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 відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів”

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

Керівник проекту
доктор філософії (PhD), доцент
_____ Дрєєва Г.М.
«____» _____ 2026 р.

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

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
Герман Дмитро Васильович
Сертифікат: 18DF2C9B93CEA204040000000FF841005CD45806
Дійсний з 30.10.2026 02:06:13 по 30.10.2027 03:06:12

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

Герману Дмитру Васильовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів*

2. Керівник роботи *Дрєєва Ганна Миколаївна, доктор філософії (PhD), 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 відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів*

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

Герман Д.В. Дослідження та програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів. 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 відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Метою розробки є дослідження та програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Об'єктом дослідження є процес відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Предметом дослідження є методи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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

Результат роботи – програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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, відео нагляд, HD-SDI, мережеві відеосервери

ABSTRACT

Herman D.V. Research and software implementation of a video surveillance system based on the HD-SDI protocol and network video servers. F7 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

This master's-level graduation thesis involves the development of software designed for a video surveillance system based on the HD-SDI protocol and network video servers.

The objective of the project is to research and implement software for a video surveillance system utilizing the HD-SDI protocol and network video servers.

The object of the study is the video surveillance process based on the HD-SDI protocol and network video servers.

The subject of the study comprises video surveillance methods based on the HD-SDI protocol and network video servers.

The research methodology relies on techniques related to computer networks, data encoding, mathematical statistics, and software development.

The outcome of the work is the software implementation of a video surveillance system based on the HD-SDI protocol and network video servers.

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 detail.

A user-friendly interface has been developed, and operating instructions are provided.

The software is designed to run on PCs with Windows 10/11 operating systems.

The software was developed using the Python environment.

Keywords: computer engineering, video surveillance, HD-SDI, network video servers

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	84	–	
2	А4	Робоча програма	49	–	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 9
ВСТУП..... 10
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 13
1.1 Призначення системи..... 13
1.2 Область застосування 14
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 16
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 16
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 30
2.3 Розгорнута постановка завдання 32
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 33
3.1 Опис функціонування системи 33
3.2 Розробка структурної схеми..... 35
3.3 Розробка функціональної схеми 40
3.4 Розробка діаграми процесів 43
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 46
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 46
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 61
6 НАУКОВА НОВИЗНА 65

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 66
7.1 Вступ 66
7.2 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста ... 67
7.3 Розробка заходів з умов поліпшення охорони праці 70
7.4 Пожежна безпека 71
7.5 Розрахункова частина 73
8 ОСНОВНІ ВИСНОВКИ 76
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АРП	–	автоматичне регулювання посилення
АТМ	–	автоматичний телевізійний моніторинг
ЕПТ	–	електронно-променева трубка
ІБ	–	інформаційна безпека
ІС	–	інформаційна система
НСД	–	несанкціонований доступ
ПЗ	–	програмне забезпечення
ПЗЗ	–	прилади із зарядовим зв'язком
СКД	–	системи контролю даних
СЦК	–	система централізованого керування
ТВЛ	–	телевізійні лінії
IP	–	Internet Protocol. Протокол міжмережної взаємодії
PIN-код	–	персональний ідентифікаційний код
TCP	–	Transmission Control Protocol. Протокол керування передачею (даних) Основний транспортний протокол у стеці протоколів TCP/IP. Встановлює зв'язок між двома ПК й організує обмін даними в дуплексному режимі
TCP/IP	–	Transmission Control Protocol/Internet Protocol. Стек протоколів, що забезпечують організацію зв'язку між комп'ютерами в мережі Інтернет

ВСТУП

Актуальність теми. У світі професійного мовлення точність не підлягає обговоренню. Камери повинні передавати відео з точністю до кадру. Передача має бути миттєвою. Саме в цьому середовищі з високими ставками SDI (Serial Digital Interface) вперше здобув популярність. Спочатку розроблений для підтримки нестисненого відео з низькою затримкою через коаксіальні кабелі, SDI швидко завоював своє місце як стандарт відео у мережі.

Але сьогодні вплив SDI виходить далеко за межі студії. Компанія непомітно стала критично важливою основою відеоспостереження в режимі реального часу в критично важливих середовищах – місцях, де кожна секунда має значення, а збій неможливий. Чи то в лікарнях, транспортних терміналах чи промислових об'єктах, SDI знайшла нову роль: надання командам безпеки надійності, швидкості та чіткості.

SDI (послідовний цифровий інтерфейс) – це стандарт передачі відео, визначений SMPTE. Він передає нестиснені цифрові відеосигнали через коаксіальні кабелі з опором 75 Ом з роз'ємами BNC . Спочатку розроблений для телерадіомовної індустрії, SDI забезпечує стабільне відео з низькою затримкою, що робить його ідеальним для моніторингу в режимі реального часу.

У відеоспостереженні використовується кілька варіантів SDI:

– HD-SDI: Підтримка відео 1080p з частотою 30 кадрів/с.

– 3G-SDI: Подвоює частоту кадрів до 60 кадрів/с із пропускною здатністю 2,97 Гбіт/с

Обидва формати є plug-and-play, не потребуючи налаштування IP-адреси. Це робить їх популярними для інсталяцій, де швидкість, простота та надійність є невід'ємними факторами.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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

– Огляд існуючих систем відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

– Дослідження системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

– Програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Об'єктом дослідження є процес відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Предметом дослідження є методи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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

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

– Удосконалено метод відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

– Розроблено вітчизняний продукт відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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 відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів, 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

Хоча IP-відеосистеми стають дедалі популярнішими, особливо в хмарних та корпоративних інсталяціях, вони не завжди є найнадійнішим вибором у кожному контексті спостереження. Фактично, багато об'єктів досі покладаються на SDI як стабільну альтернативу, що не потребує особливого обслуговування, особливо там, де потрібні видимість у режимі реального часу, коаксіальна інфраструктура або обмежені IT-ресурси.

Типові сценарії, що підтримують SDI:

– Транспортні термінали: відео з платформи в реальному часі надсилається безпосередньо до диспетчерських, минаючи затримку мережі.

– Лікарні та відділення невідкладної допомоги: безпечні, сегментовані відеошляхи без додаткового навантаження на IT.

– Промислові об'єкти: Використовує існуючу коаксіальну інфраструктуру, уникаючи дорогої пере проводки.

Передаючи відео безпосередньо з камери на монітор – без залежності від програмного забезпечення чи мережевої маршрутизації – системи SDI зменшують кількість точок збоїв та спрощують розгортання.

SDI дозволяє швидше приймати рішення на місці, усуває залежність від локальних мереж та спрощує розгортання. Він також зменшує кількість точок збою, що виникають у системах, керованих програмним забезпеченням, допомагаючи інтеграторам та командам безпеки створювати більш передбачувані та стійкі інсталяції.

Поширеною помилковою думкою є те, що проекти спостереження повинні вибирати між SDI та IP-відео. Насправді ці два типи можуть співіснувати. Багато сучасних систем є гібридними за своєю суттю, використовуючи SDI там, де затримка та простота є важливими, водночас

використовуючи IP-камери для віддаленого доступу, зберігання відео та хмарної інтеграції. Щоб зрозуміти, як SDI забезпечує чіткість зображення в режимі реального часу в польових умовах, прочитайте нашу статтю про те, чому низька затримка все ще важлива в системах спостереження .

Такий гібридний підхід особливо цінний у сценаріях, які вимагають як оперативного реагування на місці, так і централізованого управління. Наприклад, персонал платформи на залізничній станції може відстежувати прямі трансляції через SDI, тоді як штаб-квартира безпеки використовує IP-інструменти для запису та аналізу. Завдяки такому розподілу ролей SDI стає життєво важливим інструментом передової, доповнюючи ширші можливості мережевого спостереження.

Приклад: Залізнична станція може використовувати SDI для показу живого відео персоналу на місці, тоді як штаб-квартира отримує доступ до того ж відеозапису через систему запису на основі IP.

Такий подвійний підхід забезпечує негайну видимість там, де це найважливіше, без шкоди для централізованого управління.

1.2 Область застосування

Практичні переваги SDI найбільш помітні в середовищах з високим рівнем руху, високими ставками або складним для підключення обладнання. У транспортних вузлах монітори SDI забезпечують візуальний зворотний зв'язок у громадських місцях у режимі реального часу, гарантуючи, що персонал станцій може негайно реагувати на потенційні загрози. Відділення невідкладної допомоги та входи до лікарень використовують SDI для гарантування візуального доступу до вхідних сигналів, навіть коли їхні внутрішні мережі сегментовані для безпеки даних. У логістичному секторі SDI є надійним вибором для моніторингу активності на вантажних майданчиках і в коридорах, де мережеві сигнали можуть бути слабкими або переривчастими. А на віддалених об'єктах, таких як прикордонні пости або тимчасові будівельні зони,

здатність SDI працювати незалежно від локальної мережевої інфраструктури робить його безцінним для підтримки безперервності спостереження:

– Транзитні термінали: Моніторинг платформи в режимі реального часу.

– Лікарні та відділення невідкладної допомоги: Миттєва видимість у критичних точках входу.

– Логістичні зони: охорона вантажної рампи або коридору.

– Нестабільні мережі: сільські, прикордонні або промислові об'єкти.

З розвитком потреб у системах спостереження розвивається й технологія SDI-дисплеїв. Сучасні SDI-монітори комерційного класу розроблені не лише для сумісності, але й для безперервної роботи в найскладніших умовах. Багато з них підтримують вхідні сигнали Full HD та 4K, пропонують наскрізний BNC-вихід для каскадного підключення дисплеїв та мають міцні металеві корпуси, що витримують цілодобове використання. Для системних інтеграторів ці монітори скорочують час встановлення, усувають складне налаштування програмного забезпечення та легко інтегруються в коаксіальні середовища. Незалежно від того, чи йдеться про нове розгортання, чи про оновлення існуючої інфраструктури SDI, переваги є негайними: чітке зображення, надійний час безвідмовної роботи та швидше розгортання. SDI, можливо, і розпочався в телерадіомовленні, але його спадщина продовжує жити у відеоспостереженні з однієї простої причини – він працює. У критично важливих місцях, де кожен кадр має значення, а затримка неприйнятна, SDI забезпечує гарантію чіткості без компромісів. Це дозволяє командам зосередитися на тому, що найважливіше – захисті людей, активів та інфраструктури – без сумніву щодо якості відеопотоку.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів, 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

Xeoma – розумний вибір для сучасної безпеки

Оскільки технології відеоспостереження продовжують розвиватися, вибір правильного програмного забезпечення стає вирішальним для безпеки як дому, так і бізнесу. У 2026 році одних лише камер безпеки часто недостатньо для створення надійної системи відеоспостереження. Тепер набагато простіше використовувати штучний інтелект у повсякденному житті для автоматизації колись складних завдань. У цьому розділі ми розглянемо важливі моменти, на які слід звернути увагу, вибираючи систему відеоспостереження у 2026 році.

Як вибрати відеоспостереження

Отже, у вас встановлено камери безпеки – чудово! Але самі камери – це лише частина рішення. Програмне забезпечення для керування відео (VMS) – це те, що дійсно виводить вашу систему безпеки на новий рівень, обробляючи запис, аналізуючи відзнятий матеріал і надаючи вам можливість перевірити лише короткий виклад того, що сталося. Нижче наведено кілька важливих питань, які вам потрібно поставити собі, щоб знайти найкраще програмне забезпечення для відеоспостереження.

1. Визначте, що вам потрібно:

Камери: Скільки у вас камер? Чи плануєте ви збільшити їх кількість у майбутньому? Ця інформація допоможе визначити, яку ліцензію вам потрібно придбати та яке програмне забезпечення слід розглянути (чи є його ліцензування масштабованим чи ні).

Моніторинг: Ви забезпечуєте безпеку будинку чи бізнесу? Розгляньте такі функції, як розпізнавання номерних знаків, підрахунок людей або

сповіщення про тривогу, якщо потрібно, та відповідно виберіть програмне забезпечення для спостереження.

Віддалений доступ: Вам потрібно переглядати відео з будь-якого місця? Мобільний додаток є важливим для багатьох, як і безкоштовний віддалений доступ.

Запис: Вам потрібен безперервний або запланований запис? Або, можливо, лише сповіщення, активовані рухом? Виберіть те, що підходить для ваших потреб.

Бюджет: Вартість програмного забезпечення сильно варіюється, від безкоштовних варіантів до моделей передплати. Спробуйте, перш ніж купувати (виберіть програмне забезпечення, яке надає вам безкоштовні можливості тестування).

2. Ключові характеристики, яким слід визначити пріоритет:

– переконайтеся, що програмне забезпечення підтримує вашу марку та модель камери (сумісність з ONVIF надає ширші можливості)

– оберіть інтуїтивно зрозумілий інтерфейс, з яким легко працювати

– надайте пріоритет програмному забезпеченню з надійним шифруванням та контролем доступу користувачів

– шукайте налаштовувані графіки запису та роздільну здатність

– зверніть увагу на надійний мобільний додаток та веб-інтерфейс для перегляду прямих трансляцій та записаного відео

– оберіть налаштовувані зони виявлення руху та сповіщення в режимі реального часу

– оберіть програмне забезпечення з такими функціями, як розпізнавання облич, виявлення об’єктів та підрахунок людей, щоб отримувати цінну аналітику

– оберіть між локальним сховищем (HDD/SSD), хмарним сховищем або гібридним підходом для резервного копіювання

3. Перевірте, перш ніж зробити фіксацію:

Більшість постачальників VMS пропонують безкоштовні пробні версії. Скористайтеся ними! Протестуйте програмне забезпечення з вашими камерами,

щоб переконатися в сумісності та відповідності інтерфейсу вашим потребам.

Яке програмне забезпечення ми б рекомендували?

Як новачкам у сфері відеоспостереження, так і професіоналам ми рекомендуємо Xeoma – модульне програмне забезпечення для відеоспостереження на базі штучного інтелекту, яке активно розробляється вже понад 15 років. Воно працює за принципом «конструктора», де користувачі створюють власні ланцюжки, підключаючи функціональні модулі (такі як виявлення руху, розпізнавання обличчя тощо). Такий підхід, у поєднанні з гнучким ціноутворенням, багатим набором функцій та чуйною командою підтримки клієнтів, робить Xeoma однаково придатним для:

– домашня безпека;

– малий бізнес (магазини, ресторани, кафе тощо);

– великі підприємства (фабрики, заводи, офіси, аеропорти тощо);

– інтеграція розумного дому (IoT, домашня автоматизація);

Функції Xeoma:

– Міжплатформна сумісність (Windows, macOS, Linux (включно з ARM), Android, iOS).

– Масштабна підтримка камер, включаючи IP-камери (ONVIF, H.266, H.265+, H.264+), Wi-Fi та USB-камери, PTZ-камери (поворотно-нахилювальні камери) тощо.

– Розширена відеоаналітика (розпізнавання облич, розпізнавання номерних знаків, аналіз емоцій та багато іншого).

– Віддалений доступ P2P (не потрібна «публічна» IP-адреса).

– Веб-інтерфейс для перегляду в браузері.

– Багатосерверні структури для великих інсталяцій.

