агентств, що підкреслило потенційні вразливості в їхній продукції.

З впровадженням таких законів, як NDAA, та поширенням аналогічних норм на такі країни, як Велика Британія, Канада та деякі країни ЄС у 2026 році, багато урядових організацій та приватних компаній шукають надійні, кібербезпечні рішення, які відповідають національним та галузевим нормам і стандартам. Це одна з ключових тенденцій відеоспостереження на 2026 рік.

Поряд із цим також спостерігається рух до нової технології камер безпеки на базі штучного інтелекту, яка відповідає етичним обов'язкам бізнесу. Закон ЄС про штучний інтелект та канадський законопроект С- 27 тепер визначають, що штучний інтелект має використовуватися відповідально, з вичерпними журналами аудиту та поясненнями рішень на основі відео.

Організації в ЄС, Канаді та потенційно інших країнах, які в майбутньому запровадять аналогічні правила, повинні продемонструвати відповідність вимогам під час впровадження технології відеоспостереження на базі штучного інтелекту. Як результат, підприємства шукають рішення на основі штучного інтелекту, які надають чітку та лаконічну інформацію про те, як ця технологія використовується в їхніх операціях з безпеки.

3.3 Розробка функціональної схеми

Розроблене програмне забезпечення призначене для функціонування в складі апаратно-програмного комплексу мережевого відеоспостереження, що забезпечує безперервний (24/7) контроль і патрулювання охоронюваного простору. Система інтегрує сучасні IP-камери та модулі комп'ютерного зору з апаратним прискоренням, що дозволяє виконувати високодеталізований аналіз відеопотоків у реальному часі.

Згідно з інженерними вимогами до охоронних комплексів, у системі реалізовано підтримку як стандартних, так і професійних (зовнішніх і внутрішніх) камер. Зовнішні модулі оснащені захисними антивандальними корпусами, вологозахистом та системами автоматичного підігріву для стабільної роботи в умовах низьких температур. Також передбачено підтримку та правове регулювання використання спеціалізованих (прихованих) засобів відеоконтролю для захисту власності та контролю доступу з дотриманням чинного законодавства України (зокрема ст. 307 ЦК України).



Рисунок 3.2 – Функціональна схема системи

Функціональна структура комплексу

Архітектура розробленої системи побудована на базі оригінальних алгоритмів спільного калібрування камер та виділення областей інтересу (ROI). Функціональна схема комплексу поділяється на три ключові блоки за ролями користувачів:

1. Блок функцій адміністратора. Відповідає за адміністрування та конфігурацію параметрів безпеки:

– додавання нових користувачів та розмежування прав доступу;

– контроль загальної конфігурації комплексу та керування системними ресурсами.

2. Блок функцій оператора. Забезпечує щоденний моніторинг та оперативне реагування на події:

– Перегляд відеоряду з підключених камер у режимі реального часу.

– Оцінка ситуації за двовимірним планом: візуалізація зон видимості камер, доданих об'єктів та автоматично виявлених порушень у контрольованому просторі (з можливістю виявлення «сліпих зон», не охоплених жодною камерою).

– Керування камерами: зміна ракурсів та панорамування за допомогою кліків мишею по відеопотоку або інтерактивній карті, активація режимів автоматичного супроводу рухомих об'єктів.

– Зміна оперативних налаштувань системи.

3. Блок функцій інженера. Призначений для первинного розгортання, калібрування та обслуговування інфраструктури:

– завантаження та калібрування двовимірного плану контрольованого простору;

– додавання та редагування заборонених зон на карті;

– інтеграція нових об'єктів і маркування контрольних точок;

– калібрування камер: виконання процедур просторового узгодження за допомогою розроблених методів спільного калібрування;

– додавання, конфігурація або видалення мережевих камер.

Завдяки реалізації розширеного графічного інтерфейсу та алгоритмам автоматичного калібрування, система забезпечує вищу ефективність порівняно з традиційними комплексами на базі нерухомих камер, мінімізуючи вплив людського фактора під час моніторингу складних об'єктів.

3.4 Розробка діаграми процесів

На рисунку 3.3 наведено діаграму потоків даних розробленої системи, детальний розгляд якої дозволяє простежити логіку взаємодії її функціональних компонентів. У процесі проєктування використовується структурний підхід та графічне представлення інформаційних потоків у системі (Data Flow Diagram, DFD), що дає змогу ефективно візуалізувати процеси обробки та передачі даних між мережевими камерами, модулями апаратного прискорення та сервером аналізу відеопотоків.

Згідно з інженерною методологією, розробка розпочинається з побудови контекстної діаграми (діаграми нульового рівня), яка визначає глобальні межі системи та її інтерфейси із зовнішнім середовищем. Надалі ця модель підлягає ітераційній декомпозиції шляхом деталізації базових процесів та потоків даних з метою повного відображення архітектури розроблюваного комплексу.

Складені діаграми потоків даних базуються на чотирьох основних типах елементів:

– Процеси – функціональні перетворення даних у межах описуваної системи (наприклад, захоплення відеопотоку, апаратне детектування об'єктів, розрахунок траєкторій та оновлення стану плану приміщень).

– Сховища даних (репозиторії) – структуровані бази даних для збереження відеоархівів, логів подій та калібрувальних матриць камер.

– Зовнішні сутності – джерела та споживачі інформації поза межами системи (оператори, адміністратори, зовнішні охоронні датчики).

– Потоки даних – канали передачі інформаційних масивів (відеокадри, керуючі команди, координати об'єктів) між попередніми трьома типами елементів.



Рисунок 3.3 – Діаграма взаємодії процесів

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Функціонування апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу ґрунтується на послідовному виконанні операцій приймання, декодування, попереднього оброблення та інтелектуального аналізу відеоданих. Основним завданням алгоритмічного забезпечення є автоматизоване виявлення об'єктів і подій у контрольованих зонах із мінімізацією затримки між отриманням відеокадру та формуванням результату аналізу. Для цього необхідно узгодити роботу мережевих камер, серверного обладнання, апаратних засобів прискорення обчислень і програмних модулів комп'ютерного зору.

Загальну послідовність функціонування комплексу відображає основна блок-схема програми на рисунку 4.1.

Програмна архітектура передбачає розподіл функцій між підсистемою отримання відеопотоків, модулем апаратного декодування, компонентом нейромережевого аналізу та сервером керування результатами спостереження. Мережеві камери передають стиснені відеодані через IP-мережу. Серверна частина приймає потоки, виконує декодування кадрів і передає підготовлені зображення до обчислювального модуля. Результати аналізу використовуються для визначення положення об'єктів, встановлення їхньої належності до заданих категорій та реєстрації контрольованих подій. Окремий компонент відповідає за збереження відеоархіву й метаданих, необхідних для подальшого перегляду.

Особливістю запропонованого рішення є використання апаратного прискорення на декількох етапах відеооброблення. Декодування стиснених даних може виконуватися спеціалізованими апаратними блоками графічного процесора

або медіаприскорювача. Обчислення нейронної мережі можуть передаватися графічному процесору чи іншому сумісному прискорювачу. Це дозволяє відокремити ресурсоємні операції від загальної логіки керування системою. Однак наявність графічного адаптера сама по собі не гарантує апаратного прискорення всіх етапів. Необхідно перевірити підтримку відеокодеків, сумісність драйверів, середовища виконання нейронної мережі та фактичне розміщення обчислень.