– Зручний інтерфейс.

– Не потрібна установка (працює портативно).

– Інтуїтивно зрозуміла модульна система перетягування.

– Безпека та контроль доступу (зашифрована передача даних).

– Різні права доступу для користувачів.

– Сумісність із системами розумного дому (автоматизація та інтеграція).

– Миттєві мобільні сповіщення.

Xeoma пропонує гнучку модель ліцензування залежно від кількості камер (масштабована до необмеженої кількості камер). Клієнтський застосунок безкоштовний, ліцензування потребує лише серверна частина. Для корпоративних розгортань доступні оптові знижки.



Рисунок 2.1 – Інтерфейс користувача Xeoma

Чому варто обрати Xeoma у 2026 році?

Функції на базі штучного інтелекту.

Алгоритми машинного навчання покращують точність модулів.

Масштабованість.

Від домашньої системи з однією камерою до мереж відеоспостереження по всьому місту – Xeoma адаптується до ваших потреб.

Підтримка 99% камер.

Працює з 99% існуючого обладнання для камер, що зменшує витрати на

оновлення.

Регулярні оновлення

Команда розробників постійно додає нові функції.

Варіанти використання Xeoma

Безпека дому: моніторинг входів, подвір'їв та домашніх тварин за допомогою сповіщень про рух, використання Xeoma як відеоняні з миттєвими мобільними сповіщеннями.

Роздрібна торгівля: запобігання крадіжкам за допомогою розпізнавання обличчя, відстеження трафіку клієнтів та збір цінної маркетингової інформації.

Промислові об'єкти: автоматизація входу за допомогою Face ID та забезпечення захисту в нічний час.

Офіси: інтеграція із системами контролю доступу та облік робочого часу.

Транспорт: використання розпізнавання номерних знаків для парковок та автоматичного відкриття воріт.

Налаштування Xeoma займає кілька хвилин:

1. Завантажте та запустіть програмне забезпечення (встановлення не потрібне).

2. Автоматичне виявлення камер у вашій мережі.

3. Перетягуйте модулі для створення власної системи спостереження.

4. Налаштуйте сповіщення та параметри сховища.

5. Доступ до камер через мобільний додаток або браузер.

Штучний інтелект у відеоспостереженні

Xeoma пропонує різноманітні функції на базі штучного інтелекту:

– Інтелектуальне виявлення руху: Датчик руху Xeoma на базі штучного інтелекту може розрізняти людей і транспортні засоби, зменшуючи кількість хибних тривог.

– Розпізнавання облич: ідентифікація відомих осіб або позначка незнайомих облич, що підвищує безпеку та активує такі функції, як автоматичне відмикання дверей для уповноваженого персоналу.

– Виявлення та класифікація об'єктів: Виявлення конкретних об'єктів,

таких як зниклі сумки або залишені без нагляду коробки, для виявлення потенційних загроз у чутливих зонах. Розрізнення виявлених об'єктів для зменшення кількості хибних спрацьовувань (Xeoma може виявляти різні типи транспортних засобів, тварин, птахів, дронів тощо).

– Моніторинг щільності натовпу: відстежуйте кількість людей у певній зоні, що надає цінну інформацію для управління натовпом та забезпечення безпеки.

– Теплові карти: Візуалізація моделей руху для визначення часто використовуваних зон та оптимізації розміщення систем безпеки.

– Розпізнавання номерних знаків (LPR): Автоматичне захоплення та запис номерних знаків для контролю доступу або розслідування (доступні чорні та білі списки).

– Поведінкова аналітика: виявляйте незвичайну активність, таку як байдикування, ковзання або падіння, що запускає сповіщення про потенційні інциденти.

У 2026 році Xeoma залишається найкращим вибором для відеоспостереження завдяки своєму балансу потужності та простоти. Незалежно від того, чи ви домовласник, який шукає спокою, чи підприємство, якому потрібна професійна аналітика, модульна конструкція Xeoma та кросплатформна підтримка роблять його універсальним рішенням. Будьте попереду з рішенням, яке завжди інноваційне. Ознайомтеся з Xeoma сьогодні та створіть систему спостереження, яка ідеально підходить саме вам!

CCTV Design Tool

CCTV Design Tool – це програмне забезпечення для проектування систем відеоспостереження та безпеки на базі браузера, створене для установників та інтеграторів. Це не інструмент моніторингу. Його використовують перед встановленням окремої камери на стіну, щоб спланувати охоплення, підтвердити поле зору клієнту та сформувати цінову пропозицію. Це робить його природним доповненням до програмного забезпечення для запису та відтворення, яке знаходиться далі у цьому списку.

Робочий процес зосереджений на плані поверху. Ви імпортуєте план, розміщуєте камери та моделюєте поле зору, DORI та кількість пікселів на метр, щоб довести, що дана камера дійсно розрізняє грань або пластину на заданій відстані. Звідти система прокладає кабель, розраховує довжину та генерує специфікацію матеріалів з цінами, яка одразу перетворюється на готову для клієнта PDF-пропозицію.

Найкраще підходить для: установників та інтеграторів систем безпеки, яким потрібно проектувати системи та вигравати тендери до придбання будь-якого обладнання.

– Ключові сильні сторони.

– Імпорт плану поверху з моделюванням FOV, DORI та PPM.

– Маршрутування кабелів, розрахунок довжини та створення специфікації матеріалів (BOM).

– Готові для клієнта PDF-пропозиції з індивідуальним брендингом.

– Синхронізація з хмарою та командна співпраця над проектами

Чому варто обрати інструмент для проектування систем відеоспостереження: Якщо ваша робота полягає в визначенні та складанні цінових пропозицій щодо систем, це позбавляє від здогадок щодо розміщення камер і робить пропозиції професійними. Він поєднується з інструментом моніторингу, а не замінює його, тому ставтеся до нього як до основної частини вашого комплексу, що займається проектуванням.

Ціни на інструменти для проектування відеоспостереження: безкоштовна версія охоплює до трьох камер або пристроїв на один проект з основними інструментами проектування. Преміум-план коштує 72 долари США на рік і додає необмежену кількість проектів, синхронізацію з хмарою, експорт без водяних знаків, власний брендинг і симуляцію нічного бачення. Корпоративний план починається від 50 доларів США за робоче місце на рік з обліковими записами для кількох користувачів і оптовими знижками.

Agent DVR від iSpyConnect

Agent DVR від iSpyConnect – це програмне забезпечення для відеоспостереження, що дозволяє записувати відео з локальної та віддаленої камери, виявляти відео через штучний інтелект та моніторити на основі браузера. Це програмне забезпечення для самостійного розміщення відеореєстраторів, яке запускається на власному комп'ютері та приваблює покупців, які хочуть контролювати місце зберігання відеозаписів та не вимагати математики ліцензування кожної окремої камери.

Головна перевага – необмежена кількість камер і мікрофонів. Додайте стільки каналів, скільки може обробляти ваше обладнання. Програма підтримує віддалений доступ через веббраузер і мобільні додатки, а також пропонує можливості локального та стороннього виявлення об'єктів на основі штучного інтелекту, щоб ви могли фільтрувати сповіщення, відображаючи лише людей або транспортні засоби, а не тонути в шумі руху. Як програмне забезпечення для камер RTSP із широкою підтримкою протоколів, воно підходить для більшості парків IP-камер без проблем із сумісністю.

Найкраще для: організацій, яким потрібне власне програмне забезпечення для відеоспостереження/мережевої відеореєстрації з необмеженою кількістю камер та додатковим віддаленим доступом.

Ключові сильні сторони:

– Необмежена кількість камер та мікрофонів.
– Віддалений доступ через веббраузер та мобільні додатки.
– Виявлення локальних та сторонніх об'єктів штучного інтелекту.
– Працює на основних операційних системах.

Чому варто обрати Agent DVR: Ви отримуєте можливості NVR-рівня без необхідності купувати окремий пристрій, а безкоштовний локальний рівень дійсно зручний для розгортання вдома та на невеликих об'єктах. Перейдіть на платний план, якщо вам потрібне використання для бізнесу та віддалений доступ.

Ціни на агентський відеореєстратор: безкоштовно для приватного локального використання з необмеженою кількістю камер. Платні плани підписки починаються від $7,95/місяць для бізнес-використання та віддаленого доступу, Standard – $14,95/місяць, Professional – $19,95/місяць.

CameraFTP Virtual Security System

CameraFTP Virtual Security System – це хмарне програмне забезпечення для відеоспостереження, яке перетворює ПК або ноутбук на систему безпеки типу CCTV/DVR. Замість купівлі спеціального відеореєстратора, ви направляєте наявні камери або веб-камеру на програмне забезпечення, і воно займається записом, переглядом у реальному часі та відтворенням.

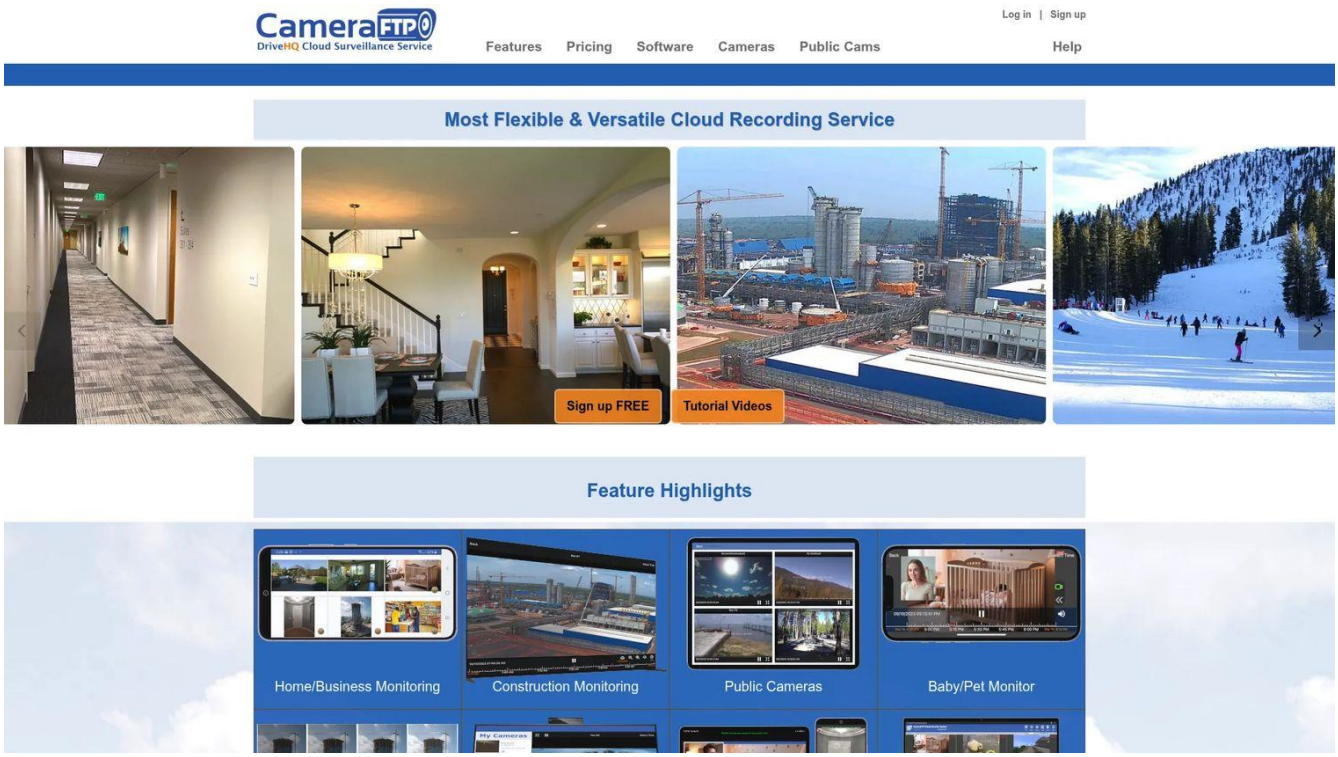


Рисунок 2.2 – Інтерфейс користувача CameraFTP Virtual Security System

Суть полягає в хмарному записі з записом на локальний диск як резервним варіантом. Відеозаписи зберігаються поза межами об'єкта, що захищає їх у разі крадіжки або збою локального обладнання. Ви отримуєте віддалений перегляд у реальному часі та відтворення з будь-якого місця, що підходить

власникам, які хочуть стежити за місцем розташування під час подорожей. Для низькобюджетних систем з одним об'єктом це один з найдешевших шляхів до справжнього хмарного резервного копіювання.

Найкраще підходить для: користувачів, які хочуть встановити недорогий хмарний відеореєстратор/відеореєстратор, використовуючи ПК або ноутбук та наявні камери.

Ключові сильні сторони:

– Перетворює ПК або ноутбук на систему відеоспостереження/реєстратора.

– Хмарний запис з підтримкою локального запису на диск.

– Віддалений перегляд у реальному часі та відтворення з будь-якого місця.

– Налаштовувані плани запису зображень та відео.

Чому варто обрати CameraFTP: Якщо збереження відео поза межами об'єкта важливіше за розширену аналітику, то це забезпечує хмарне резервне копіювання за ціною, з якою більшість конкурентів не можуть зрівнятися. Це підходить для малого бізнесу та домашніх користувачів, а не для великих парків обладнання з кількома об'єктами.

Ціни на CameraFTP: Існує безкоштовний базовий рівень, а також плани з можливістю налаштування. На сайті вказано вартість запису зображень від $1,50 на місяць, а запису відео – від $2,50 на місяць. Приклади тарифів на відео становлять $2,95, $4,95 та $6,95 на місяць для рівнів Entry, Standard та Premier.

ITVDesk

ITVDesk – це програмне забезпечення для віртуальних камер ONVIF, яке перетворює комп’ютери, веб-камери, медіафайли та джерела RTSP або ONVIF на сигнали з камер, які може використовувати ваш існуючий стек відеоспостереження. Воно вирішує вузьку, але реальну проблему: у вас є VMS або NVR, і ви хочете підключити до нього нестандартне джерело так, ніби це звичайна IP-камера.

Як програмне забезпечення, сумісне з ONVIF, воно відображає будь-яке

підтримуване джерело як віртуальну камеру ONVIF, тому ваша VMS записує та керує ним, як і будь-яким іншим потоком даних. Воно використовує обробку H.264 та H.265 з прискоренням на графічному процесорі для зниження навантаження на процесор, а також підтримує керування робочим столом на основі PTZ та двосторонній аудіозв'язок. Для інтеграторів, які розширюють існуючу систему, а не створюють нову, саме така сумісність з керуванням камерами спостереження є головною метою.

Найкраще для: команд, яким потрібно перетворити ПК або інші цифрові джерела на камери ONVIF для існуючих систем спостереження.

Ключові сильні сторони:

– Потокова передача даних ONVIF та RTSP для інтеграції VMS та NVR.

– Обробка H.264/H.265 з прискоренням на графічному процесорі.

– Керування робочим столом на основі PTZ та двосторонній звук.

– Різні розміри ліцензій, включаючи пакети для кількох комп'ютерів.

Чому варто обрати ITVDesk: Оберіть його, коли вашою проблемою є інтеграція, а не моніторинг. Він підключає нові джерела до існуючої екосистеми ONVIF, а не просить вас перебудовувати її, що саме той вузькоспеціалізований підхід, який команди передпродажної підготовки повинні ретельно розглядати.

Ціни на ITVDesk: 15-денна пробна версія безкоштовна. Ліцензія на підписку коштує 45 євро на 365 днів, а довічна ліцензія – одноразово 59 євро. Варіанти для кількох комп’ютерів включають підписку на 5 комп’ютерів за 329 євро на рік та безстрокову ліцензію на 5 комп’ютерів за 399 євро.

Banalytics

Banalytics – це платформа периферійного інтелекту для камер, датчиків та фізичних систем з доступом на основі браузера. Вона виходить за рамки простого відеоспостереження та охоплює сферу датчиків та автоматизації, але для спостереження вона охоплює важливі стандарти та працює локально.

Він підтримує джерела камер ONVIF, RTSP та USB, що робить його гнучким програмним забезпеченням для відеоспостереження на основі браузера для змішаного обладнання. Окрім потоків даних, він додає запис, панелі

керування, віддалену консоль та сповіщення, а також інтеграцію MQTT та Modbus для команд, яким потрібні відео та дані датчиків в одному місці. Розгортання plug-and-play та безкоштовний рівень спільноти спрощують тестування перед використанням.

Найкраще підходить для: команд або окремих осіб, яким потрібен локальний моніторинг периферійних мереж та модульна автоматизація відео чи датчиків.

Ключові сильні сторони:

– Підтримка ONVIF, RTSP та USB-камер.

– Запис, інформаційні панелі, віддалена консоль та сповіщення.

– Інтеграції MQTT та Modbus.

– Доступ через браузер з локальною обробкою.

Чому варто обрати Banalytics: Оберіть його, коли ваш моніторинг поширюється за межі камер на сенсори та фізичні системи, і вам потрібна єдина платформа на периферії. Рівень безкоштовного доступу назавжди знижує ризик тестування на вашому реальному обладнанні.

Ціни на Banytics: рівень Community безкоштовний назавжди. Basic коштує 15 доларів США на місяць, а Pro – 50 доларів США на місяць. Enterprise діє за контрактом, а платні компоненти оплачуються окремо.

Verkada

Verkada – це хмарна керована платформа фізичної безпеки, що охоплює камери, контроль доступу, сигналізацію, домофони, датчики та управління робочим місцем. Вона знаходиться в кінці цього списку серед підприємств, де рішення про покупку зумовлене централізованим адмініструванням та масштабуванням, а не економією коштів на одній камері.

Платформа працює на хмарному інтерфейсі Command від Verkada, який об'єднує відеобезпеку, контроль доступу, сигналізацію та домофони в один рівень управління. Він додає аналітику на основі штучного інтелекту та цілодобову технічну підтримку. Для організацій, які керують багатьма об'єктами та користувачами, привабливою є одна консоль, одна модель дозволів та

керована апаратна екосистема замість об'єднання інструментів. Саме за таке управління платять корпоративні покупці.

Найкраще підходить для: організацій, яким потрібна єдина хмарна платформа для інтегрованої фізичної безпеки та обладнання на робочому місці.

Ключові сильні сторони:

– Хмарна платформа управління командами.

– Інтегрована відеобезпека, контроль доступу, сигналізація та домофони.

– Аналітика на основі штучного інтелекту.

– Цілодобова технічна підтримка.

Чому варто обрати Verkada: Оберіть її, коли централізоване управління, дозволи користувачів та адміністрування, готове до аудиту, на всіх сайтах важливіші за початкові витрати. Це кероване зобов'язання, що передбачає використання апаратного та програмного забезпечення, а не інструмент із власною камерою, тому заздалегідь оцініть сумісність камер з їхньою екосистемою.

Ціни Verkada: Ціна вказана як рекомендована роздрібна ціна для обладнання та деяких ліцензій. Камера CM22 коштує 699 доларів США, базова сигналізація – 600 доларів США за річну ліцензію на сигналізацію, а відеосигналізація – 1500 доларів США. Багато товарів потребують додаткових ліцензій, а деякі продукти надаються за умови отримання комерційної пропозиції.

Перш ніж взяти на себе зобов'язання, ознайомтеся з цим контрольним списком, враховуючи реальне середовище покупця.

Сумісність камери

Це перше, що потрібно перевірити, і найпоширеніша причина, через яку покупці шкодують. Переконайтеся, що програмне забезпечення підтримує саме ті моделі камер, які використовуються, а не лише «камери ONVIF» загалом. Покриття ONVIF, RTSP та USB має значення, але також має значення база даних пристроїв постачальника. Запитайте список підтримуваних моделей і протестуйте справжню камеру перед покупкою.

Запис та зберігання

Вибирайте між локальним записом, хмарним записом та гібридним, виходячи з профілю ризику покупця. Локальний запис швидкий та конфіденційний, але вразливий до крадіжки на місці. Хмарний запис захищає відзнятий матеріал поза межами об'єкта, але з часом коштує дорожче та потребує пропускної здатності. Зіставте вимоги до зберігання з вартістю зберігання та підтвердьте, як докази експортуються, коли комусь дійсно потрібен кліп.

Віддалений доступ і безпека

Віддалений перегляд є стандартним, але модель безпеки дуже різниться. Перевірте SSL, доступ браузера та детальний контроль доступу. Головним питанням для покупців, які купують житло з кількома сайтами, є віддалений доступ без переадресації портів, оскільки відкриття портів маршрутизатора на кожному сайті є проблемою обслуговування та безпеки. Будьте готові до того, що команда безпеки перегляне модель підключення, тому заздавайте.

Середовище розгортання

Перш ніж обіцяти дату розгортання, підберіть програмне забезпечення до середовища встановлення. Існує програмне забезпечення для відеоспостереження Windows, macOS, Linux, Docker та Raspberry Pi, але жоден інструмент не охоплює всі варіанти. Варіанти на основі браузера зменшують труднощі при встановленні. Відповідність середовища безпосередньо впливає на швидкість розгортання та постійне навантаження на обслуговування.

Масштаб та управління

Якщо ви не стосується одного об’єкта, запитайте про кількість камер, дозволи користувачів, журнал активності та адміністративні елементи керування. Корпоративним покупцям потрібне централізоване управління, журнали аудиту та доступ на основі ролей . Переконайтеся, що модель ліцензування не передбачає покарання за додавання камер, і що адміністративні елементи керування масштабуються залежно від кількості об’єктів.

Висновок

Не існує єдиного найкращого програмного забезпечення для відеоспостереження, лише те, яке найкраще підходить для певної моделі розгортання.

Якщо ви визначите та оціните системи, CCTV Design Tool візьме на себе роботу з проектування та розробки пропозицій до відправки обладнання. Для самостійного запису з необмеженою кількістю камер Agent DVR є найкращим безкоштовним варіантом для початку роботи. CameraFTP перемагає завдяки недорогому хмарному запису з ПК. ITVDesk – це спеціаліст з інтеграції, коли вам потрібно підключити нестандартні джерела до існуючого стеку ONVIF. Banalytics підходить для моніторингу на периферії на основі браузера через камери та датчики. Verkada – це вибір, коли централізоване адміністрування та масштабування переважують вартість.

Ваш наступний крок: скласти короткий список на основі вашої моделі сховища та стандартів камер, а потім протестувати одну реальну камеру порівняно з двома найкращими варіантами, перш ніж приймати рішення. Сумісність – це те, що визначає успішність або зупинку розгортання, тому перевірте її в першу чергу, а не в останню.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python є високорівневою об'єктно-орієнтованою мовою програмування, яка широко застосовується в інженерній практиці для розробки серверного ПЗ, систем автоматизації та алгоритмів комп'ютерного зору. Завдяки простому синтаксису, динамічній типізації та інтерпретованій природі мова оптимально підходить для швидкого прототипування і створення програмних модулів інтеграції відеопотоків.

Серед ключових переваг Python для систем відеоспостереження виділяють:

– логічний та зручний синтаксис, що спрощує читання та підтримку вихідного коду;

– кросплатформність і гнучкість, що дозволяє легко адаптувати високорівневу логіку до архітектури мережевих відеосерверів;

– динамічну типізацію, яка полегшує передачу та обробку масивів даних від камери до сервера;

– потужну екосистему бібліотек, що критично важливо для задач обробки відео у реальному часі.

До обмежень мови відносять підвищене споживання обчислювальних ресурсів порівняно з низькорівневими мовами (наприклад, C++), проте це компенсується швидкістю розробки та можливістю підключення оптимізованих модулів.

Сфери застосування Python у проекті:

1. Розробка серверної архітектури – управління взаємодією між мережевими відеосерверами та клієнтськими додатками.

2. Обробка потокового відео – реалізація алгоритмів аналізу кадрів, детекції подій та оптимізації передачі відеосигналів стандарту HD-SDI.

3. Автоматизація тестування та моніторингу – створення скриптів для перевірки стабільності передачі даних по мережі.

Для реалізації систем відеоспостереження та обробки сигналів на Python використовуються профільні бібліотеки:

– OpenCV-Python – базовий інструмент для комп'ютерного зору, цифрової обробки зображень та аналізу відеопотоків у реальному часі;

– NumPy – забезпечує ефективне управління багатовимірними масивами та числовими даними (кадрами відео);

– Matplotlib та Pandas – застосовуються для візуалізації статистичних даних про роботу мережевих відеосерверів та стану каналів зв'язку.

Для написання, дебагінгу та тестування програмного забезпечення системи відеоспостереження використовуються сучасні середовища розробки, зокрема PyCharm та інші кросплатформні редактори коду.

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 відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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

HD-SDI

Технології мовлення стрімко розвиваються, і мовники шукають способи побудови більш гнучкої, масштабованої та готової до майбутнього інфраструктури. Хоча традиційний SDI був основою професійної передачі відео протягом десятиліть, сучасні виробничі середовища дедалі більше вимагають віддаленої співпраці, спільного використання ресурсів та більшої операційної гнучкості.

Цей зсув прискорив впровадження SDI поверх IP, що дозволяє мовникам передавати професійні відео, аудіо та допоміжні дані через керовані IP-мережі, зберігаючи при цьому якість і надійність, необхідні для трансляційних операцій.

На відміну від традиційних інфраструктур SDI, які в основному покладаються на спеціалізоване кабельне з’єднання «точка-точка», HD-SDI over IP використовує високошвидкісні мережі Ethernet для передачі медіа між виробничими місцями та системами. Незалежно від того, чи розгортається воно для прямого ефіру, віддаленого виробництва, багатолокаційного мовлення чи розширення інфраструктури, мовлення через IP може забезпечити мовникам більш адаптивний шлях до сучасних виробничих робочих процесів.

У цьому розділу пояснюється, як працює SDI over IP, які стандарти мовлення використовуються, його основні переваги та обмеження, а також коли це правильний вибір для професійного мовного центру.

Розуміння SDI та причини переходу мовників на SDI через IP

Послідовний цифровий інтерфейс, або SDI, є одним з основних сигнальних інтерфейсів у телерадіомовній галузі з кінця 1980-х років. Розроблений для передачі нестисненого цифрового відео, вбудованого аудіо та допоміжних даних з передбачуваною продуктивністю та дуже низькою

затримкою, SDI став кращою технологією для підключення камер, виробничих комутаторів, серверів відтворення, маршрутизаторів, моніторів та іншого телерадіомовного обладнання. З часом стандарт еволюціонував від SD-SDI до HD-SDI, 3G-SDI, 6G-SDI та 12G-SDI, підтримуючи поступово вищу роздільну здатність та частоту кадрів. Незважаючи на ці зміни, базова інфраструктура залишилася практично незмінною: виділені коаксіальні кабелі з опором 75 Ом, що з'єднують один пристрій або порт маршрутизатора з іншим.

Ця архітектура продовжує забезпечувати надійну та детерміновану продуктивність. Однак сучасні мовники все частіше працюють на розподілених об'єктах, віддалених виробничих майданчиках, спільних диспетчерських та гібридних локальних та хмарних середовищах. Ці робочі процеси вимагають більшої гнучкості, ніж завжди можуть забезпечити традиційні інфраструктури SDI "точка-точка". SDI over IP пропонує практичний шлях міграції. Замість негайної заміни існуючого обладнання SDI, мовники можуть використовувати IP-шлюзи та інтерфейси медіамереж для інтеграції джерел та пунктів призначення SDI з керованими IP-інфраструктурами.

Цей перехід зумовлений кількома факторами:

– Зростаючий попит на віддалене виробництво та робочі процеси REMI.

– Міграція до програмно-визначених систем мовлення.

– Ширше використання розподіленої та хмарно-підключеної обробки медіа.

– Легше розширення інфраструктури без значної перемонтажі.

– Покращений розподіл виробничих ресурсів між кількома об'єктами.

– Більш гнучка маршрутизація та моніторинг сигналів.

– Впровадження таких стандартів, як SMPTE ST 2022 та SMPTE ST 2110.

Для багатьох мовників перехід відбувається поступово. Існуюче обладнання SDI продовжує підтримувати локальний збір, обробку та моніторинг, тоді як IP-мережі забезпечують масштабований транспорт, маршрутизацію та спільний доступ до ресурсів між системами та локаціями.

3.2 Розробка структурної схеми

На високому рівні, HD-SDI over IP перетворює або відображає професійні медіасигнали в IP-пакети, які можуть передаватись через належним чином спроектовану мережу Ethernet з високою пропускною здатністю.

На відміну від споживчого потокового відео, професійне мовлення через IP розроблено з урахуванням таких вимог, як низька затримка, точна синхронізація, передбачувана доставка пакетів, резервування та безперервна робота.

Типовий робочий процес включає наступні етапи.

1. Захоплення сигналу SDI.

Процес починається з джерела SDI, такого як:

– Трансляційні камери.

– Відеосервери.

– Перемикачі виробництва.

– Генератори символів.

– Системи повторного відтворення.

Кожен пристрій виводить нестиснений SDI-сигнал, що містить відео, вбудований звук та допоміжні дані.

2. Інкапсуляція IP.

Шлюз перетворює потік SDI на IP-пакети, зберігаючи інформацію про синхронізацію та метадані. Така інкапсуляція дозволяє сигналу проходити через стандартну інфраструктуру Ethernet без зміни його вмісту.

Професійний шлюз SDI-IP може підключити існуюче обладнання SDI до виробничої мережі SMPTE ST 2110, зберігаючи при цьому встановлені робочі процеси мовлення.

Багато професійних систем підтримують SMPTE ST 2110 або SMPTE ST 2022, що забезпечує сумісність обладнання різних виробників.

3. Мережевий транспорт.

Після інкапсуляції потік передається через керовані комутатори Ethernet другого або третього рівня.

На відміну від традиційної SDI-маршрутизації, IP-мережі дозволяють кільком пунктам призначення одночасно отримувати один і той самий сигнал без необхідності додаткових фізичних виходів. Це значно покращує гнучкість маршрутизації, одночасно зменшуючи складність апаратного забезпечення.