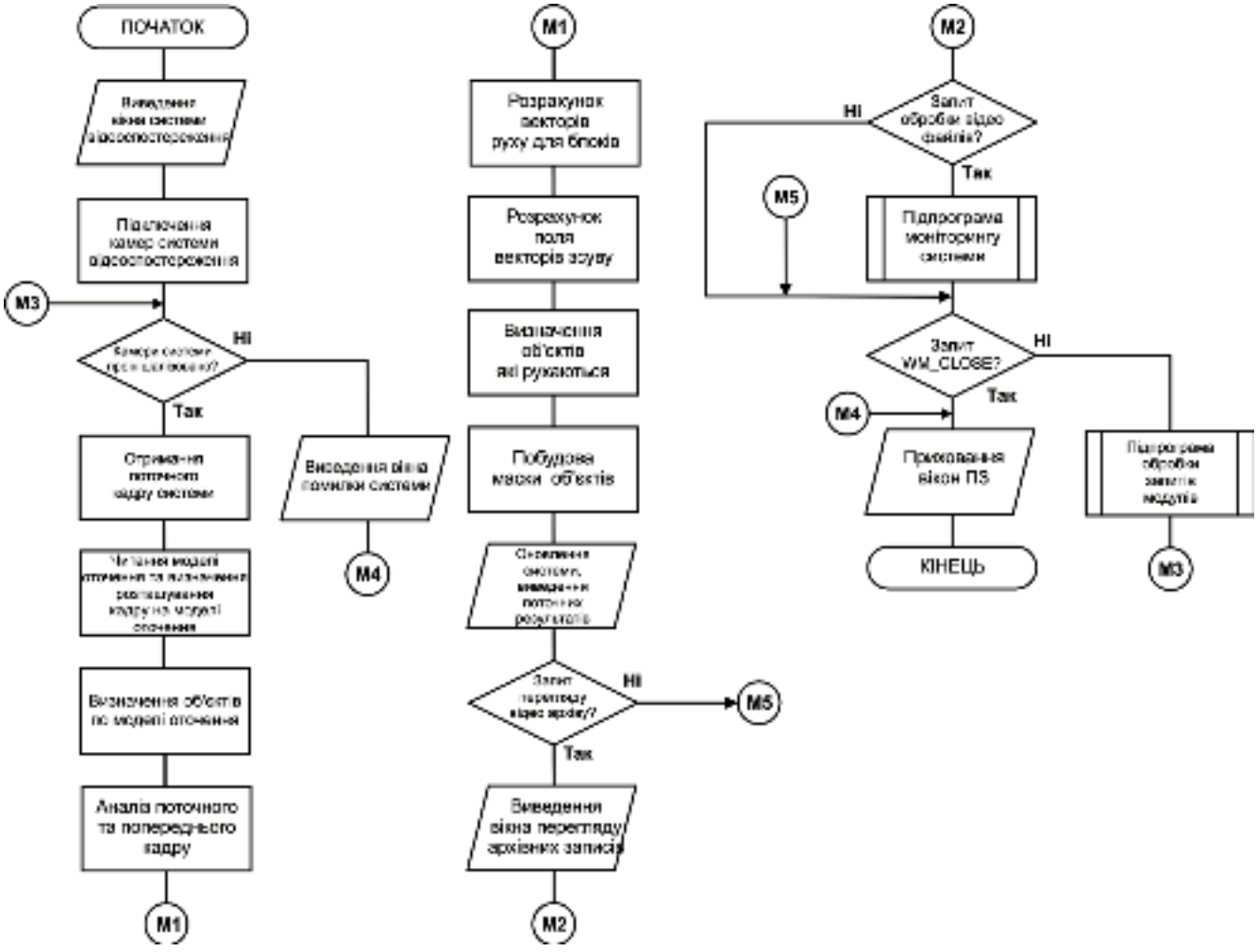

Рисунок 4.1 – Блок-схема основної програми

Одним із основних алгоритмічних завдань є підтримання актуальності відеокадрів. Під час одночасного отримання декількох потоків швидкість надходження даних може перевищувати можливості обчислювальної підсистеми.

Якщо всі кадри накопичуються в необмеженій черзі, затримка аналізу поступово збільшується.

Для запобігання цьому необхідно застосовувати обмежену буферизацію, контролювати вік кадру та визначати допустиму політику його пропускання. Логіку відповідної підпрограми керування чергою відеокадрів і передавання їх на аналіз представлено на рисунку 4.2.

Роботу комплексу доцільно організувати за конвеєрною моделлю, у якій окремі операції виконуються незалежними програмними компонентами. Отримання відео не повинно блокуватися на час виконання нейромережевого аналізу іншої камери. Аналогічно запис відеоархіву має здійснюватися незалежно від формування повідомлень про виявлені події.

Для цього використовуються черги кадрів, асинхронні операції та механізми синхронізації результатів. Кожен кадр повинен мати ідентифікатор камери, часову позначку та порядковий номер, необхідні для зіставлення результатів різних етапів.

У межах проєктного рішення доцільно передбачити застосування мережевих камер із підтримкою RTSP та відеокодеків H.264 або H.265. Приймання й декодування потоків можуть реалізовуватися засобами GStreamer або FFmpeg.

Для нейромережевого аналізу можна використовувати модель виявлення об'єктів, підготовлену до виконання через ONNX Runtime або TensorRT. За використання сумісного обладнання NVIDIA окремим варіантом є NVIDIA DeepStream, який поєднує елементи декодування, пакетного оброблення кадрів, інференсу та супроводження об'єктів.

Конкретний технологічний варіант визначається фактично доступним обладнанням. Подальший опис охоплює технічно здійсненні алгоритми без припущень про вже виконане впровадження.

Організація багатоканального приймання відеоданих із мережевих камер

Початковим етапом функціонування комплексу є встановлення з'єднань із мережевими відеокамерами. Для кожного пристрою визначаються мережеві параметри, адреса відеопотоку, підтримуваний кодек, роздільна здатність і частота кадрів.

Додатково необхідно враховувати спосіб автентифікації та доступність відповідного мережевого ресурсу. Усі параметри доцільно зберігати в окремій конфігураційній структурі. Це дозволяє додавати нові камери без зміни основного програмного коду.

Для передавання відео може застосовуватися протокол RTSP, який забезпечує керування сеансом потокового відтворення. Безпосередні медіадані зазвичай передаються з використанням RTP. Залежно від конфігурації мережі RTP-пакети можуть надходити через UDP або транспортуватися в межах TCP-з'єднання.

Використання UDP дозволяє уникнути затримок, спричинених повторним передаванням транспортних даних, але потребує оброблення втрат і порушення порядку пакетів. Передавання через TCP забезпечує надійну доставку байтового потоку, проте за наявності мережевих втрат може збільшувати затримку відео.

Для реалізації приймання доцільно використовувати елемент rtspsrc середовища GStreamer. Він забезпечує встановлення RTSP-сеансу, оброблення RTP-потоків і взаємодію з механізмом компенсації мережевого джитеру. Після отримання пакетів виконується відновлення закодованих відеоданих, які передаються до відповідного декодера. Параметри буферизації повинні визначатися з урахуванням допустимої затримки й характеристик мережі.

Для кожної камери необхідно підтримувати окремий стан з'єднання. На початку використовується стан DISCONNECTED, який означає відсутність активного сеансу. Після початку встановлення з'єднання використовується CONNECTING.

Успішне отримання декодованих кадрів переводить потік до STREAMING. Якщо надходження кадрів припиняється, система переходить до RECONNECTING. У випадку некоректної конфігурації або перевищення встановленої кількості спроб відновлення може використовуватися стан ERROR.