Сучасні IP-мережі мовлення також підтримують механізми резервування, які захищають від втрати пакетів та збоїв мережі, забезпечуючи безперебійне пряме мовлення.

4. Синхронізація.

Точна синхронізація залишається важливою у професійному мовленні.

Такі технології, як Precision Time Protocol (PTP), визначений у SMPTE ST 2059, синхронізують усі пристрої в мережі, замінюючи традиційні генератори чорних пакетів або трирівневих синхронізацій.

В результаті, комутація відео, синхронізація аудіо та багатокамерне виробництво залишаються точними навіть у великих IP-інфраструктурах.

5. Реконструкція сигналу.

На приймальному кінці інший шлюз реконструює оригінальний сигнал SDI з вхідних IP-пакетів.

Для виробничого обладнання сигнал виглядає ідентичним звичайному SDI-з'єднанню, що дозволяє існуючим камерам, моніторам та комутаторам продовжувати роботу без модифікацій.

Такий гібридний підхід дозволяє мовникам поступово модернізувати інфраструктуру, водночас захищаючи попередні інвестиції в обладнання SDI.

Основні переваги SDI через IP для робочих процесів відеонагляду

Оскільки операції мовлення стають дедалі більш розподіленими, SDI через IP надає кілька переваг порівняно з традиційними інфраструктурами SDI "точка-точка".

Більша масштабованість є однією з найважливіших переваг. Розширення об'єкта SDI часто вимагає додаткових маршрутизаторів, кабелів та спеціалізованого обладнання. Натомість, системи на основі IP можуть зростати за рахунок збільшення ємності мережі, що робить розширення швидшим та економічно ефективнішим.

Підвищена гнучкість дозволяє мовникам направляти будь-яке джерело практично до будь-якого пункту призначення за допомогою програмно-визначеного мережевого керування замість фіксованих фізичних з'єднань. Це спрощує зміни у виробництві та зменшує складність експлуатації.

Ще однією важливою перевагою є нижчі витрати на інфраструктуру. Використовуючи стандартні комутатори Ethernet та комерційне мережеве обладнання, мовники зменшують залежність від власного обладнання для маршрутизації, водночас краще використовуючи існуючу IT-інфраструктуру.

Дистанційне виробництво також стало набагато простішим. Завдяки трансляції через IP-адресу, виробничі команди можуть отримувати доступ до сигналів з різних об'єктів або місць проведення заходів, не транспортуючи велику кількість обладнання, що зменшує витрати на поїздки та підвищує операційну ефективність.

Зрештою, готовність до майбутнього робить HD-SDI поверх IP привабливою довгостроковою інвестицією. Оскільки UHD, HDR, висока частота кадрів та хмарне виробництво продовжують розвиватися, IP-інфраструктури забезпечують масштабованість, необхідну для підтримки нових технологій мовлення без значної заміни обладнання.

SDI проти SDI через IP: у чому різниця?

Хоча обидва підходи передають професійні медіасигнали, SDI та SDI over IP суттєво відрізняються інфраструктурою, маршрутизацією, масштабованістю та експлуатаційними вимогами.

Традиційний SDI залишається надійним вибором для компактних студій, фіксованих робочих процесів та застосувань, що вимагають простих та

передбачуваних шляхів проходження сигналу. SDI over IP краще підходить для масштабованих, розподілених та програмно-визначених середовищ.

Рішення не повинно ґрунтуватися виключно на тому, що є новішим – SDI чи IP. Слід враховувати розмір об'єкта, існуюче обладнання, вимоги до маршрутизації, наявну технічну експертизу, плани розширення та загальну вартість володіння.

Чи завжди SDI через IP є правильним вибором?

Хоча SDI поверх IP пропонує значні експлуатаційні переваги, це не обов'язково ідеальне рішення для кожного мовного центру.

Менші студії з обмеженою кількістю джерел та цільових пристроїв можуть продовжувати отримувати переваги від традиційного SDI. Ці системи звичні, передбачувані, прості в усуненні несправностей та можуть вимагати менше специфічних для мережі знань.

Для підприємств зі стабільними робочими процесами та обмеженими очікуваннями щодо майбутнього розширення, перехід на інтелектуальну власність може не забезпечити негайної окупності інвестицій.

Однак середнім та великим мовникам може знадобитися підтримка:

– Багатофабричне виробництво.
– Дистанційний внесок.
– Спільні виробничі ресурси.
– Централізований моніторинг.
– Гнучка маршрутизація.
– UHD та формати з вищою пропускною здатністю.
– Інтеграція з програмно-визначеною обробкою.
– Поступове підключення до хмари.

У цих середовищах SDI поверх IP може забезпечити масштабованість та операційну гнучкість, яких стає дедалі важче досягти за допомогою традиційної інфраструктури "точка-точка".

Технічна експертиза є ще одним важливим фактором. Проектування та підтримка надійної IP-мережі відеонагляду вимагає знань у сфері багатоадресної

розсилки, QoS, VLAN, планування пропускної здатності, безпеки мережі, резервування, PTP та моніторингу потоків медіа.

Для багатьох мовників гібридне розгортання є найбільш практичною стратегією. Існуюче обладнання SDI може продовжувати підтримувати локальне виробництво, тоді як IP-шлюзи та мережева інфраструктура забезпечують транспортування сигналу, спільний доступ до ресурсів, віддалені робочі процеси та майбутнє розширення.

Отже, рішення не є просто SDI чи IP. Мета полягає в тому, щоб побудувати інфраструктуру, яка пропонує належний баланс надійності, продуктивності, гнучкості, вартості та довгострокової цінності.

Індустрія відеонагляду неухильно рухається до більш гнучких, мережевих та програмно-керованих виробничих середовищ. SDI over IP забезпечує практичний спосіб передачі професійних медіафайлів через керовані мережі, одночасно інтегруючи існуюче обладнання SDI із сучасною виробничою інфраструктурою.

Традиційний SDI продовжує забезпечувати надійну, низькозатримувальну та передбачувану продуктивність, особливо в компактних та стабільних середовищах. Однак розширення великого об'єкта SDI може вимагати значної додаткової кабельної мережі, маршрутизації та обладнання.

Транслюючи HD-SDI через IP-мережі, мовники можуть отримати гнучкішу маршрутизацію, легше розширення інфраструктури, покращений спільний доступ до ресурсів та кращу підтримку віддаленого виробництва.

ST 2022-6 та ST 2110 забезпечують різні шляхи міграції. ST 2022-6 передає повний сигнал SDI через IP, тоді як ST 2110 передає відео, аудіо та допоміжні дані як окремі синхронізовані потоки.

Замість того, щоб розглядати SDI та IP як конкуруючі технології, багато мовників поєднують їх у гібридних інфраструктурах. Такий підхід захищає існуючі інвестиції, водночас створюючи контрольований шлях до масштабованого виробництва на основі IP.

Структурна схема системи зображена на рисунку 3.1.



Рисунок 3.1 – Структурна схема системи

3.3 Розробка функціональної схеми

На рисунку 3.2 наведено функціональну схему розробленого програмно-апаратного комплексу. Проєктована цифрова система відеоспостереження забезпечує виконання таких ключових вимог:

– високу роздільну здатність і якість відтворення відеопотоків стандарту HD-SDI;

– оперативний доступ до розподілених відеоархівів через мережеві відеосервери;

– підтримку цифрового збільшення та покадрового масштабування зображення без втрати критичних деталей;

– швидкий індексний пошук фрагментів за камерою, міткою часу та датою;

– можливість інтеграції із суміжними підсистемами комплексної безпеки об'єкта;

– ефективну та масштабовану трансляцію відеоданих по IP-каналах

зв'язку;

– автоматизовану розсилку тривожних сповіщень (на електронну пошту та через SMS-шлюзи);

– експорт відеоінформації на стандартизовані зовнішні носії.

Основні функціональні модулі системи:

1. Моніторинг та мультиекранне відображення Забезпечує підключення та синхронне виведення відеопотоків на монітори оперативного складу з можливістю розподілу на два чи більше дисплеїв. Використання апаратного прискорення дозволяє транслювати зображення з максимальним збереженням деталізації. Реалізовано багаторівневе цифрове масштабування (в 2, 4, 8 і 16 разів) та супроводження подій аудіосигналами (за наявності периферийного обладнання).

2. Архівація та запис Компресія відеопотоків здійснюється за допомогою ефективних алгоритмів стиснення, що забезпечує оптимальний бітрейт за високої деталізації кадру. Підтримуються гнучкі режими запису: за детекцією руху, за зовнішньою командою, безперервний режим, а також попередній запис (Pre-alarm) та дозапис (Post-alarm) для кожної камерної лінії.

3. Детекція руху Інтегрований програмний детектор виконує безперервний моніторинг динамічних об'єктів у кадрі. Перевагами рішення є висока стійкість до хибних спрацьовувань (перешкодозахищеність), емпіричне калібрування за контрастністю та габаритами об'єктів, налаштування незалежних зон детекції для кожної камери, візуальне маркування контурів рухомих об'єктів та динамічний перерозподіл обчислювальних ресурсів сервера для тривожних каналів.

4. Відтворення та аналіз архіву Дозволяє здійснювати одночасний перегляд архівних матеріалів паралельно із записом нових даних. Система виконує індексування бази даних при завантаженні, забезпечує часовий пошук, відображення інтенсивності запису за добу, реверсивне та покадрове відтворення, а також прискорення візуалізації до 25 кадрів за секунду (Fps). Передбачено утиліту зовнішнього декодування для збереження фрагментів у

контейнери формату AVI з метою їх подальшого відтворення на сторонніх робочих станціях.

5. Вбудований Web-сервер Надає віддаленим операторам і адміністраторам повноцінний інтерфейс для моніторингу камер, перегляду архівних даних, а також керування режимами охорони через стандартний веббраузер без встановлення додаткового клієнтського ПЗ.

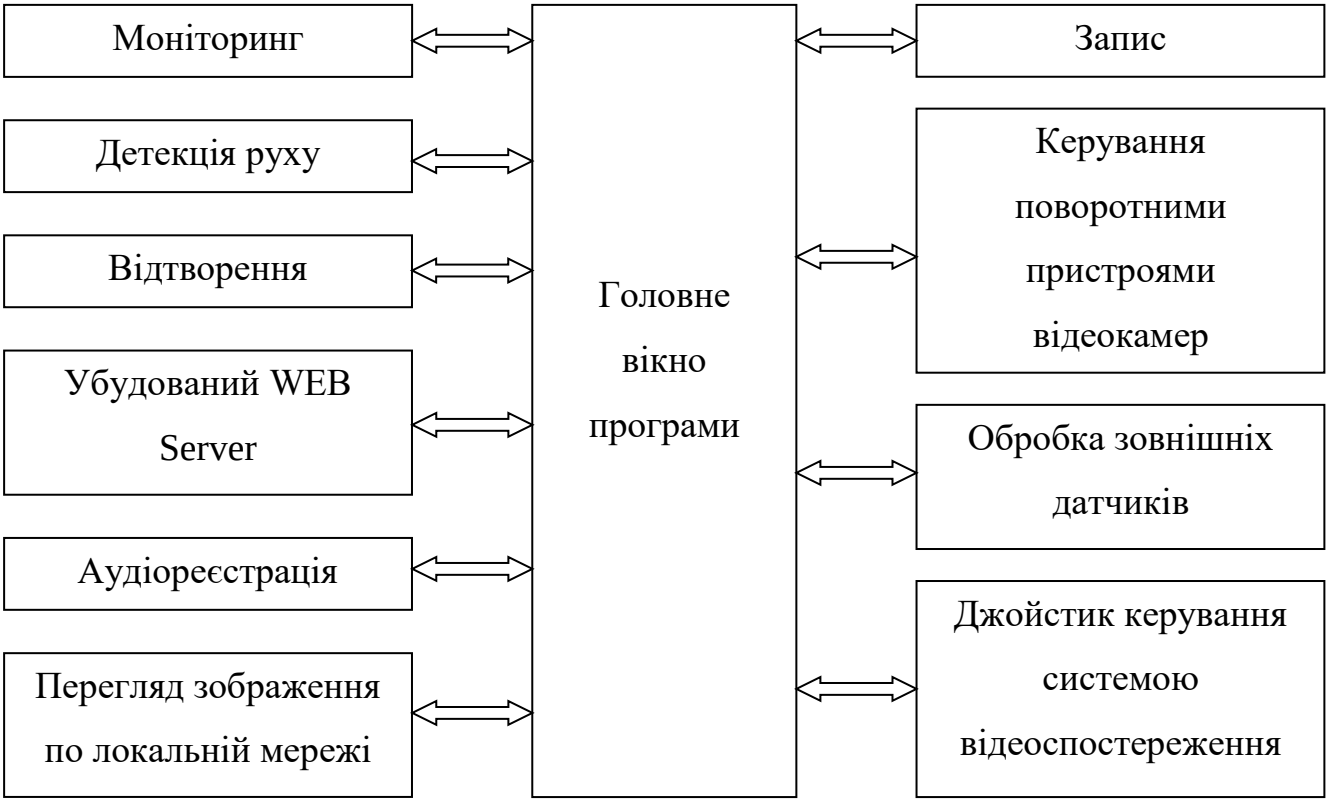


Рисунок 3.2 – Функціональна схема системи

6. Аудіореєстрація Здійснює прийом, оцифрування та синхронний запис аналогових аудіосигналів із зовнішніх джерел (мікрофонів, лінійних виходів). Синхронізація аудіо- та відеопотоків дозволяє проводити глибший аудит і контроль на об'єктах підвищеної безпеки (переговорні кімнати, спеціалізовані зони тощо). Для забезпечення високої розбірливості звуку передбачено використання якісного тракту попереднього підсилення.

7. Мережевий режим (віддалені робочі місця) Архітектура кліент-сервер

дозволяє розгортати віддалені пости моніторингу, інтерфейс яких повністю ідентичний серверному. Передача стислого потоку через мережу забезпечує повноцінний доступ до управлінських функцій, перегляду архівів та аудіосупроводу з урахуванням пропускної спроможності каналів зв'язку.

8. Керування поворотними пристроями (PTZ) Програмне забезпечення підтримує інтеграцію з поворотними платформами відеокамер, забезпечуючи їх оперативне позиціонування та панорамування безпосередньо з робочого місця оператора.

9. Обробка зовнішніх тривожних датчиків Модуль інтеграції з периферійними пристроями дозволяє контролювати стан охоронних і пожежних датчиків, а також автоматично активувати виконавчі механізми (сирени, світлові сповіщувачі тощо) при спрацьовуванні тривожних сценаріїв.

10. Спеціалізовані маніпулятори (джойстики) керування Для підвищення надійності та захисту від несанкціонованого втручання операторів (зміни конфігурації ОС, встановлення стороннього ПЗ чи ігор) передбачено можливість заміни стандартних пристроїв введення (миші та клавіатури) на спеціалізований промисловий маніпулятор, який блокує доступ до операційної системи та взаємодіє виключно з інтерфейсом комплексу відеонагляду.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Діаграма взаємодії процесів системи, розробленої у результаті виконання магістерського проектування, наведена на рисунку 3.3. Після успішного запуску розробленого програмного забезпечення здійснюється ініціалізація головного управляючого модуля (Core Interface), через який реалізується доступ до ключових підсистем комплексу:

1. Інтерфейс користувача (GUI) – забезпечує візуалізацію робочого середовища, ергономічне компонування віконних панелей та загальне керування

функціоналом програмного забезпечення.

2. Модуль обробки та перехоплення помилок (Error Handler) – виконує моніторинг виключних ситуацій, логування збоїв у роботі ПЗ та стабілізацію системи при критичних навантаженнях.

3. Моніторинг отриманих даних – здійснює безперервний контроль над надходженням, буферизацією та актуальністю цифрових відеопотоків стандарту HD-SDI.

4. Файловий відеоархів – керує процесами запису, індексації, пошуку та довгострокового зберігання відзнятих матеріалів на носіях даних.

5. Керування системою відеоспостереження – відповідає за мультиекранний вивід, управління режимами запису, активацію детекторів руху та загальну логіку відеонагляду.

6. Керування поворотними пристроями відеокамер (PTZ Control) – реалізує інтерфейс позиціювання, панорамування та зміни фокусної відстані поворотних камер безпосередньо з робочого місця.

7. Обробка даних зовнішніх датчиків – забезпечує взаємодію з периферійними пристроями (охоронно-пожежною сигналізацією, тривожними кнопками та виконавчими реле).

8. Модуль конфігурації та налаштування ПЗ (Settings) – дозволяє змінювати параметри роботи системи, конфігурувати мережеві сокети, розподіляти права доступу та задавати алгоритми компресії.

9. Обробка мережних запитів – керує сокетами, передачею пакетів, стабільністю з'єднань та синхронізацією даних між сервером і віддаленими клієнтськими робочими місцями.

10. Вбудований Web-сервер – забезпечує віддалений доступ до потокового відео, архівів та параметрів безпеки через стандартизовані інтернет-браузери без необхідності встановлення спеціалізованого клієнтського ПЗ.

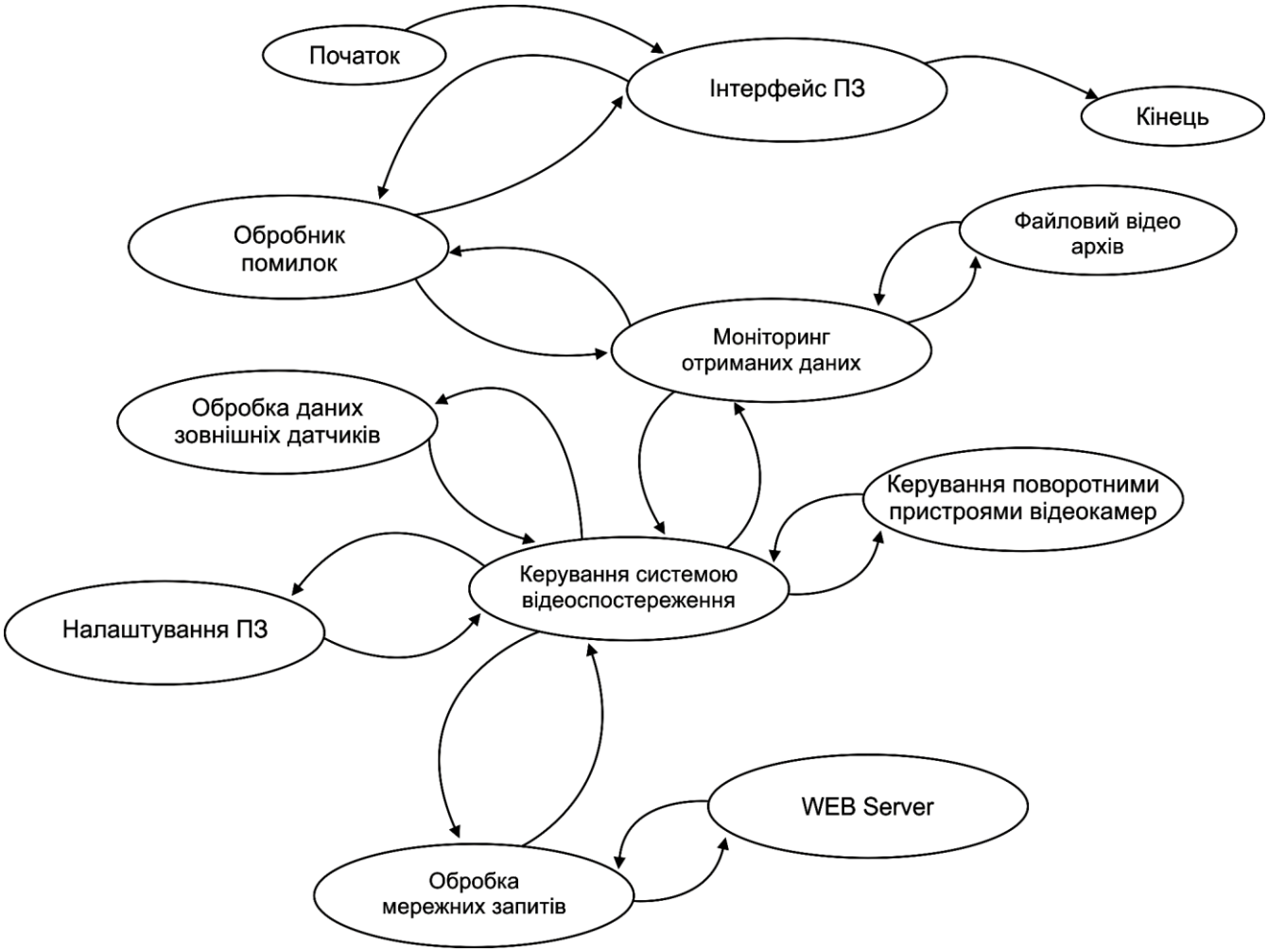


Рисунок 3.3 – Діаграма взаємодії процесів

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 системи відеонагляду на основі HD-SDI та мережевих відеосерверів ґрунтується на послідовному прийманні цифрового відеосигналу, його перетворенні у формат, придатний для передавання мережею, подальшому зберіганні та наданні доступу користувачам.

Основним завданням алгоритмічного забезпечення є узгодження роботи відеокамер, апаратних пристроїв захоплення, мережевих відеосерверів і програмних модулів перегляду.

Особливу увагу необхідно приділити безперервності оброблення відеопотоків, контролю стану джерел сигналу, керуванню архівом та обмеженню доступу до відеоданих. Для цього пропонується використовувати модульну структуру, у якій кожен функціональний компонент виконує визначені операції та передає результати наступному етапу оброблення.

Загальна організація системи передбачає підключення HD-SDI відеокамер до відповідних приймальних пристроїв за допомогою коаксіальних ліній зв'язку. HD-SDI забезпечує передавання нестисненого цифрового відеосигналу, а мережевий відеосервер здійснює його приймання, кодування та розповсюдження через IP-мережу.

Загальну блок-схему функціонування програмного комплексу передбачено на рисунку 4.1.

Вона відображає послідовність оброблення сигналу від відеокамери до програмних компонентів зберігання й віддаленого перегляду. Такий підхід дозволяє використовувати цифрові відеокамери із послідовним інтерфейсом у складі мережевої системи спостереження.

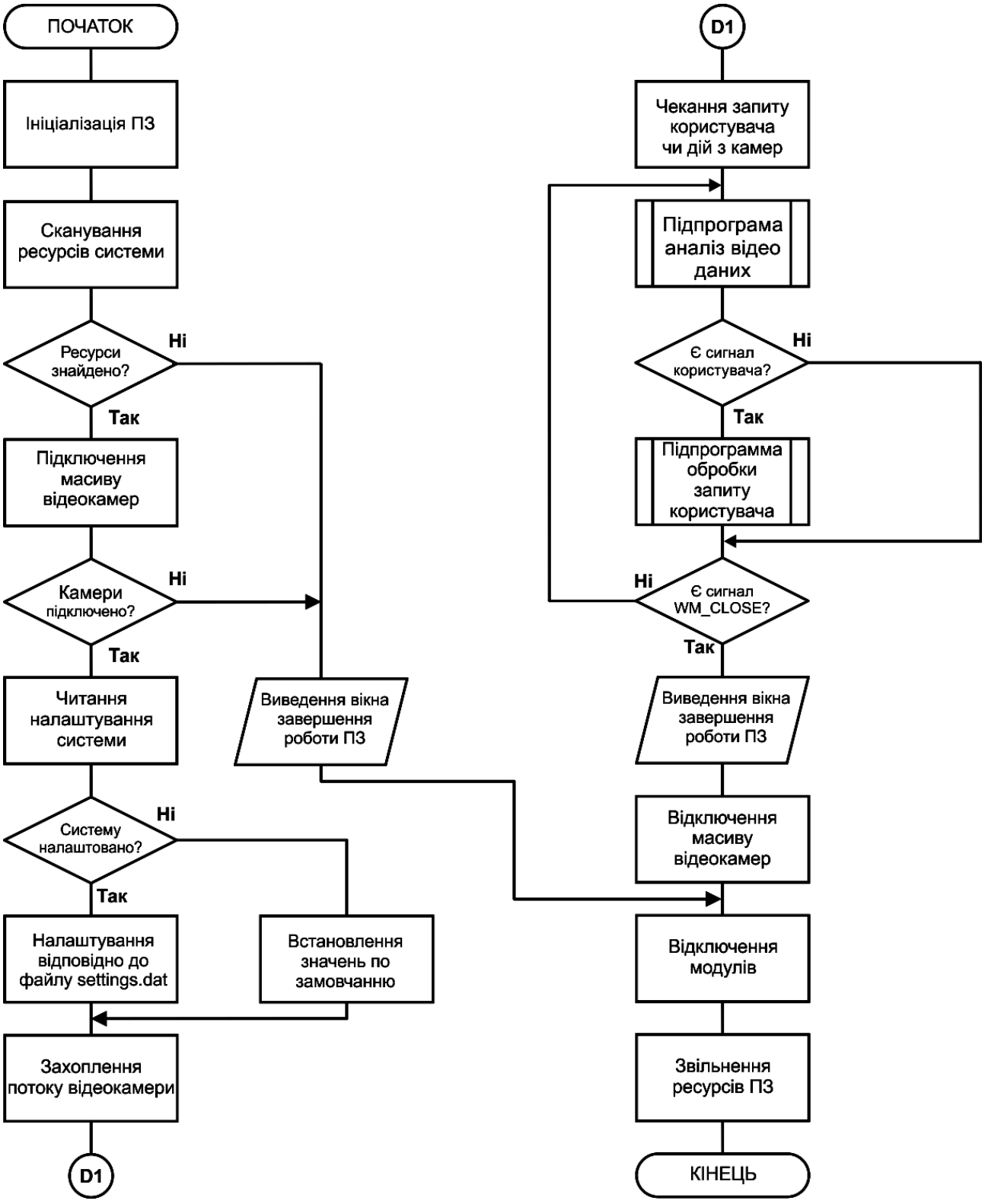


Рисунок 4.1 – Блок схема основної програми

Особливістю HD-SDI є передавання цифрових відеоданих без застосування компресії безпосередньо в інтерфейсі камери. Відповідно до SMPTE ST 292-1 для

такого інтерфейсу використовуються швидкості 1,485 Гбіт/с або 1,485/1,001 Гбіт/с. Це накладає вимоги на фізичний тракт і обладнання захоплення.

Проте наведена швидкість не визначає навантаження на IP-мережу після відеокодування. Мережевий потік формується окремим компонентом і залежить від вибраного кодека, параметрів зображення та режиму компресії. Відокремлення цих характеристик необхідне для правильного розрахунку пропускної здатності й дискового простору.

Для програмної реалізації доцільно виділити підсистему контролю приймання відеосигналу. Її завдання полягає у визначенні наявності сигналу, перевірці параметрів відеоформату, контролі надходження кадрів та передаванні відеоданих модулю кодування.

Роботу окремої підпрограми приймання й контролю відеопотоку передбачено на рисунку 4.2.

Алгоритмічна модель повинна враховувати тимчасову втрату сигналу, повторне встановлення з'єднання з пристроєм захоплення та відновлення оброблення без необхідності перезапуску всієї системи.

Проєктне рішення щодо організації приймання HD-SDI відеосигналів

Початковим етапом функціонування системи є отримання цифрового відеосигналу від підключених камер. Для цього використовується апаратний пристрій із підтримкою HD-SDI, який забезпечує приймання послідовного цифрового потоку та його подальше передавання до програмного середовища.

Таким пристроєм може бути плата відеозахоплення або автономний HD-SDI відеокодер. Вибір визначається необхідною кількістю каналів, підтримуваними відеоформатами та можливостями програмної інтеграції.

У варіанті з платою відеозахоплення оброблення відеокадрів здійснюється на сервері, до якого підключено обладнання. Програма отримує дані через драйвер або програмний інтерфейс виробника. Якщо використовується автономний мережевий відеокодер, перетворення HD-SDI сигналу в стиснений потік відбувається безпосередньо в апаратному пристрої.

У такому випадку сервер приймає вже сформований мережевий відеопотік. Обидва варіанти забезпечують можливість мережевого відеонагляду, але відрізняються розподілом обчислювального навантаження.