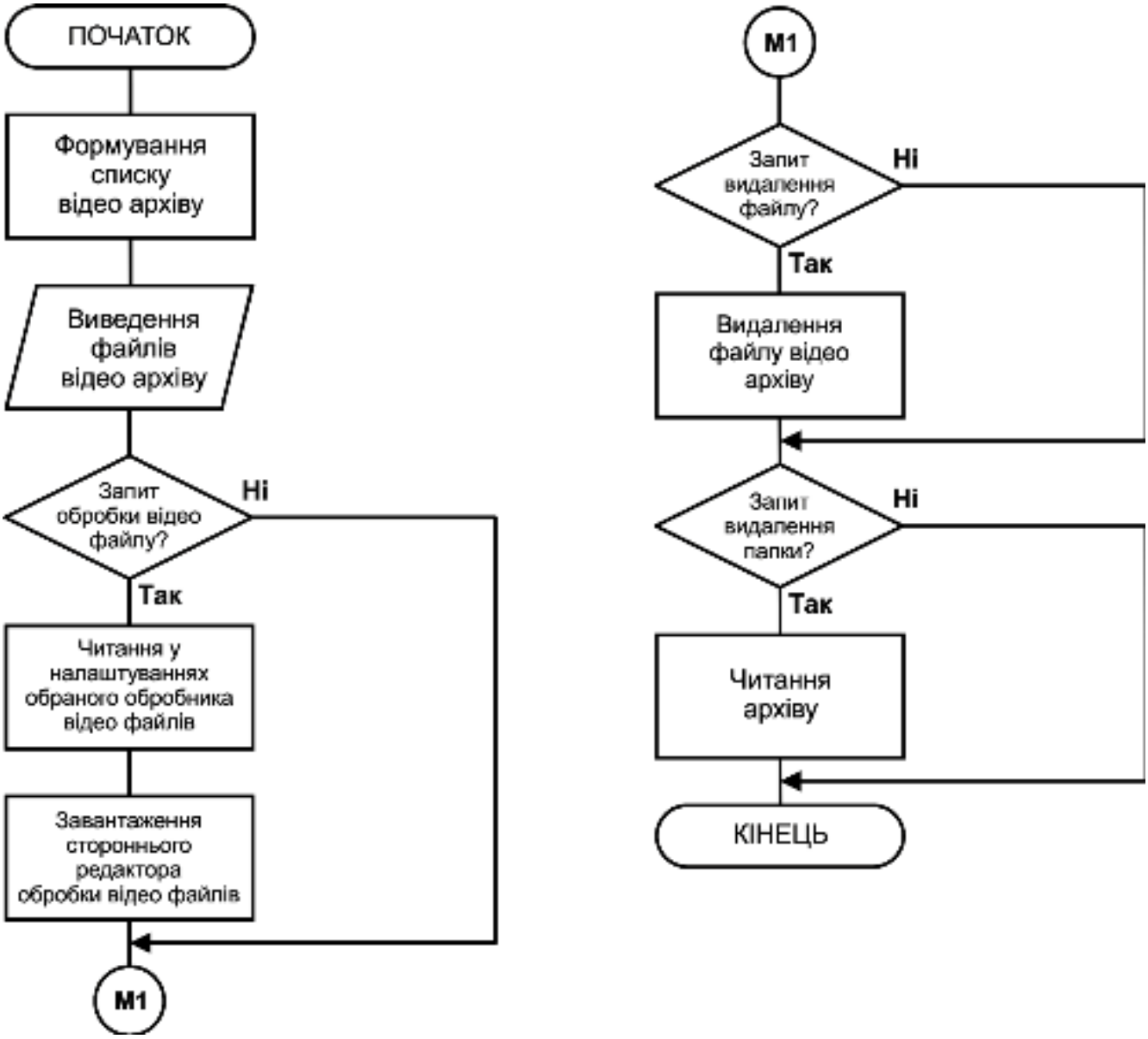

Рисунок 4.2 – Блок-схема роботи підпрограми

Під час встановлення сеансу алгоритм перевіряє доступність камери та відповідність параметрів потоку. Після успішного підключення розпочинається отримання RTP-пакетів. Компонент приймання контролює наявність нових даних

і фіксує час останнього успішного отримання кадру. Якщо протягом допустимого інтервалу нові кадри не надходять, формується повідомлення про втрату потоку. Після цього виконується процедура повторного підключення.

Для уникнення надмірного навантаження на мережеві пристрої повторні підключення доцільно виконувати зі збільшенням інтервалу очікування. Початковий інтервал може бути коротким, але після послідовних невдалих спроб він поступово збільшується до встановленої межі. Додатково може використовуватися випадкова складова затримки, яка запобігає одночасним спробам підключення великої кількості камер. Після відновлення потоку інтервал повторних спроб повертається до початкового значення.

Для коректного відновлення часу відеокадрів необхідно враховувати часові позначки RTP та інформацію про синхронізацію джерела. Якщо система отримує синхронізовані позначки часу від камери, вони можуть використовуватися для зіставлення відео з подіями. За відсутності достовірної інформації про час джерела сервер повинен окремо фіксувати момент отримання кадру. Змішування цих двох часових шкал без відповідного перетворення може спричиняти помилки під час пошуку фрагментів відеоархіву.

У багатокамерній конфігурації кожен потік обробляється незалежно до етапу об'єднання кадрів для нейромережевого аналізу. Це необхідно для запобігання ситуації, коли несправність однієї камери зупиняє оброблення інших джерел. Для кожного потоку ведуться власні лічильники отриманих кадрів, помилок декодування, повторних підключень та поточної частоти кадрів. Ці показники використовуються для контролю працездатності мережевої частини комплексу.

Обґрунтування апаратного прискорення відеоконвеєра

Одним із найбільш ресурсоємних етапів оброблення є декодування відео. Камери передають стиснені потоки, які необхідно перетворити на послідовності зображень. За програмного декодування значна частина обчислювального навантаження припадає на центральний процесор. Якщо одночасно обробляється декілька потоків високої роздільної здатності, обсяг необхідних обчислень

зростає. Використання апаратного декодера дозволяє передати цю операцію спеціалізованим функціональним блокам.

Вибір конкретного механізму апаратного декодування залежить від використовуваного обладнання. Для сумісних графічних адаптерів NVIDIA можуть використовуватися засоби апаратного декодування NVDEC. Для інших платформ можливе застосування відповідних механізмів VA-API, Intel Quick Sync Video або V4L2. Кожен варіант має власні вимоги до драйверів, підтримуваних кодеків та формату відеоданих. Тому програмний комплекс повинен перевіряти доступність потрібного механізму під час ініціалізації.

Як один із варіантів реалізації можна розглядати NVIDIA DeepStream. У відповідному конвеєрі декодування може виконуватися компонентом Gst-nvvideo4linux2, об'єднання кадрів забезпечується Gst-nvstreammux, а нейромережевий аналіз здійснюється через Gst-nvinfer. Для супроводження об'єктів передбачено компонент Gst-nvtracker. Така структура дозволяє побудувати апаратно прискорений конвеєр із передаванням метаданих між його етапами.

Необхідно розмежовувати апаратне декодування та апаратне виконання нейромережевої моделі. Ці операції використовують різні функціональні можливості обчислювального пристрою. Успішне декодування через GPU не означає, що інференс також виконується апаратно. Аналогічно запуск нейронної мережі через CUDA не гарантує апаратного декодування відео. Для підтвердження використання обох механізмів потрібні окремі перевірки фактично задіяних компонентів.

Для оцінювання необхідної продуктивності можна використати загальну інтенсивність надходження кадрів. Якщо система обслуговує N камер із частотами f_i, сумарна інтенсивність визначається за формулою

$$F_{(\Sigma)} = \sum (i = 1)^{(N)} f_i.$$

Наприклад, збільшення кількості камер за незмінної частоти кадрів призводить до пропорційного зростання кількості зображень, які необхідно

обробити f_i фактичне обчислювальне навантаження додатково заладності сцени, характеристик кодека та параметрів моделі комп'ютерного зору.

Для попереднього оцінювання обсягу нестиснених відеоданих можна використовувати співвідношення

$$M = F_{(\Sigma)} \cdot W \cdot H \cdot b,$$

де W та H визначають розміри кадру в пікселях, а b характеризує середню кількість байтів на піксель у вибраному форматі.

Значну частину накладних витрат можуть створювати копіювання кадрів між оперативною пам'яттю та відеопам'яттю. Тому під час проєктування конвеєра необхідно мінімізувати зайві перетворення форматів і переміщення великих масивів зображень. Якщо середовище виконання підтримує передавання кадрів у пам'яті прискорювача без проміжного копіювання, такий механізм доцільно використовувати. Його фактична доступність залежить від сумісності декодера, формату відеоповерхонь та нейромережевого компонента.

Розроблення механізму буферизації та планування оброблення кадрів

Під час одночасного функціонування декількох відеокамер важливо забезпечити узгодження швидкості надходження кадрів із продуктивністю аналітичного модуля. Якщо декодер формує кадри швидше, ніж нейронна мережа здатна їх обробити, виникає черга необроблених зображень. За відсутності обмежень її розмір поступово збільшується, що призводить до зростання затримки аналізу та використання оперативної пам'яті. Тому для роботи в режимі реального часу доцільно використовувати обмежені буфери й визначений порядок вибору кадрів.

Вхідними даними алгоритму планування є декодовані кадри, їхні часові позначки, ідентифікатори камер і поточний стан обчислювальних ресурсів. Для кожного джерела створюється окрема черга обмеженої місткості. Під час надходження нового кадру перевіряється наявність вільного місця. Якщо буфер заповнений, алгоритм застосовує встановлену політику перевантаження. Для поточного аналізу допускається видалення найстаріших кадрів, оскільки вони вже можуть не відповідати актуальному стану контрольованої сцени.

Політика відкидання кадрів повинна залежати від призначення відеоконвеєра. Для задач виявлення поточної активності пріоритетним є отримання максимально актуального зображення. Для задач розпізнавання короткочасних подій пропуск кадрів може спричинити втрату важливої інформації. Тому доцільно відокремити конвеєр аналітичного оброблення від конвеєра відеозапису. Архівування виконується незалежно від рішень щодо пропускання кадрів для нейромережевого аналізу.

Для оцінювання навантаження можна використовувати коефіцієнт

$$\rho = \lambda / \mu,$$

де λ визначає інтенсивність надходження кадрів до аналітичної черги, а μхарактеризує середню продуктивність її оброблення.

Програмну реалізацію буферизації можна організувати за допомогою потокобезпечної структури, яка підтримує обмежену кількість кадрів. Нижче наведено приклад Python, що демонструє зберігання актуальних кадрів, контроль часу надходження та видалення застарілих даних. Він призначений для ілюстрації логіки взаємодії між потоком декодування та обробником відео.

```
from collections import deque
from dataclasses import dataclass
from threading import Condition
from time import monotonic
from typing import Any

# Кадр із метаданими конкретної відеокамери
@dataclass(frozen=True)
class VideoFrame:
    camera_id: str
    frame_number: int
    received_at: float
    image: Any

class LatestFrameBuffer:
    def __init__(self, capacity=4, max_age=0.5):
        if capacity < 1 or max_age <= 0:
            raise ValueError("Некоректні параметри буфера")
        self.frames = deque()
        self.capacity = capacity
        self.max_age = max_age
        self.condition = Condition()
        self.dropped = 0
        self.closed = False
    def push(self, frame: VideoFrame):
        # Новий кадр не повинен блокувати декодер
        with self.condition:
            if self.closed:
                return False
```

```
            if len(self.frames) >= self.capacity:
                self.frames.popleft()
                self.dropped += 1
            self.frames.append(frame)
            self.condition.notify()
            return True
    def take_latest(self, timeout=0.2):
        # Очікування кадру з обмеженням часу
        with self.condition:
            available = self.condition.wait_for(
                lambda: self.frames or self.closed,
                timeout=timeout
            )
            if not available or not self.frames:
                return None
            # Для поточного аналізу обирається
            # найновіший кадр відеопотоку
            newest = self.frames.pop()
            self.dropped += len(self.frames)
            self.frames.clear()
        # Застарілі кадри не передаються на інференс
        if monotonic() - newest.received_at > self.max_age:
            with self.condition:
                self.dropped += 1
            return None
        return newest
    def close(self):
        with self.condition:
            self.closed = True
            self.condition.notify_all()
```

У цьому прикладі використовується монотонний годинник для визначення віку кадру. Значення received_at необхідно встановлювати в момент отримання зображення за допомогою time.monotonic(). Такий підхід не залежить від коригування системного часу. Для запису подій і синхронізації відео з іншими джерелами необхідно окремо зберігати часову позначку джерела або серверний час UTC. Політика вибору останнього кадру є придатною для аналізу поточного стану, але не повинна використовуватися без змін для задач, які потребують оброблення кожного кадру.

Для багатоканального аналізу необхідно передбачити механізм планування між камерами. Якщо всі ресурси постійно використовуються одним потоком, інші камери можуть отримувати надмірну затримку. Тому доцільно застосовувати циклічне обслуговування джерел із перевіркою наявності актуальних кадрів. Для камер підвищеної критичності може встановлюватися більша частка обчислювального часу. При цьому необхідно контролювати максимальний інтервал між послідовними обробленнями кожного джерела.

Окремим способом підвищення продуктивності є пакетне оброблення зображень. Якщо нейронна мережа підтримує пакетний інференс, кадри від декількох камер можуть об'єднуватися в один обчислювальний пакет. Це дозволяє ефективніше використовувати паралельні обчислювальні ресурси. Водночас очікування заповнення пакета збільшує затримку. Тому необхідно встановити максимальний розмір пакета та допустиму тривалість його формування.

Для оцінювання наскрізної затримки відеоаналізу доцільно використовувати співвідношення

$$T_{(\Sigma)} = T_n + T_d + T_q + T_p + T_i + T_o + T_e,$$

де T_n характеризує мережеве передавання та буферизацію, T_d означає декодування, T_q визначає очікування в черзі, T_p відповідає попередньому обробленню, T_i є тривалість.

Програмна реалізація попереднього оброблення та нейромережевого інференсу

Після вибору кадру для аналізу виконується його підготовка до передавання нейронній мережі. Основними операціями є перетворення колірного простору, зміна роздільної здатності, нормалізація значень пікселів і формування тензора необхідної структури. Конкретний порядок дій визначається вимогами навченої моделі. Невідповідність формату вхідних даних може призводити до погіршення якості виявлення навіть за правильного виконання обчислень.

Для моделей, які приймають зображення фіксованого розміру, необхідно визначити спосіб масштабування. Просте змінювання ширини та висоти може спотворювати геометричні пропорції об'єктів. Тому доцільно використовувати масштабування зі збереженням співвідношення сторін і заповненням вільної області. Такий підхід часто позначається терміном letterbox. Для подальшого відновлення координат прямокутників необхідно зберігати коефіцієнт масштабування та величини відступів.

Як можливий засіб виявлення об'єктів можна використовувати нейромережеву модель сімейства YOLO або іншу модель, підготовлену для роботи з відповідними категоріями об'єктів. Її вхідними даними є тензор

зображення, а вихідними результатами можуть бути координати обмежувальних прямокутників, оцінки впевненості та ідентифікатори класів. Точна структура вихідного тензора залежить від архітектури та способу експорту моделі. Тому програмний модуль післяоброблення повинен відповідати фактичному формату вихідних даних.

Для апаратного інференсу на сумісному обладнанні NVIDIA може використовуватися TensorRT. Альтернативним варіантом є ONNX Runtime із відповідним постачальником виконання. Для середовища CUDA може використовуватися CUDAExecutionProvider, а для програмного виконання на центральному процесорі CPUExecutionProvider. Важливо перевіряти фактично доступні засоби виконання, оскільки встановлення бібліотеки не гарантує сумісності з драйвером, графічним адаптером і форматом моделі.

Програмний механізм вибору обчислювального середовища доцільно відокремити від логіки аналізу зображень. Це дозволяє перевіряти можливість апаратного прискорення до початку оброблення потоків. Наступний фрагмент демонструє створення сеансу ONNX Runtime з явною перевіркою доступності CUDA. Якщо конфігурація вимагає апаратного прискорення, його відсутність розглядається як помилка запуску.

```
from pathlib import Path
import onnxruntime as ort

def create_inference_session(
    model_path,
    require_gpu=True
):
    # Перевірка наявності файлу нейронної мережі
    model_path = Path(model_path)

    if not model_path.is_file():
        raise FileNotFoundError(model_path)

    available = ort.get_available_providers()

    # Вибір пристрою відповідно до політики системи
    if require_gpu:
        if "CUDAExecutionProvider" not in available:
            raise RuntimeError(
                "Апаратний CUDA-прискорювач недоступний"
            )

        providers = ["CUDAExecutionProvider"]
    else:
        providers = ["CPUExecutionProvider"]
```

```
# Створення сеансу виконання моделі
session = ort.InferenceSession(
    str(model_path),
    providers=providers
)
# Перевірка активованого постачальника
active = session.get_providers()

if require_gpu and "CUDAExecutionProvider" not in active:
    raise RuntimeError("CUDA не активовано")

return session
```

Реалізація механізму супроводження об'єктів і визначення подій відеоспостереження

Одноразове виявлення об'єкта на відеокадрі не дозволяє встановити характер його переміщення. Для аналізу поведінки необхідно пов'язувати результати виявлення на послідовних кадрах. Це завдання вирішується модулем багатооб'єктного супроводження. Його вхідними даними є координати виявлених об'єктів, їхні класи, оцінки впевненості та часові позначки. Вихідним результатом стають траєкторії об'єктів із тимчасово сталими ідентифікаторами.

Як можливий алгоритм супроводження можна використовувати SORT або ByteTrack. Перший підхід поєднує прогнозування положення об'єктів із призначенням нових виявлень наявним траєкторіям. Другий передбачає додаткове використання виявлень із нижчими оцінками впевненості для підтримання супроводження. Вибір алгоритму залежить від щільності об'єктів у кадрі, частоти їхнього перекриття та доступних обчислювальних ресурсів. Для кожного варіанта необхідно визначити правила створення, оновлення та завершення траєкторії.

Під час надходження нового кадру алгоритм спочатку прогнозує положення раніше виявлених об'єктів. Далі виконується зіставлення прогнозованих областей із новими результатами нейромережевого аналізу. Для цього може використовуватися показник IoU або комбінована функція подібності, яка враховує положення й характеристики об'єкта. Після встановлення відповідностей оновлюються координати та стан траєкторій. Виявлення, для яких не знайдено відповідності, можуть створювати нові траєкторії.

Якщо об'єкт тимчасово зникає з кадру, його траєкторія не повинна завершуватися миттєво. Причиною відсутності виявлення може бути

короткочасне перекриття іншим об'єктом або зниження якості зображення. Для таких випадків доцільно встановити допустимий інтервал відсутності підтвердження. Після його перевищення траєкторія переводиться до завершеного стану. Надмірно тривалий інтервал може спричинити помилкове об'єднання різних об'єктів під одним ідентифікатором.

На основі результатів супроводження визначаються події у контрольованих зонах. До них можуть належати входження об'єкта в задану область, перетинання віртуальної лінії, тривале перебування в зоні та перевищення допустимої кількості об'єктів. Для кожної події необхідно визначити геометричні умови, допустимі класи об'єктів і часові параметри. Наприклад, для фіксації тривалого перебування необхідно контролювати час від першого підтвердженого входження до моменту виконання встановленої умови.

Контрольована зона може представлятися багатокутником у координатах вихідного кадру. Для перевірки належності об'єкта до зони визначається його опорна точка. Для людини такою точкою може бути середина нижньої сторони обмежувального прямокутника, яка наближено відповідає положенню ніг на площині сцени. Використання центра прямокутника також можливе, але може створювати інші похибки під час часткового перекриття об'єкта. Вибір опорної точки повинен відповідати характеру контрольованої події.