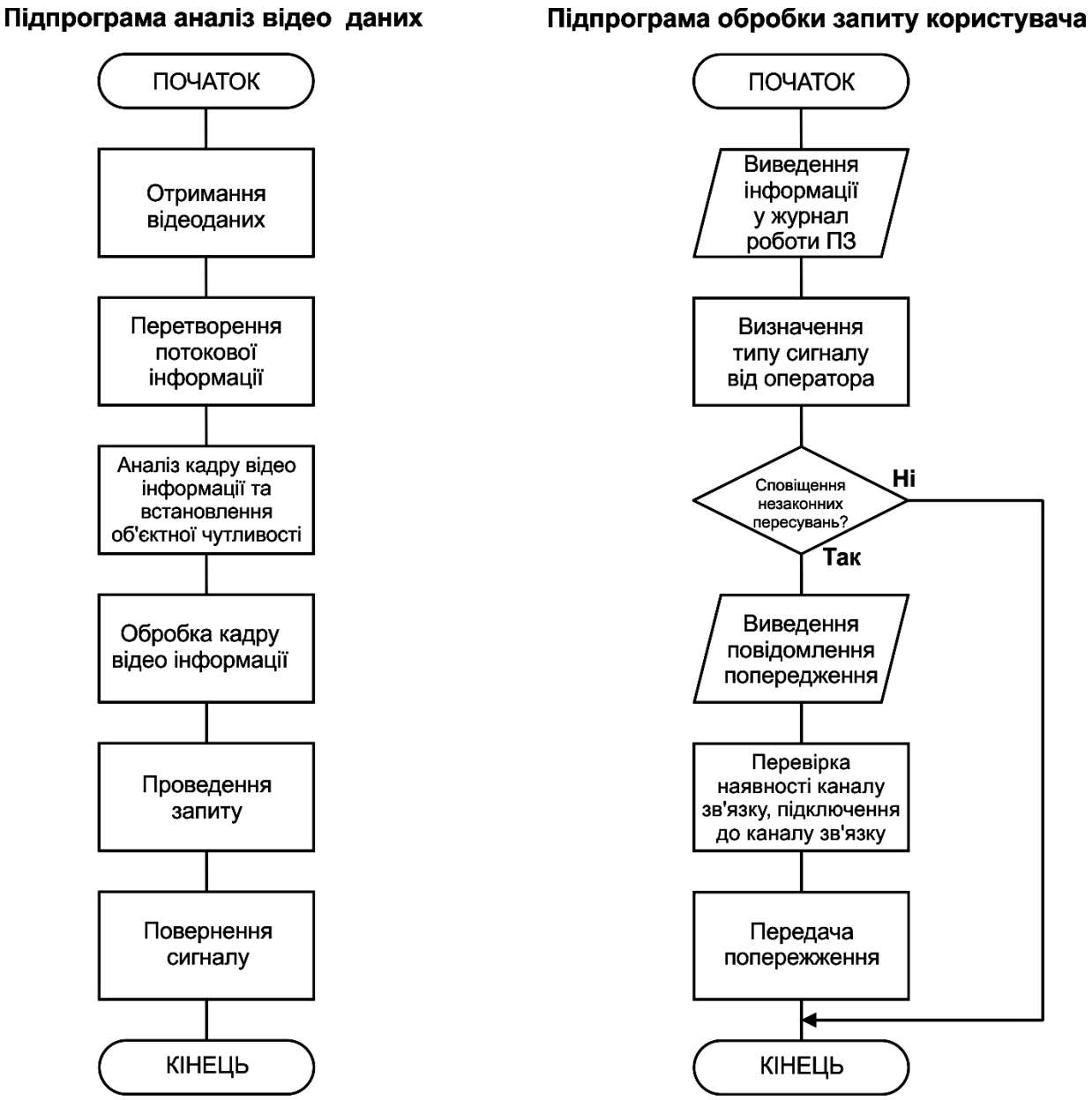


Рисунок 4.2 – Блок схема підпрограм

Для кожної камери необхідно створити конфігураційний запис, який містить унікальний ідентифікатор, номер фізичного каналу, очікуваний відеоформат і параметри оброблення. Додатково визначається мережевий

відеосервер, відповідальний за приймання потоку. Такий запис дозволяє пов'язати фізичне обладнання з логічним об'єктом програмної системи.

Процедура ініціалізації починається з отримання переліку доступних пристроїв. Після цього здійснюється перевірка відповідності апаратних каналів конфігураційним записам. Для кожного активного каналу визначається можливість приймання відеосигналу. Якщо обладнання підтримує отримання параметрів вхідного формату, система повинна перевірити роздільну здатність, частоту кадрів і режим розгортки.

HD-SDI використовується для передавання визначених форматів цифрового відео, тому налаштування приймального пристрою повинні відповідати параметрам сигналу. Наприклад, прогресивне та черезрядкове зображення потребують правильного трактування формату кадрів. Якщо отримані характеристики не відповідають можливостям пристрою захоплення, відповідний канал необхідно перевести в стан помилки.

Для опису працездатності каналу доцільно використовувати модель скінченного автомата зі станами DISCONNECTED, INITIALIZING, STREAMING, SIGNAL_LOST та ERROR. Стан DISCONNECTED відповідає відсутності доступного пристрою. Після початку ініціалізації виконується перехід до INITIALIZING. За умови успішного встановлення приймання система переходить до STREAMING.

Якщо відеокадри перестають надходити протягом встановленого інтервалу, канал переводиться в стан SIGNAL_LOST. У цьому стані запускається процедура повторної перевірки фізичного сигналу та доступності пристрою. Після відновлення надходження кадрів система повертається до робочого стану. Якщо відновлення не відбувається або пристрій повертає критичну помилку, необхідно сформувати відповідний діагностичний запис.

Важливо розділяти втрату HD-SDI сигналу та відмову програмного компонента. У першому випадку приймальний пристрій залишається доступним, але не отримує коректного відеосигналу. У другому випадку може бути втрачено

доступ до драйвера, апаратного інтерфейсу або мережевого відеокодера. Ці ситуації потребують різних процедур відновлення.

Для запобігання необмеженому накопиченню даних між приймальним і наступним модулем доцільно використовувати буфер кадрів обмеженої місткості. Його розмір визначається частотою надходження кадрів та допустимою затримкою оброблення. Якщо наступний програмний компонент не встигає отримувати дані, алгоритм повинен застосовувати визначену політику переповнення. Для оперативного перегляду допустимим рішенням є відкидання найстаріших кадрів. Для архівного запису така політика не повинна використовуватися без фіксації втрат, оскільки вона порушує повноту відеоархіву.

Математична модель формування та передавання мережевого відеопотоку

Після приймання HD-SDI сигналу необхідно сформувати мережеве представлення відеоданих. У випадку використання плати захоплення ця операція передбачає отримання відеокадрів і подальше кодування. Для автономного HD-SDI відеокодера відповідні операції виконуються апаратним пристроєм, а мережевий сервер забезпечує приймання, реєстрацію та оброблення створеного потоку.

Універсальну послідовність відеокадрів можна визначити як

$$V = \{F_0, F_1, \dots, F_{(N-1)}\},$$

де F_i є окремим кадром, а N визначає кількість отриманих кадрів за час спостереження.

Кожен кадр характеризується роздільною здатністю, форматом пікселів і часовою міткою. Для прогресивного відео тривалість між сусідніми кадрами за сталої частоти визначається співвідношенням

$$\Delta t = (1)/(f),$$

де f позначає частоту кадрів. Для черезрядкових форматів необхідно враховувати співвідношення між частотою полів і частотою повних кадрів.

Нестиснений відеопотік може створювати значне навантаження на пам'ять і внутрішні канали передавання. Для орієнтовного розрахунку швидкості потоку активних пікселів можна використати формулу

$$R_{\text{raw}} = W \cdot H \cdot b \cdot f,$$

де W і H визначають ширину й висоту кадру в пікселях, b є середньою кількістю бітів на піксель для вибраного представлення даних, а f характеризує частоту кадрів.

Отримане значення визначає лише розрахункову швидкість передавання активних відеоданих. Воно не враховує службові інтервали, синхронізацію та особливості серіалізації HD-SDI. Тому для розрахунку фізичного інтерфейсу необхідно використовувати параметри відповідного стандарту, а для оцінювання програмного навантаження слід враховувати формат кадрів, який фактично надається пристроєм захоплення.

Для зменшення обсягу даних доцільно використовувати відеокодування H.264 або H.265 за умови їх підтримки вибраним обладнанням. Алгоритм кодування виконує просторове та міжкадрове стискання, завдяки чому передаваний потік зазвичай має суттєво менший обсяг порівняно з нестисненим представленням.

Важливою характеристикою мережевого відеопотоку є бітрейт. Його можна визначити як відношення кількості переданих бітів до тривалості спостереження

$$R_v = (B_v)/(T),$$

де B_v визначає загальну кількість бітів закодованого відео, а T є тривалістю відповідного фрагмента.

Значення бітрейту залежить від параметрів кодера, динаміки сцени та обраного режиму керування якістю. За постійного бітрейту система прагне підтримувати встановлену швидкість передавання. За змінного бітрейту обсяг даних може суттєво змінюватися залежно від складності зображення. Для проєктування мережі та архіву необхідно враховувати ці коливання.

У випадку одночасної роботи декількох відеоканалів сумарне навантаження на мережевий інтерфейс сервера визначається як

$$R_{(\Sigma)} = \sum (i = 1)^{(K)} R_i + R_{\text{overhead}},$$

де K є кількістю активних каналів, R_i визначає швидкість відповідного потоку. Наведена формула повинна застосовуватися окремо для конкретного мережевого сегмента. Якщо сервер одночасно приймає відеопотоки та передає їх кільком клієнтам, вихідне навантаження необхідно розраховувати з урахуванням кількості одержувачів і способу розповсюдження. Використання серверної ретрансляції може зменшити кількість прямих підключень до відеокодера, але не усуває навантаження на мережу між сервером та клієнтами.

Для передавання відео може використовуватися RTP, а керування потоковими сеансами може здійснюватися через RTSP. При цьому RTSP не є механізмом кодування кадрів. Його призначення полягає в організації та керуванні потоковим відтворенням. Конкретна версія RTSP, транспортний режим і сумісність із клієнтськими застосунками визначаються можливостями відеосервера.

Розроблення механізму приймання й контролю мережевих потоків

Мережевий відеосервер повинен підтримувати постійний контроль стану підключених джерел.

Для кожного потоку доцільно створювати окремий логічний об'єкт, який містить параметри підключення, поточний стан, час останнього отриманого кадру та кількість зафіксованих помилок. Після запуску підсистеми приймання виконується перевірка конфігурації джерела.

Далі встановлюється мережеве з'єднання та ініціюється отримання потоку. У разі успішного підключення сервер починає приймати медіапакети й передавати їх компонентам зберігання та перегляду. Якщо підключення не встановлено, запускається механізм повторних спроб.

Для контролю працездатності необхідно враховувати не лише стан транспортного з'єднання, а й фактичне надходження відеоданих. Наявність

відкритого мережевого сокета не гарантує, що відеокодер продовжує передавати кадри. Тому система повинна контролювати час останнього успішного отримання даних та визначати перевищення допустимого інтервалу очікування.

Механізм повторного підключення доцільно реалізувати зі збільшенням інтервалу між спробами. Такий підхід запобігає надмірному навантаженню на сервер і мережеве обладнання під час тривалих відмов. Відповідний інтервал можна розраховувати за формулою

$$t_k = \min\left(t_{(max)}, t_0 2^k\right),$$

де t_0 є початковою затримкою, k визначає номер повторної спроби, а $t_{(max)}$ межує максимальний час очікування.

Програмну реалізацію контролю потоку можна представити окремим класом Python. Він відстежує час надходження останнього кадру та визначає необхідність відновлення з'єднання.

Наведений приклад є алгоритмічною моделлю і не містить викликів конкретного HD-SDI обладнання або RTSP-клієнта.

```
from dataclasses import dataclass
from time import monotonic

@dataclass
class StreamMonitor:
    # Ідентифікатор камери та допустима пауза між кадрами
    camera_id: str
    timeout: float = 3.0
    def __post_init__(self):
        # Початковий стан каналу
        self.state = "INITIALIZING"
        self.last_frame_time = None
        self.failures = 0
    def on_frame(self):
        # Оновлюємо час останнього отриманого кадру
        self.last_frame_time = monotonic()
        self.state = "STREAMING"
        self.failures = 0
    def check_state(self):
        # Перевіряємо, чи надходили кадри
        if self.last_frame_time is None:
            return self.state
        elapsed = monotonic() - self.last_frame_time
        if elapsed > self.timeout:
            self.state = "SIGNAL_LOST"
        return self.state
    def reconnect_delay(self):
        # Обмежуємо кількість наростань затримки
        delay = min(30.0, 0.5 * 2 ** min(self.failures, 6))
        self.failures += 1
```

```
return delay
```

У наведеній реалізації використовується монотонний годинник, який не залежить від зміни системного часу. Це важливо для коректного визначення часових інтервалів. Метод on_frame() викликається після успішного приймання кадру. Метод check_state() визначає факт перевищення допустимої паузи, а reconnect_delay() повертає інтервал очікування перед наступною спробою.

Для повноцінної системи потрібно доповнити цей механізм перевіркою доступності мережевого пристрою, керуванням фактичним з'єднанням та реєстрацією подій. Після відновлення потоку сервер повинен визначити нові часові параметри й повідомити підсистему архівування про можливий розрив відеозапису.

Особливої уваги потребує оброблення змінних мережевих затримок. У випадку передавання RTP через UDP можливі втрати та зміна порядку надходження пакетів. Для правильного відтворення використовується буферизація й упорядкування відповідно до часових міток і номерів послідовності. Розмір буфера визначає компроміс між плавністю відтворення та затримкою.

Якщо буфер надто малий, тимчасові коливання затримки можуть спричинити втрату кадрів. Надмірний буфер збільшує затримку відображення. Тому для оперативного перегляду доцільно використовувати обмежену буферизацію, а для запису забезпечувати стабільне приймання й збереження максимально можливої кількості коректних даних. У разі перевищення доступних ресурсів система повинна фіксувати втрати, а не приховувати їх від адміністратора.

Реалізація підсистеми сегментованого архівування відеоданих

Однією з основних функцій системи відеонагляду є безперервне збереження відеоінформації з можливістю подальшого пошуку та відтворення.

Для цього необхідно організувати архівування потоків, отриманих від мережевих відеосерверів. Зберігання доцільно здійснювати окремими

відеофрагментами, які пов'язуються з відповідними камерами та часовими інтервалами.

Сегментований підхід дозволяє обмежити розмір окремих файлів, спростити очищення архіву й забезпечити пошук відеоданих за визначений проміжок часу. Тривалість сегмента встановлюється з урахуванням вимог до відтворення та організації дискової підсистеми. Надто короткі сегменти збільшують кількість файлів і службових операцій. Надто довгі можуть ускладнювати пошук та відновлення після аварійного завершення запису.

Для програмної реалізації сегментації можна використовувати FFmpeg або аналогічні бібліотеки оброблення мультимедійних потоків. У разі сумісності вхідного потоку з вибраним контейнером можливе збереження відеоданих без повторного кодування. Це дозволяє уникнути додаткового навантаження на процесор. При цьому межі сегментів необхідно узгоджувати з ключовими кадрами, оскільки довільне розділення міжкадрово закодованого відео може ускладнювати незалежне відтворення фрагментів.

Для кожного відеосегмента доцільно зберігати метадані, які містять ідентифікатор камери, початковий і кінцевий час, шлях до файлу, розмір і стан завершення запису. Окремо можуть зберігатися відомості про виявлені події та контрольна сума файлу. Метадані дозволяють організувати швидкий пошук без послідовного перегляду всього дискового сховища.

Процес запису необхідно розділити на створення нового сегмента, накопичення відеоданих та завершення файлу.

Поки запис триває, відповідний сегмент перебуває в активному стані. Після завершення запису необхідно коректно закрити контейнер, перевірити наявність файлу та оновити його метадані. Лише після цього сегмент може бути позначений як готовий до архівного відтворення.

Для запобігання втраті узгодженості між файловим сховищем та базою даних доцільно використовувати проміжний стан FINALIZING.

Він означає, що приймання даних до сегмента завершено, але його остаточне збереження ще не підтверджено. У разі аварійного завершення

програми такі сегменти повинні проходити повторну перевірку після запуску системи.

Програмний механізм розрахунку дискової місткості можна реалізувати мовою Python. Наведена функція дозволяє оцінити необхідний обсяг сховища за заданою кількістю камер, середнім бітрейтом, терміном зберігання та резервом.

```
def calculate_archive_size(
    cameras: int,
    bitrate_mbps: float,
    retention_days: int,
    reserve_percent: float = 20.0
) -> float:
    # Перевіряємо параметри розрахунку
    if cameras <= 0 or bitrate_mbps <= 0:
        raise ValueError("Некоректні параметри відеоканалів")

    if retention_days <= 0:
        raise ValueError("Некоректний термін зберігання")

    if reserve_percent < 0:
        raise ValueError("Резерв не може бути від'ємним")

    # Загальна швидкість усіх відеопотоків
    total_bitrate = cameras * bitrate_mbps * 1_000_000

    # Тривалість зберігання у секундах
    duration = retention_days * 24 * 3600

    # Розраховуємо обсяг відеоданих у байтах
    video_bytes = total_bitrate * duration / 8

    # Враховуємо додатковий резерв місткості
    required_bytes = video_bytes * (
        1 + reserve_percent / 100
    )

    # Повертаємо місткість у десяткових терабайтах
    return required_bytes / 1_000_000_000_000
```

Наведений розрахунок може використовуватися під час налаштування системи та визначення необхідного обсягу сховища. Функція формує орієнтовне значення й не замінює вимірювання фактичного розміру архіву. Для неоднорідних камер доцільно передавати окремі значення бітрейту кожного відеоканалу, оскільки параметри кодування можуть суттєво відрізнятися.

Контроль вільного простору необхідно реалізувати як окремий алгоритм. Він періодично отримує інформацію про доступну місткість дискового тому та порівнює її з установленими порогами. Якщо обсяг вільного простору

зменшується до критичного значення, система повинна ініціювати відповідну процедуру очищення або сформувати повідомлення адміністратору.

Для циклічного відеоархіву доцільно застосовувати політику видалення найстаріших сегментів після завершення встановленого строку зберігання. Однак видаленню не повинні підлягати активні файли та записи, позначені як необхідні для розслідування подій. Операція очищення має враховувати поточний стан сегмента, його строк зберігання та наявність адміністративного блокування.

Важливо забезпечити узгоджене видалення відеофайлів та їхніх метаданих. Якщо фізичний файл уже видалено, відповідний запис у базі даних не повинен залишатися доступним для відтворення. Якщо видалення не вдалося через помилку файлової системи, операцію необхідно зареєструвати для повторної обробки.

Для прискорення пошуку архівних фрагментів можна застосувати індексування за ідентифікатором камери та часовими мітками початку й завершення запису. Пошуковий запит повинен повертати сегменти, часові інтервали яких перетинаються із заданим періодом. Це дозволяє працювати з великим архівом без аналізу безпосереднього вмісту відеофайлів.

Розроблення механізму виявлення подій у відеозображенні

Додатковою функцією системи відеонагляду може бути автоматичне виявлення змін у контрольованій сцені. Такий механізм дозволяє формувати події для подальшого аналізу та пошуку відповідних фрагментів архіву. Для базового варіанта реалізації доцільно використовувати алгоритм виявлення руху на основі порівняння поточного кадру з фоновою моделлю.

Вхідними даними алгоритму є послідовність декодованих кадрів. Кожен кадр проходить попереднє оброблення, яке може включати зменшення роздільної здатності та перетворення у відтінки сірого. Це дозволяє скоротити обсяг обчислень, якщо для виявлення змін не потрібна повна колірна інформація.

Після підготовки кадру виконується визначення відмінностей між поточним зображенням і фоновою моделлю. Фон може формуватися адаптивно на основі попередніх кадрів. Отримана карта відмінностей перетворюється на

бінарну маску, у якій виділяються ділянки, що потенційно відповідають рухомим об'єктам.

Для зменшення впливу шумів доцільно застосовувати морфологічні операції. Вони дозволяють усувати дрібні ізольовані ділянки та об'єднувати суміжні області змін. Після цього визначаються контури або зв'язні компоненти бінарної маски. Ділянки, площа яких менша за встановлений поріг, виключаються з подальшого аналізу.

Для програмної реалізації такого алгоритму може застосовуватися бібліотека OpenCV. Вона надає засоби оброблення кадрів, побудови фонової моделі та аналізу контурів. Приклад функції виявлення руху наведено нижче.

```
import cv2

class MotionDetector:
    def __init__(self, min_area=900):
        # Формуємо адаптивну модель фону
        self.background = cv2.createBackgroundSubtractorMOG2(
            history=500,
            varThreshold=32,
            detectShadows=True
        )

        # Мінімальна площа області руху
        self.min_area = min_area

        # Матриця для морфологічного оброблення
        self.kernel = cv2.getStructuringElement(
            cv2.MORPH_RECT, (3, 3)
        )

    def detect(self, frame):
        # Отримуємо маску змін відносно фону
        foreground = self.background.apply(frame)

        # Відкидаємо тіні та слабкі зміни
        _, mask = cv2.threshold(
            foreground, 200, 255, cv2.THRESH_BINARY
        )

        # Видаляємо дрібні шумові компоненти
        mask = cv2.morphologyEx(
            mask, cv2.MORPH_OPEN, self.kernel
        )

        # Знаходимо контури потенційно рухомих об'єктів
        contours, _ = cv2.findContours(
            mask,
            cv2.RETR_EXTERNAL,
            cv2.CHAIN_APPROX_SIMPLE
        )

        # Перевіряємо площу виявлених областей
        for contour in contours:
```

```
            if cv2.contourArea(contour) >= self.min_area:
                return True

        return False
```

Запропонована реалізація ілюструє можливий механізм аналізу кадрів після їх декодування. Клас MotionDetector підтримує фонову модель між послідовними викликами. При виявленні області достатньої площі метод повертає True, що може використовуватися для формування події.

Для практичного використання механізм необхідно доповнити часовою фільтрацією. Одноразова зміна зображення не завжди свідчить про появу рухомого об'єкта. Причиною можуть бути коливання освітлення, цифрові шуми або короткочасне порушення декодування. Тому подію доцільно підтверджувати лише після виявлення руху протягом кількох послідовних кадрів.

Окремо слід передбачити можливість визначення зон спостереження. Адміністратор може задавати ділянки кадру, для яких виконується аналіз. Це дозволяє виключити області з постійним некритичним рухом. Координати таких зон доцільно зберігати у відносному вигляді, щоб забезпечити їх масштабування відповідно до роздільної здатності зображення.

Після підтвердження події система повинна сформувати запис із зазначенням камери, часу початку, типу події та пов'язаного відеофрагмента. За потреби можна зберігати окремий кадр для попереднього перегляду. Виявлення руху не слід автоматично ототожнювати з подією порушення безпеки, оскільки базовий алгоритм не визначає тип і наміри об'єкта.

Механізм аналізу доцільно виконувати незалежно від основного процесу архівування. Якщо оброблення кадру потребує більше часу, ніж доступний міжкадровий інтервал, аналітичний модуль може пропускати окремі кадри. При цьому основний відеопотік повинен продовжувати записуватися без залежності від швидкодії алгоритму виявлення руху.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Програмне забезпечення системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів призначене для централізованого приймання, оброблення, передавання та зберігання цифрових відеосигналів. Програма забезпечує взаємодію з пристроями відеозахоплення, керування мережевими потоками, організацію відеоархіву та віддалений перегляд зображення. Основою роботи є перетворення нестисненого HD-SDI сигналу на закодований відеопотік, придатний для передавання через IP-мережу. Головне вікно програми показано на рисунку 5.1.

Робоче середовище системи передбачає використання HD-SDI відеокамер, апаратних засобів приймання цифрових сигналів і мережевого сервера. Камери підключаються до відповідних приймальних пристроїв через коаксіальні лінії зв'язку. Для перетворення сигналу можуть застосовуватися плати відеозахоплення або автономні HD-SDI відеокодери.

У першому випадку кодування здійснюється серверним програмним забезпеченням. У другому випадку сервер отримує сформовані мережеві потоки від відеокодерів. Вибір схеми підключення визначається характеристиками наявного обладнання.

Для програмної реалізації серверної частини може використовуватися мова Python. Вона забезпечує оброблення конфігураційних параметрів, керування потоками та контроль стану підключених відеокамер.

Для роботи з мультимедійними даними доцільно застосувати FFmpeg, який підтримує приймання, кодування, перетворення та запис відеопотоків. Оброблення окремих кадрів і виявлення руху можна організувати засобами OpenCV. Зазначений набір компонентів відповідає запропонованому алгоритмічному рішенню та потребує узгодження з фактичною програмною реалізацією.

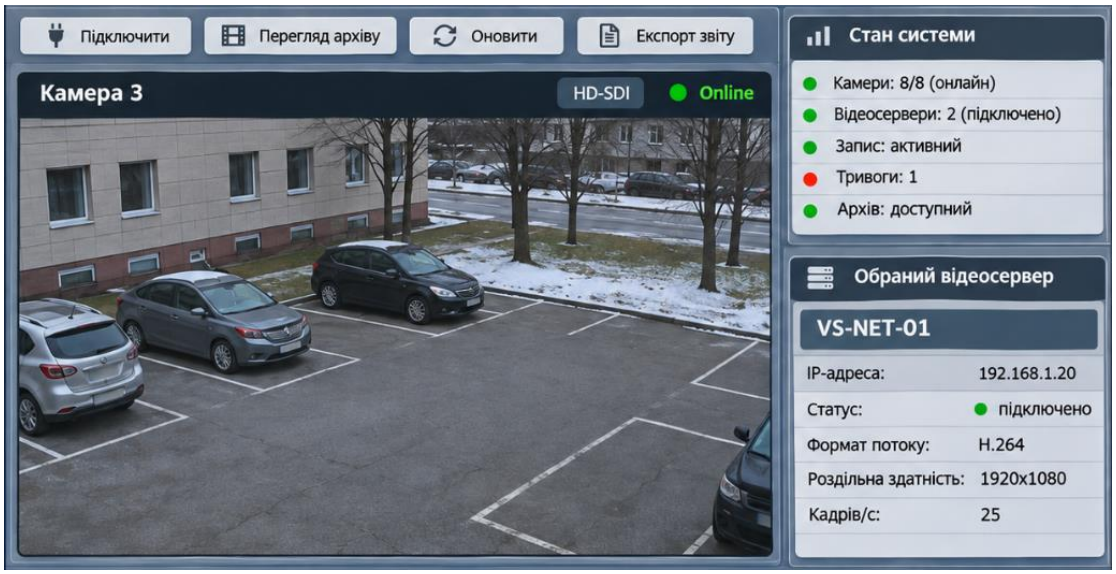


Рисунок 5.1 – Головне вікно ПЗ

Підготовка серверного середовища починається зі встановлення операційної системи, налаштування мережевих інтерфейсів і перевірки доступності обладнання. Для плат відеозахоплення необхідно встановити сумісні драйвери та переконатися, що система правильно визначає пристрої. Якщо використовуються автономні відеокодери, потрібно перевірити їхню доступність через IP-мережу. Перед встановленням прикладного програмного забезпечення необхідно визначити параметри відеоканалів і доступні формати оброблення сигналів.

Наступним етапом є підготовка середовища виконання Python та встановлення необхідних бібліотек. Рекомендується створити окреме віртуальне середовище для ізоляції програмних залежностей. Для оброблення відеопотоків необхідно забезпечити доступність FFmpeg, а для функцій аналізу зображення встановити OpenCV. Сумісність бібліотек і системних компонентів потрібно перевірити до запуску основних програмних модулів. Конкретні версії визначаються вимогами застосунку та підтримуваними можливостями обладнання.

Для організації відеоархіву необхідно підготувати дискове сховище з достатньою місткістю та продуктивністю запису. Його обсяг визначається

кількістю камер, середнім бітрейтом потоків і встановленим терміном зберігання. Рекомендується передбачити окрему область для відеофайлів і метаданих. Якщо використовується база даних, у ній доцільно зберігати відомості про камери, часові інтервали запису, розташування відеосегментів та зареєстровані події. Для цього може застосовуватися PostgreSQL.

Первинне налаштування відеоканалів передбачає визначення ідентифікаторів камер, параметрів джерел сигналу та способів отримання відеопотоків. Для мережевих відеокодерів необхідно вказати адреси підключення та відповідні параметри автентифікації. За підтримки обладнанням RTSP можна використовувати цей протокол для організації потокових сеансів. Окремо встановлюються параметри відеокодування, зокрема роздільна здатність, частота кадрів, бітрейт і формат стиснення. Вибрані значення повинні відповідати можливостям джерел сигналу.

Рекомендована послідовність запуску системи починається з перевірки фізичних підключень відеокамер і приймальних пристроїв. Після цього запускаються мережеві відеокодери або ініціалізуються плати захоплення. Наступним кроком є запуск серверних модулів приймання потоків. Після підтвердження надходження відеоданих активується підсистема архівування. Модулі аналітичного оброблення та віддаленого перегляду доцільно запускати після перевірки працездатності основного відеотракту.

Для кожного підключеного джерела система повинна перевірити наявність відеопотоку та правильність визначення його параметрів. За відсутності сигналу необхідно встановити причину несправності. Вона може бути пов'язана з фізичним підключенням, несумісністю відеоформатів або недоступністю мережевого пристрою. У випадку втрати з'єднання програмний модуль повинен зафіксувати помилку та ініціювати повторне підключення. Після відновлення потоку необхідно перевірити коректність часових міток і продовження запису.

Налаштування архівування передбачає визначення тривалості відеосегментів, місця зберігання файлів і політики очищення дискового простору. Для безперервного запису необхідно контролювати доступну місткість сховища

та стан файлової системи. Після завершення запису кожного сегмента повинна виконуватися перевірка його доступності. Окремо необхідно передбачити захист активних файлів від автоматичного видалення. За потреби встановлюються правила збереження фрагментів, пов'язаних із зареєстрованими подіями.

Важливою складовою супроводу програмного комплексу є збереження відомостей про його походження та версію. Для цього доцільно передбачити інформаційний елемент програмного інтерфейсу з даними про розробника, назвою програмного продукту та його версією. Такі відомості використовуються під час оновлення, технічного обслуговування та ідентифікації програмного забезпечення. Авторські дані розробленої системи відеонагляду представлені на рисунку 5.2.

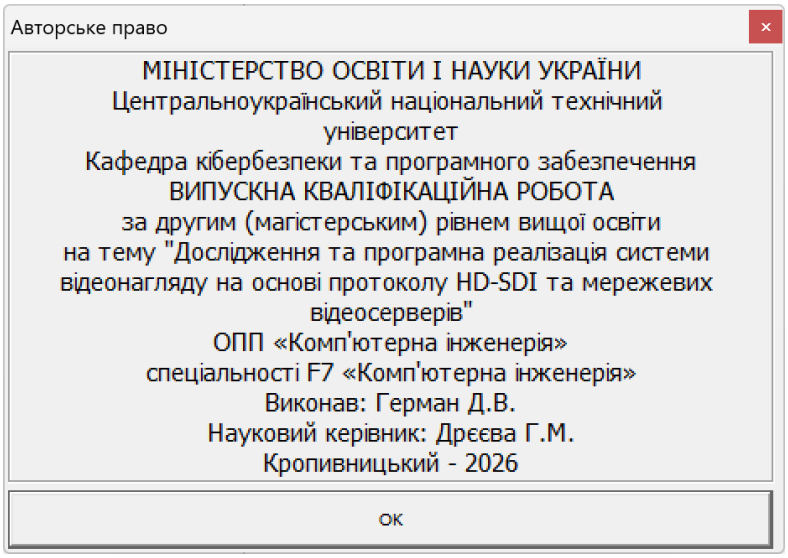


Рисунок 5.2 – Вікно авторського права

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Метою розробки є дослідження та програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Об'єктом дослідження є процес відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Предметом дослідження є методи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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

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

– Удосконалено метод відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

– Розроблено вітчизняний продукт відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

Вимога щодо впровадження заходів з охорони праці передбачається, зокрема, статтею 13 Закону України «Про охорону праці». У відповідності з цим законом, кожна компанія, в рамках якої реалізуються трудові відносини, зобов’язана вжити всіх необхідних заходів з охорони праці та розробити відповідні документи. Правильний підхід до організації охорони праці на виробництві дає працівникам почуття стабільності, захищеності їх прав та інтересів, уваги з боку керівництва. Налагоджена система охорони праці також знижує плинність кадрів, що позитивно впливає на стабільність роботи підприємств.