Програмну реалізацію виявлення тривалого перебування можна організувати за допомогою збереження часу входження об'єкта до зони. Наступний фрагмент Python демонструє перевірку геометричної належності та формування одноразової події після досягнення встановленої тривалості. Передбачається, що модуль супроводження вже надав ідентифікатор об'єкта та координати його опорної точки.

```
from dataclasses import dataclass
from math import isfinite
# Координати об'єкта, отримані від трекера
@dataclass(frozen=True)
class TrackedObject:
    camera_id: str
    track_id: int
    x: float
    y: float
    timestamp: float
```

```
def point_in_polygon(x, y, polygon):
    # Перевірка належності точки до багатокутника
    inside = False
    count = len(polygon)
    if count < 3:
        raise ValueError("Недостатньо вершин зони")
    for i in range(count):
        x1, y1 = polygon[i]
        x2, y2 = polygon[(i + 1) % count]
        if (y1 > y) != (y2 > y):
            intersection = (
                (x2 - x1) * (y - y1) / (y2 - y1)
            ) + x1
            if x < intersection:
                inside = not inside
    return inside

class ZoneEventDetector:
    def __init__(self, polygon, dwell_seconds=3.0):
        if dwell_seconds <= 0:
            raise ValueError("Некоректний час перебування")
        self.polygon = polygon
        self.dwell_seconds = dwell_seconds
        self.entered_at = {}
        self.last_seen = {}
        self.triggered = set()
    def process(self, obj: TrackedObject):
        # Ключ однозначно визначає траєкторію
        key = (obj.camera_id, obj.track_id)
        if not all(isfinite(v) for v in (
            obj.x, obj.y, obj.timestamp
        )):
            raise ValueError("Некоректні координати або час")
        previous = self.last_seen.get(key)
        if previous is not None and obj.timestamp < previous:
            raise ValueError("Порушено часовий порядок")
        self.last_seen[key] = obj.timestamp
        inside = point_in_polygon(
            obj.x, obj.y, self.polygon
        )
        if not inside:
            # Після виходу дозволяється нова подія
            self.entered_at.pop(key, None)
            self.triggered.discard(key)
            return None
        if key not in self.entered_at:
            self.entered_at[key] = obj.timestamp
            return None
        duration = obj.timestamp - self.entered_at[key]
        # Подія формується один раз за перебування
        if duration >= self.dwell_seconds:
            if key not in self.triggered:
                self.triggered.add(key)
                return {
                    "camera_id": obj.camera_id,
                    "track_id": obj.track_id,
                    "event_type": "zone_dwell",
                    "timestamp": obj.timestamp,
                    "duration": duration
                }
        return None
```

Наведений алгоритм використовує часові позначки кадрів для визначення тривалості перебування. Для практичного застосування необхідно додатково реалізувати очищення станів завершених траєкторій та оброблення тимчасової втрати об'єкта. Значення track_id повинно бути унікальним у межах відповідної камери та періоду існування траєкторії. Якщо алгоритм супроводження змінює ідентифікатор того самого об'єкта, можливе повторне формування події. Тому якість супроводження безпосередньо впливає на достовірність результатів аналізу.

Формування події повинно виконуватися незалежно від її подальшого збереження. Після підтвердження встановленої умови створюється структурований запис, який містить ідентифікатор камери, тип події, часову позначку, координати об'єкта та додаткові характеристики. Цей запис передається до модуля керування подіями. Якщо система передбачає повідомлення оператора, відповідне сповіщення формується на підставі збереженої інформації. Такий розподіл дозволяє уникнути повторного нейромережевого аналізу під час перегляду зареєстрованих подій.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Програмне забезпечення апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу призначене для централізованого отримання відеоданих від IP-камер, автоматизованого виявлення об'єктів та реєстрації подій у контрольованих зонах. Робота системи передбачає використання апаратного декодування відео, нейромережевої обробки зображень і програмних механізмів керування багатоканальними потоками. Отримані результати використовуються для формування повідомлень, супроводження виявлених об'єктів і збереження пов'язаних відеофрагментів. Головне вікно програми показано на рисунку 5.1.

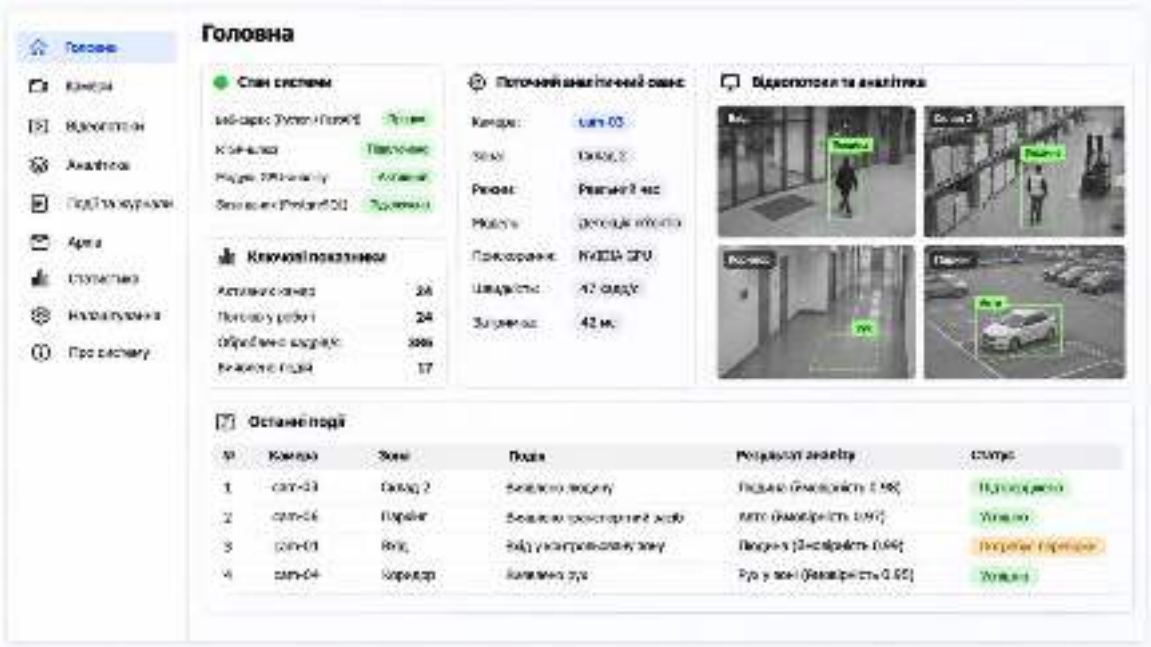

Рисунок 5.1 – Головне вікно ПЗ

Для впровадження комплексу необхідно підготувати серверне середовище, мережеву інфраструктуру та обладнання для апаратного прискорення відеооброблення. Як основу розгортання доцільно використовувати серверну

операційну систему Linux із підтримкою необхідних драйверів і мультимедійних бібліотек. Сервер повинен мати процесор із достатньою кількістю обчислювальних ядер, оперативну пам'ять для буферизації відеокадрів та дискову підсистему для збереження архівних записів. Для прискорення нейромережевого аналізу передбачається використання сумісного графічного процесора. Його характеристики визначаються кількістю камер, роздільною здатністю відео та складністю застосованої моделі.

Приймання мережевих відеопотоків може бути організоване через RTSP із використанням RTP для передавання медіаданих. Для програмної реалізації відповідного конвеєра доцільно застосувати GStreamer або FFmpeg. Ці засоби забезпечують отримання, декодування та перетворення відеоданих. У запропонованому варіанті GStreamer може використовуватися для побудови незалежних потокових конвеєрів, а Python для керування їхньою роботою, оброблення метаданих та взаємодії з аналітичними модулями. Конкретний склад бібліотек необхідно узгоджувати з фактичною структурою програмного проєкту.

Перед встановленням компонентів потрібно перевірити підтримку апаратного декодування відеокодеків H.264 та H.265. Для сумісних графічних адаптерів NVIDIA може використовуватися механізм NVDEC. Для прискорення нейромережевих обчислень доцільно передбачити CUDA, TensorRT або ONNX Runtime з відповідним постачальником виконання. Окремим варіантом є NVIDIA DeepStream, який дозволяє організувати декодування, пакетне оброблення кадрів та інференс у межах єдиного конвеєра. Вибір конкретного рішення залежить від підтримки відповідних технологій графічним обладнанням.

Підготовка програмного середовища передбачає встановлення драйвера графічного адаптера, сумісного мультимедійного середовища та бібліотек чисельного аналізу. Для модулів Python доцільно створити окреме віртуальне середовище. Після встановлення залежностей необхідно перевірити доступність графічного прискорювача та можливість створення сеансу нейромережевого інференсу. Важливо окремо підтвердити роботу апаратного декодера й виконання

обчислень на GPU. Наявність установленого драйвера не гарантує автоматичного використання всіх апаратних можливостей.

Наступним етапом є підготовка мережевих камер. Для кожного пристрою визначаються IP-адреса, параметри RTSP-підключення, формат кодування, роздільна здатність і частота кадрів. Необхідно перевірити доступність камер із сервера оброблення та коректність автентифікації. Облікові дані повинні зберігатися в захищеній конфігурації. Мережевий сегмент відеоспостереження доцільно відокремити від користувацької мережі. Для передавання відео необхідно забезпечити достатню пропускну здатність і контроль втрат пакетів.