Аналізуючи умови працівників IT-сфери, на перший погляд, може здатися, що працівники сфери інформаційних технологій не схильні до ризиків на виробництві, та якщо більш глибоко розглянути умови і специфіку праці фахівців сфері IT-індустрії, можна виявити ряд факторів які будуть мати негативний сплив на стан охорони праці, так і на самого it-фахівця. Сюди можна віднести як невідповідність освітлення, так і високий рівень шуму, що негативно позначатимуться як на емоційному так і на фізичному стані фахівця, призводитимуть до зниження ефективності праці та виробничих травм. Також, важливим моментом охорони праці IT-фахівця є врахування його психологічних можливостей (швидкість реакції, особливості пам'яті та уваги, емоційний стан тощо).

Для того, щоб забезпечити ефективну роботу IT-фахівця, потрібно враховувати та максимально компенсувати такі негативні фактори як: надмірне нервово-емоційне навантаження, довготривалі статичні перевантаження, обмежена рухова активність. Всі ці чинники призводить до різноманітних відхилень у стані здоров’я, зокрема до перевтоми, зниження фізичної та

розумової працездатності, неврозів, захворювань серцево-судинної системи тощо.

Метою даного розділу є огляд конкретних умов праці спеціаліста у сфері IT-індустрії. Завданнями для даного розділу є: аналіз умов праці на робочому місці фахівця it-індустрії, розробка конкретних рекомендацій щодо покрашення умов праці фахівців IT-індустрії, огляд пожежної безпеки на IT-підприємстві та розрахунок системи загального штучного освітлення виробничого приміщення де працюють IT-фахівці.

7.2 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Розглянемо умови праці у приміщенні, в якому працюють програмісти. Геометричні розміри приміщення наведено у таблиці 7.1.

Таблиця 7.1 – Розміри приміщення

Найменування	Значення, м
Ширина	3
Довжина	4,6
Висота	3

Таблиця 7.2 – Площа та обсяг приміщення, на одного працюючого*

Геометрична характеристика	Одиниця виміру	Нормативне значення*	Фактичне значення
Площа, S	$м^2$	не менше 6.0	6,9
Об'єм, V	$м^3$	не менше 20.0	20,7

* Згідно ДСанПіН 3.3.2.007-98 (Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин).

У зазначеному приміщенні працюють двоє людей. За даними, які наведено у табл. 7.1, та табл. 7.2, можна зробити висновок, що площа та об'єм приміщення у розрахунку на одно робоче місце програміста не відповідають нормативним вимогам ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [2], але відповідають нормативним вимогам Наказу Міністерства соціальної політики України № 207, від 14.02.2018 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» та НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин»). Таним чином можна зробити висновок, що санітарно-гігієнічні умови праці на робочому місці програміста відповідають вимогам.

Температура повітря в приміщенні визначається впливом температури зовнішнього повітря і тепловою енергією, яка виділяється всередині приміщення. Джерелами виділення теплоти в даному приміщенні є електроустаткування, освітлювальні прилади, а також люди. У світлий час доби джерелом надлишкового тепла є сонячна радіація. Згідно Постанови № 42 від 01.12.1999 Головного державного санітарного лікаря України, робота, виконувана в даному приміщенні, відноситься до категорії Іа. В цьому випадку людина витрачає енергії до 120 ккал у годину. Вологість повітря в приміщенні визначається впливом багатьох факторів, серед яких: вологість атмосферного повітря, виділення вологи людьми (при диханні та випарами з поверхні шкіри).

Мікроклімат повітряного середовища в приміщенні характеризується запиленістю та загазованістю повітря. Мікроклімат приміщення визначається діючим на організм людини поєднанням, вологості, температури, швидкості руху повітря та інтенсивності теплового випромінювання. Аналіз мікроклімату складається з визначення зазначених вище факторів і порівняння результатів із встановленими нормами.

У таблиці 7.3 наведено оптимальні та фактичні значення параметрів мікроклімату як для категорії ваги робіт Іа, так і розглянутого приміщення. У

приміщеннях, де встановлено ЕОМ, рекомендується застосування тільки оптимальних значень показників мікроклімату.

Проведений аналіз показує, що показники мікроклімату в приміщенні відповідають установленим нормам. Штучне опалення застосовується у холодний період року.

В літню пору застосовується кондиціонер.

Таблиця 7.3 – Оптимальні і фактичні значення параметрів мікроклімату

Пора року	Оптимальні для Іа			Фактичні		
	Температура, °С	Воло-гість,%	Швидкість повітря, м/с	Температура, °С	Воло-гість%	Швидкість повітря, м/с
Холодна	22-24	40-60	0,1	22-24	40-55	0,12
Тепла	23-25	50-70	0,1	24-25	50-65	0,9

Для боротьби з пилом робляться регулярні провітрювання та вологі прибирання приміщенні.

У приміщенні знаходяться наступні джерела шуму: принтер Xerox WorkCentre 3025BI (3025VBI), електродвигуни вентиляторів ЕОМ.

Одним з найважливіших факторів, які впливають на ефективність трудової діяльності людини, та попереджають травматизм і професійні захворювання програмістів є освітлення на робочому місці.

З 2019 року діють Державні будівельні норми України “Природне і штучне освітлення” – ДБН В.2.5-28:2018 [1], у яких прописані вимоги до використання всіх освітлювальних приладів, у тому числі світлодіодних.

Працю працівника, який постійно працює за комп’ютером, згідно ДБН В.2.5-28:2018 [1], 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 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 поєднаному, спільному освітленні), повинен становити не більше 1,5%, освітленість при штучному висвітленні повинна становити 300 Лк [1], Крім того, все поле зору повинно бути освітлено достатньо рівномірно – це основна гігієнічна вимога. Оскільки яскраве світло на ділянці периферийного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими.

7.3 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог.

Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який повинен розташовуватись на видному місці у приміщенні), включення до колективного договору мінімально можливого вмісту аптечок з обов’язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання.

Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга).

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

Так як при ураженні електричним струмом у людини може статися фібриляція шлуночків серця, в організації бажано мати дефібрилятор і підготовлений персонал для роботи з ним.

7.4 Пожежна безпека

Вимоги до пожежної безпеки на підприємстві неухильно повинен дотримуватися кожен співробітник, а організаційна складова при цьому покладається на посадових осіб за відповідним рішенням керівництва і прописується в посадових інструкціях і положеннях по структурним підрозділам.

Зокрема, вказуються конкретні території, ділянки, зони, об’єкти, цілі будівлі і їх частини, поверхи, на яких відповідального співробітника повинне проводити такі організаційні роботи.

Відповідальні особи зобов’язуються розробити, впровадити та підтримувати в певному інструкцією і положенням на ввірених їм об’єктах протипожежний режим і інструкції відповідно до вимог, викладених в нормативних актах.

Передбачено також створення підрозділу добровільної пожежної охорони та пожежно-рятувальної команди в його складі.

Встановлений режим включає порядки з описом місць спеціального призначення та правила їх користування та утримання, наприклад:

– евакуаційних шляхів;

– так званих «курилок»;

– місць складування продукції та сировини;

– стоянки транспорту.

Також встановлюється порядок роботи та технічного обслуговування:

– вентиляційного устаткування;

– засобів пожежогасіння і захисту від загорянь;

– нагрівальних приладів;

– електрообладнання.

Розробляються і впроваджуються правила роботи з відкритим вогнем і горючими матеріалами. Створюються графіки проходження інструктажів з пожежної безпеки співробітників, а також порядок і терміни перевірок знань пожежно-технічного мінімуму, в тому числі, тих працівників, які відповідальні за цю ділянку роботи на підприємстві. При цьому можуть передбачатися внутрішні лекції, семінари, тренінги та практичні заняття на підприємстві, а також зовнішні – на базі спеціалізованих навчальних центрів з професійними викладачами.

Важливою складовою протипожежного режиму на будь-якому об’єкті є розробка і впровадження порядку дій при виникненні пожежі. Неодмінно має бути план евакуації, описано, як повинні відключатися електроустановки, що і в якій послідовності необхідно робити співробітникам.

Відповідно, для кожного об’єкта, кожного приміщення (крім коридорів, санвузлів, басейнів і подібних приміщень), окремих видів робіт складаються інструкції, за якими повинен працювати персонал, залучений на певних ділянках і в виконанні окремих видів робіт. За інструкціями проводиться навчання (інструктаж) персоналу з подальшим контролем знань.

Детально про те, як розробити протипожежний режим, прописати порядки та інструкції, пояснюють на тематичних курсах і семінарах [2].

7.5 Розрахункова частина

Система освітлення робочого місця користувача ПК має відповідати наступним вимогам (рис. 7.1).

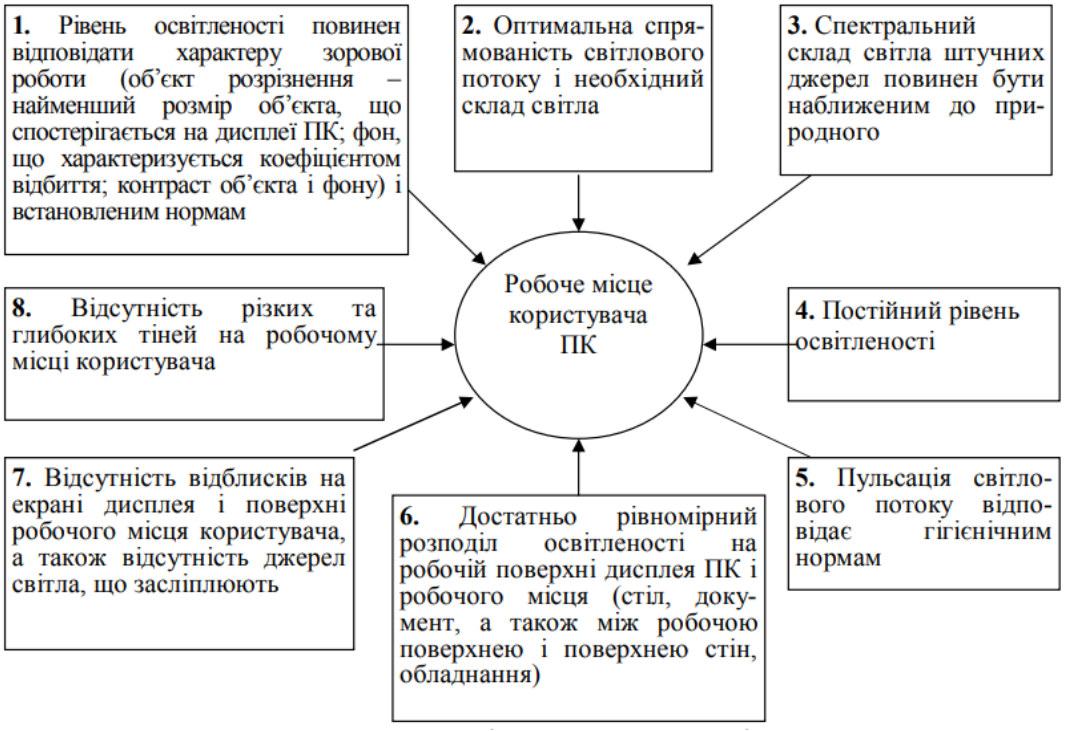


Рисунок 7.1 – Вимоги до системи освітлення робочого місця користувача ПК

Проведемо розрахунок штучного освітлення за методом коефіцієнта використання світлового потоку для приміщення, ширина якого складає 6,4 м, довжина – 8,3 м, висота – 3,2 м.

У зазначеному приміщенні працює 8 людей.

Для того, щоб визначити потрібну кількість світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою:

$$F=E\cdot S\cdot K\cdot Z/n,$$

де:

F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк; *E = 300 Лк;*

S – площа освітлюваного приміщення.

K – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку *K = 1,5);*

Z – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1.1... 1.2, в нашому випадку *Z = 1,1*);

n – коефіцієнт використання світлового потоку, (відношення світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп і обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{стін.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{стін}$ = 50% і $\rho_{стелі}$ = 50%.

Обчислимо індекс приміщення за формулою:

$$i=S/(h\cdot (A+B)),$$

де:

S – площа приміщення, *S* = 53,1 $м^2$*;*

h – розрахункова висота підвісу, *h* = 3,2 *м. (співпадає з в*исотою стелі, оскільки лампи освітлення закріплюються на стелі)*;*

A – ширина приміщення, *A = 6,4 м;*

B – довжина приміщення, *B* = 8,3 *м.*

Підставимо всі значення у формулу та визначимо індекс приміщення:

$$i=1,1.$$

Знаючи індекс приміщення, за знаходимо n = 0,46 (з табличних даних коефіцієнтів використання світлового потоку (n) світильників з відповідним типом лампам) [8]. Підставимо всі значення у формулу, визначимо світловий потік: F=57161,7 Лм.

Для розрахунку будемо використовувати стельові *світлодіодні панелі* Призма-72 6400К, світловий потік яких $F_л$ = 7200 *Лм.*

Число ламп визначається по формулі:

$$N=F/F_л$$

де:

F – світловий потік,

$F_л$ – світловий потік однієї лампи.

Підставимо всі значення у формулу та визначимо індекс приміщення:

$$N= 57161,7/ 7200=7,9 \text{ шт.}$$

Приймаємо необхідну кількість світлодіодних *світильників* 8 шт.

Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров’я працівників, а також підвищує ефективність виробництва в цілому.

З цих міркувань було здійснено аналіз умов праці, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Виконано розрахунок штучного освітлення, як одного з ключових факторів впливу на працездатність та здоров’я програміста. Розроблено заходи з охорони праці.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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 відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

– Досліджена система відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

– На основі отриманих результатів досліджень створена програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів.

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. Герман Д.В. Дослідження та програмна реалізація системи відеонагляду на основі протоколу HD-SDI та мережевих відеосерверів // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.

2. 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.

3. Проців В.В. Прикладна комп'ютерна графіка [Текст]: Навч. розділ / 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.

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

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

6. 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.

7. 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.

8. 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.

9. 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.

10. 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

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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,

18. 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.

19. 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

20. 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.

21. 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.

22. 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.

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

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

43. 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.

44. 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.

45. 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.

46. 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.

47. 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 розділ – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

48. 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).

49. 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

50. 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.

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

52. 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.

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

54. 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