Після налаштування камер виконується підготовка програмних конвеєрів приймання відео. Для кожного джерела створюється незалежний процес або логічний потік оброблення. У його параметрах визначаються допустима затримка буферизації, спосіб декодування та порядок повторного підключення після втрати зв'язку. Для запобігання накопиченню застарілих зображень передбачається обмежена черга кадрів. Якщо швидкість надходження перевищує продуктивність аналітичного модуля, система повинна застосовувати встановлену політику пропускання кадрів.

Окремої підготовки потребує нейромережева модель виявлення об'єктів. Перед запуском необхідно перевірити наявність файлу моделі, відповідність формату вхідних даних і підтримку обраного середовища інференсу. Для кожної моделі задаються розміри вхідного зображення, порядок нормалізації та параметри післяоброблення. Додатково налаштовуються пороги впевненості та усунення дубльованих виявлень. Після завантаження моделі необхідно виконати контрольний інференс на тестовому зображенні й перевірити правильність отриманих координат об'єктів.

Для функціонування модуля супроводження об'єктів необхідно визначити параметри зіставлення виявлень між послідовними кадрами. До них належать допустимий ступінь перекриття обмежувальних прямокутників, тривалість збереження непідтвердженої траєкторії та правила присвоєння ідентифікаторів. Якщо система використовує контрольовані зони, їхні координати задаються

відносно розмірів вихідного відеокадру. Для кожної зони визначається тип події та необхідна тривалість виконання умови. Перед експлуатацією необхідно перевірити відповідність заданих областей фактичному зображенню камери.

Для ідентифікації програмного продукту необхідно передбачити відображення відомостей про його розробника та зв'язок із відповідною магістерською кваліфікаційною роботою. Авторська інформація може розміщуватися в окремому інформаційному розділі програмного інтерфейсу. Вона повинна бути відокремлена від службових параметрів обладнання, облікових даних камер і конфіденційної конфігурації серверного середовища. Авторські дані розробленого програмного забезпечення представлено на рисунку 5.2.

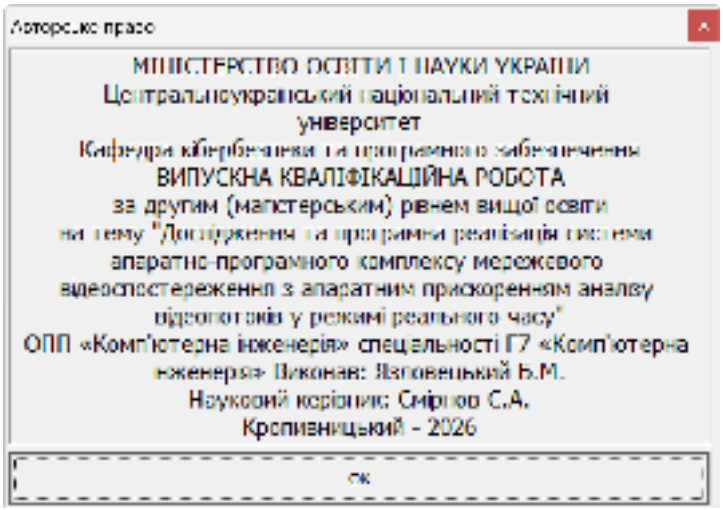

Рисунок 5.2 – Форма авторського права

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Метою розробки є дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Об'єктом дослідження є процес апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Предметом дослідження є методи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Методи дослідження базуються на методах теорії кодування, методів теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

– Розроблено вітчизняний продукт апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

В охорону праці включають санітарно-гігієнічні, лікувально-профілактичні та організаційно-технічні системи правових і соціально-економічних заходів.

В кожній ІТ компанії є трудові відносини з працівниками. Згідно закону України “Про охорону праці” [1] кожна компанія впроваджує заходи з охорони праці. Реалізується трудові відносини з вживанням необхідних засобів з охорони праці та розробки відповідних документів:

– Інструкцій з охорони праці по кожній професії і загальні.

– Положення про охорону праці.

– Накази з охорони праці.

– Журнали реєстрації та інструктажу.

Роботодавець створює відділ який працює відповідно до типового положення, яку затверджується центральним органом виконавчої влади і забезпечує виконання вимог державної політики у сфері охорони праці.

За недотриманням вимог, керівники ІТ компаній можуть бути притягнуті до відповідальності, яка виглядає у виді накладання штрафу. Якщо в результаті порушення умов охорони праці є постраждалі працівники то керівні особи ІТ компаній притягуються до кримінальної відповідальності.

Законом України “Про охорону праці” регламентуються загальні положення державної політики в галузі охорони праці, а конкретизуються ці положення нормативно-правовими актами про охорону праці, зокрема Наказом Міністерства соціальної політики України 14.02.2018 № 207, який зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за №508/31960 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [2], яким затверджено нормативно-правовий

акт з охорони праці НПАОП 0.00-7.15-18, «Правила охорони праці під час експлуатації електронно-обчислювальних машин», та «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [3].

Програмісти у процесі роботи мають негативний вплив на органи зору, а також мають значну розумову напругою і нервово-емоційне навантаження. Руки (суглоби пальців та м'язи рук) при роботі з клавіатурою мають теж істотне навантаженням. До шкідливих факторів, які впливають на робітників галузі інформаційних технологій (ІТ) спеціалісти відносять високочастотні електромагнітні коливання (випромінювання) роботи апаратної частини ЕОМ та виділення шкідливих газів.

Ці шкідливі фактори можуть привести до професійних захворювань.

Розглянемо шкідливі чинники роботи програмістів керуючись наступними нормативно-правовими актами: «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [3], та «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» НПАОП 0.00-7.15-17.

Умови праці програміста включають наступні фактори:

– вентиляція приміщення;

– освітлення приміщення;

– параметри повітряного середовища в приміщенні, тощо.

Щоб запропонувати заходи щодо зменшення негативного впливу комп’ютера на організм людини визначимо фактори, які можуть викликати професійне захворювання і впливають на працездатність програміста.

7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером

Електронно-обчислювальна машин (ЕОМ) та інше обладнання є джерелами небезпеки ураження електричним струмом. Так як робота

програміста характеризується істотним зоровим навантаженням, то вимагає належного освітлення. У приміщенні, в якому працюють люди (у тому числі програмісти) необхідно створити належний мікроклімат, праметри якого регламентуються, Державними санітарними правилами і нормами, зокрема ДСанПіН 3.3.2.007-97.

При роботі з використанням ЕОМ відзначають наступні небезпечні та шкідливі фактори:

– ризик виникнення надзвичайних ситуацій природного або штучного характеру на об’єкті або території.

– ризик виникнення пожежі;

– негативний вплив на органи зору людини;

– ризики ураження електричним струмом;

– недостатня, або надмірна освітленість робочого місця;

– електромагнітні (у тому числі високочастотні) випромінювання (коливання);

– несприятливі мікрокліматичні умови;

– нервово-емоційна напруженість праці;

– інтелектуальні навантаження;

– монотонність праці;

– невідповідність ергономічних показників робочого місця діючим вимогам;

– шум;

– статичні навантаження на кістково-м’язовий апарат.

7.3 Аналіз умов праці на робочому місці фахівця

Робота програміста пов'язана з постійною роботою на ЕОМ, яка відбувається у кімнаті розмірами 4,4 м×6,2 м×2,9 м. Одна з її більших стін має шість двостулкових вікон, розмірами 2 м×1,8 м, які виходять на північний захід. Вікна розташовані рівномірно по всій довжині стіни. Підлога в кімнаті покрита

лінолеумом, всі стіни пофарбовані світло оранжевого кольору до висоти 2,8 м, а далі підвісна стеля. Уздовж стін розташовані комп'ютерні столи. На них розташовуються 2 персональні комп'ютери й інша оргтехніка (сканер принтери, телефони й ксерокс). Столи мають пластикове покриття. Габарити їхньої робочої поверхні 1255 мм×845 мм. Висота столів 760 мм. Висота стільців від рівня підлоги становить 430 мм.

Згідно НПАОП 0.00 – 1.28 – 10 «Правила охорони праці під час електронно-обчислювальних машин» площа повинна задовольняти умові – не менш 6 $м^2$ на одне робоче місце. Кратність повітрообміну в приміщенні вузла також регламентується ДСанПіН 3.3.2.007-98 [3], вона повинна становити 20 $м^3$/годину на одне місце. Виконання даних вимог забезпечить підтримку в приміщенні вузла оптимального значення вологості й складу повітря.

Відповідно ДБН В.2.5 – 28 – 2006 [4] роботу програміста можна віднести до роботи з малою точністю (найменший розмір об'єкта розрізнення від 1 до 5 мм) V-го розряду зорової роботи, з великою контрастністю об'єкта розрізнення (символів на екрані дисплея), з темним тлом (під розряд зорової роботи В). Приміщення вузла можна віднести до 1-ої групи приміщень, у яких проводиться розрізнення об'єктів зорової роботи при фіксованому напрямку лінії зору того, що працює на робочу поверхню. Для такого типу приміщень і розряду зорової роботи нормоване значення коефіцієнта природної освітленості (КПО) робочої поверхні (при сполученому висвітленні), повинен становити 0,5%, освітленість при штучному висвітленні повинна становити 300 лк.

За результатами виміру освітленості відділом охорони праці величина освітленості від системи загального штучного висвітлення лежить у межах 200-250 лк, що не відповідає вимогам, які пред'являються до приміщення.

Відповідно ДСанПіН 3.3.2.007-98 [3] рівні звукового тиску в робочому приміщенні не повинні перевищувати в октавних смугах із середньо геометричними частотами наступних значень, наведених у таблиці 7.1.

У приміщенні перебувають наступні джерела шуму: електродвигуни внутрішнього вентилятора ЕОМ; працюючі принтери; працюючі дисководи.

Шум, вироблений вентилятором можна класифікувати як постійний, всі інші джерела шуму, як імпульсні. Відповідно паспорта на приміщення рівень звуку, Дб(А), обмірюваний за шкалою (А) шумоміра досяг величини 28,3 Дб(А) при роботі всього встаткування вузла, включаючи й ксерокс. Це дозволяє зробити висновок про відповідність рівня звуку в приміщенні вимогам нормативних актів.

Таблиця 7.1 – Допустимі спектри рівнів звукового тиску

Робоче місце	Рівень звукового тиску, дБ, в октавних смугах із середньо геометричними частотами, Гц								Рівень звуку і еквівалентний рівень звуку, дБА
	63	125	250	500	1000	2000	4000	8000	
Приміщення конструкторських бюро, програмістів обчислювальних машин, лабораторій для теоретичних робіт і опрацювання експериментальних даних, прийому хворих в медпунктах	71	61	54	49	45	42	40	38	50

Ергономічні вимоги до робочого місця працюючого з ВДТ ЕОМ і ПЕОМ нормуються НПАОП 0.00 – 1.28 – 10**.** Оптимальне положення тіла того, що працює забезпечується відповідною конструкцією робочого місця, а також регуляцією висоти робочої поверхні, сидіння, простори й підставки для ніг. Даного місця програміста не мають регульованих параметрів. Відмінності

реальних параметрів робочого місця від параметрів відповідні вимоги нормативного акту дані в таблиці 7.2.

Таблиця 7.2 – Відмінності реальних параметрів робочого місця від параметрів відповідні вимоги нормативного акту

Ріст людини, см	Висота робочої поверхні мм,	Висота простору для ніг, мм	Висота робочого сидіння, мм
175	765(740)	655(600)	450(440)

У дужках зазначені реальні значення параметрів робочого місця; всі вони не відповідають параметрам, зазначеним у стандарті.

Параметри мікроклімату можуть мінятися в широких межах, тоді як необхідною умовою життєдіяльності людини є підтримка сталості температури тіла завдяки властивості терморегуляції, тобто здатності організму регулювати віддачу тепла в навколишнє середовище.

У приміщеннях, де встановлені комп'ютери, повинні дотримуватися певні параметри мікроклімату. У санітарних нормах ДСН 3.3.6.042 – 99 [4] встановлені величини параметрів мікроклімату, що створюють комфортні умови. Ці норми встановлюються в залежності від пори року, характеру трудового процесу і характеру виробничого приміщення (див. табл. 7.3).

Таблиця 7.3 – Параметри мікроклімату для приміщень, де встановлені комп'ютери

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні	22 – 24°С
	Відносна вологість	40 – 60%
	Швидкість руху повітря	до 0,1 м/с
Теплий	Температура повітря в приміщенні	23 – 25°С
	Відносна вологість	40 ... 60%
	Швидкість руху повітря	0,1 ... 0,2 м / с

7.4 Розробка заходів з поліпшення охорони праці

Провівши аналіз умов праці в розглянутому вище приміщенні, було отримано наступні результати:

– значення мікроклімату в приміщенні не перевищує норму;

– розрахунки розміру робочого місця на одного працівника відповідають нормі;

– рівень шуму в приміщенні не становить вище норми.

З вище перерахованих результатів можна зробити висновок, що основний вплив на продуктивність ІТ-спеціалістів є його психологічний стан. Тому є доцільним зменшити рівень стресу на робочому місці.

Рекомендовані наступні заходи: За потреби особливої концентрації уваги під час виконання робіт суміжні робочі місця операторів необхідно відділяти одне від одного перегородками висотою 1,5 – 2м. Конструкція робочого місця користувача персонального комп'ютера має забезпечити підтримання оптимальної робочої пози офісного працівника. Конструкція робочого столу має відповідати сучасним вимогам ергономіки і забезпечувати оптимальне розміщення на робочий поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів. Висота робочої поверхні робочого столу має регулюватися в межах 680-800 мм, а ширина і глибина – забезпечувати можливість виконання операцій у зоні досяжності моторного поля (рекомендовані розміри: 600-1400мм, глибина – 800-1000мм). Робочий стіл повинен мати простір для ніг заввишки не менше ніж 600 мм, завширшки не менше ніж 500 мм, за глибиною (на рівні колін) не менше ніж 450 мм, на рівні простягнутої ноги не менше ніж 650 мм. Робочий стілець має бути підйомно-поворотним, регульованим за висотою, з кутом нахилу сидіння та спинки і за відстанню від спинки до переднього краю сидіння поверхня сидіння має бути плоскою, передній край – заокругленим [5].

7.5 Розрахункова частина

Заземлення – це з'єднання між електричним обладнанням і землею, завдяки якому утворюється нейтральна точка. Вона необхідна для захисту життя і здоров'я людини за рахунок передачі надлишку електроструму з мережі у ґрунт.

Крім того, заземлення сприяє створенню точки відліку для вимірювання електричного потенціалу в системі – це важливо для забезпечення правильної роботи обладнання, а також виявлення та усунення несправностей.

Початкові дані для розрахунку захисного заземлення:

- тип верхнього шару ґрунту – чорнозем,
- тип нижнього шару ґрунту – глина (питомий опір $\rho_2 = 40$ Ом·м),
- умовна товщина верхнього шару ґрунту: H=0,5 м.
- відстань між вертикальними заземлювачами A=1,7 м.
- глибина закладення горизонтального контура заземлення t=0,6 м.
- опір заземлювача, який нормується: $R_{ЗН} = 4$ Ом.

Необхідно визначити кількість вертикальних заземлювачів та довжину металевої смуги.

Для захисного штучного заземлення застосовуються вертикальні електроди: металевий куток 80х50х6 мм, (згідно з ДСТУ 8769:2018 «Кутики сталеві гарячекатані нерівнополичні. Сортамент») довжиною L=1,7 м., та горизонтальний електрод – металева смуга з перетином 60·5 мм. Напруга – 220/380 В. Розрахункова схема розташування заземлюючих електродів – у ряд (рис. 7.1).

Розрахунок проведемо за допустимим опором розтіканню струму заземлювача.

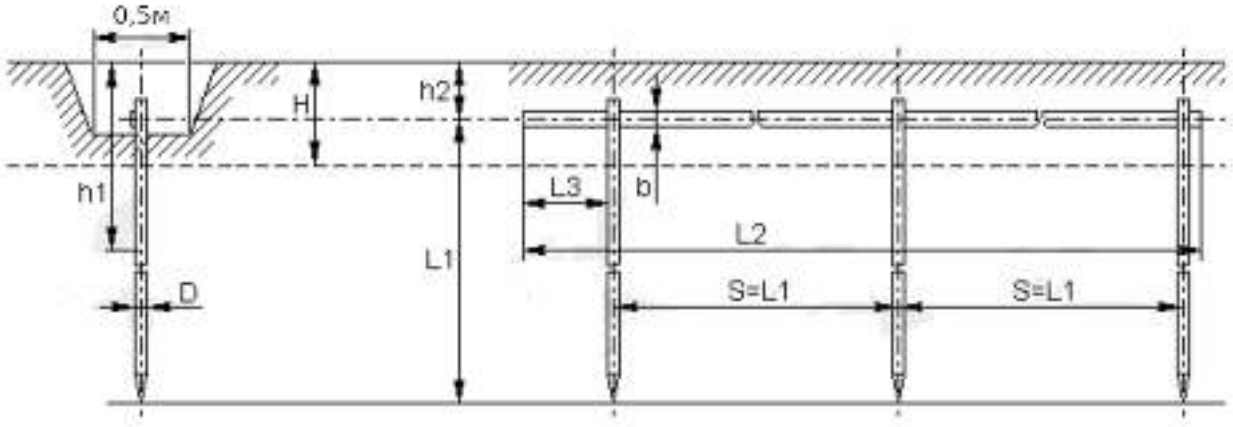

Рисунок 7.1 – Схема штучного заземлення

Відстань від центра вертикального заземлювача до поверхні землі:

$$T=t + L/2 = 0,6 +1,7/2 = 1,45 \text{ м.}$$

Розрахунковий питомий опір ґрунту (з врахуванням того, що фактично вся конструкція заземлювача розташовується у нижньому шарі ґрунту):

$$\rho = \psi \rho = 1,36 \cdot 40 = 54,5 \text{ Ом·м.}$$

де

$\psi = 1,36$ – табличне значення коефіцієнта сезонності для відповідної кліматичної зони у багатошаровому ґрунті [12];

$\rho_2 = 40$ Ом·м. – табличне значення питомого опору нижнього шару ґрунту (глина) [12].

Еквівалентний діаметр вертикального електрода (кутка) [12]:

$$D_в = 0,95 \cdot К = 0,95 \cdot 65 = 59,85 \text{ мм.} = 0,62 \text{ м.}$$

де К= (80+50)/2=65 мм. – середній розмір полиці металевого кутка.

Відношення A/L=1,7/1,7=1

Опір розтіканню електричного струму одного електроду вертикального заземлювача з урахуванням заглиблення заземлювача [8]:

$$R_O = 0,366 \cdot (\rho/L) \cdot [\lg(2L/D_в) + (1/2) \cdot \lg((4T + L)/(4T - L))] =$$

$$= 0,366 \cdot (54.5/1.7)[(\lg(2 \cdot 1.7/0.62) + (1/2) \cdot \lg((4 \cdot 1.45+1.7)/(4 \cdot 1.45-1.7))] = 21.9 \text{ Ом.}$$

Визначаємо коефіцієнт екранування вертикальних електродів Кев=0,8 при орієнтовній кількості вертикальних електродів, яке дорівнює 5 [8].

Визначаємо необхідну кількість вертикальних електродів заземлювача (без урахування горизонтального заземлювача), при $R_{ЗН}$ = 4 Ом:

$$N=R_О /(Кев\cdot R_{ЗН})= 21.9 / (0.8\cdot4)= 6.85 \approx 7 \text{ шт.}$$

Визначаємо довжину з'єднуючої смуги:

$$L_П =1,05\cdot A\cdot N= 1,05\cdot1,7\cdot7=12,22 \approx 12 \text{ м.}$$

Опір розтіканню електричного струму з'єднуючої полоси з урахуванням кліматичного коефіцієнта питомого опору ґрунту $K_П$ [8]:

$$R_П =0,366(\rho\cdot K_П/L_П)\lg(2\cdot L_П^{\,2}/(B\cdot t))=$$

$$=0,366\cdot (40\cdot5/12)\cdot\lg((2\cdot12^{\,2})/(0.06\cdot0.6))=23.5 \text{ Ом.}$$

де

$K_П$=5 – табличне значення кліматичного коефіцієнта питомого опору ґрунту для відповідної кліматичної зони для з'єднуючої смуги [8]:

B = 60 мм = 0.06 м.- ширина з'єднуючої смуги (задана).

Загальний опір розтіканню електричного струму заземлювача [8]:

$$R = (R_О\cdot R_П)/(R_О\cdot\eta_П + N\cdot R_П\cdot Кев)=$$

$$=(21.9\cdot 23.5)/(21.9\cdot 0.75+ 9\cdot 23.5 \cdot 0.8)=3.48 \text{ Ом.}$$

де $\eta_П$ = 0,75 – табличне значення коефіцієнта екранування з'єднуючої полоси [8].

Умова $R \le R_{ЗН}$ виконується ($3.48 \le 4$).

Оскільки при 7 вертикальних електродах R суттєво менше $R_{ЗН}$, зменшимо кількість вертикальних електродів N до 6 і виконаємо перерахунок. У результаті остаточно отримали: R =3,98 Ом. при кількості вертикальних електродів N=6.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

– Досліджена система апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

– На основі отриманих результатів досліджень створена програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання апаратно-програмного комплексу мережевого

відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Язловецький Б.М. Дослідження та програмна реалізація системи апаратно-програмного комплексу мережевого відеоспостереження з апаратним прискоренням аналізу відеопотоків у режимі реального часу // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.

2. Ranjan Parekh. Fundamentals of Image, Audio, and Video Processing Using MATLAB®With Applications to Pattern Recognition. CRC Press. 2021. 406 p.

3. Alasdair McAndrew. A Computational Introduction to Digital Image Processing. Chapman & Hall. 2021. 560 p.

4. Михайло Пічугін, Іван Канкін, Володимир Воротніков Комп'ютерна графіка. Навчальний посібник / Центр навчальної літератури 346 с. 2019р.

5. Маценко В.Г. Комп’ютерна графіка: Навчальний посібник. – Чернівці: Рута, 2009 – 343 с.

6. Інженерна комп’ютерна графіка: підручник / В.В. Проців [та ін.] / М-во освіти і науки України, Нац. гірн. унт-т. – Дніпро: НГУ, 2017. – 247 с.

7. Проців В.В. Прикладна комп'ютерна графіка [Текст]: Навч. посібник / В.В. Проців, К.А. Зіборов, К.М. Бас, Г.К. Ванжа; М-во освіти і наук, Нац. гірн. ун-т. – Д.: НГУ, 2016. – 187 с.

8. Kopf, Johannes and Lischinski, Dani. Depixelizing Pixel Art (англ.) // ACM Trans. Graph. – 2011. – Vol. 30, no. 4. – P. 99:1--99:8.

9. Giachetti, Andrea and Asuni, Nicola. Real-Time Artifact-Free Image Upscaling (англ.) // Trans. Img. Proc.. – 2011. – Vol. 20, no. 10. – P. 2760—2768.

10. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686.

11. Смірнов, О., Ткачук, Р., Козірова, Н., Константинова, Л., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С.. «Дослідження застосування векторних баз даних у генеративному штучному інтелекті». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 1 № 33, 667-682.

12. Смірнов О., Заріцкий В., Буравченко К., Конопліцька-Слободенюк О., Константинова Л., Якименко Н., Смірнов С. «Оптимізація розпізнавання облич за допомогою CUDA прискореної бібліотеки dlib». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2026, Том 4, № 32, С. 573-582.

13. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.

14. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447

15. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка.* 2024. №4(24), С. 6-27.

16. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології,* 2024, № 13, с. 28-35.

17. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.

18. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev,

S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265.

19. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.

20. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи,* 2023, том 7, № 2, С. 49-56.

21. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,

22. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.

23. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w

24. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418.

25. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) – 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

26. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

27. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.

28. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.

29. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.

30. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.

31. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

32. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

33. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R.,

Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.

34. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.

35. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.

36. Zhurakovskyi, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.

37. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.

38. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

39. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.517-522.

40. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.

41. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation

Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.

42. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.

43. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.

44. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

45. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». CEUR Workshop Proceedings Volume 2732, 2020, Pages 214-227.

46. Т.В. Смірнова, О.М. Дрєєв, О.А. Смірнов «Хмарна інформаційна система оцінювання шорсткості з використанням дискретного частотного аналізу макрофотографій». IV міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 15-16 квітня 2021р. – Кропивницький: ЦНТУ. – 2021. – С. 30.

47. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.

48. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.

49. Смірнов О.А., Дрєєва Г.М., Дрєєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральноукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.

50. О. Смірнов, Є. Деменко, О. Онікійчук, А. Арищенко, Л. Горбачова, «Формування псевдовипадкових послідовностей для приховування даних в зображеннях» Комп'ютерні науки та кібербезпека. № 4. С. 30-37. 2019.

51. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

52. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

53. Смірнов О.А., Дрєєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

54. Дрєєва Г.М., Смірнов О.А., Дрєєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 173-183, 2019.

55. Смірнов О.А., Кавун С.В., Коваленко О.В., Дрєєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.

56. Смірнов О.А., Смірнов С.А. Дідик А.К., Дрєєв О.М. Моделі системи нейромережевих експертів безпечної маршрутизації у хмарних антивірусних

системах. Збірник наукових праць "Системи обробки інформації". – Випуск 3 (140). – Х.: ХУПС – 2016. – С. 36-39.

57. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.

58. Смірнов О.А., Дрєєв О.М. Порівняння бітових щільностей при використанні різних методів кодування інформації. Збірник наукових праць "Системи обробки інформації". – Випуск 2 (118). т.2. – Х.: ХУПС – 2014. – С. 64-67

59. Смірнов О.А., Дрєєв О.М. Порівняння бітових щільностей при використанні різних методів кодування інформації. Збірник тез VI міжнародної науково-практичної конференції "Проблеми та перспективи розвитку ІТ-індустрії". м. Харків. 17-18 квітня 2014р. – Харків: ХНЄУ. – 2014. – С. 240.