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
“____” _____ 2025 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“ Дослідження та програмно-апаратна реалізація комплексу відеоспостереження для виробничого підприємства з інтеграцією модуля розпізнавання обличчя”

Виконав здобувач вищої освіти
ІІ курсу, групи КІ-24М
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Кондратенко І.О.
«____» _____ 2025 р.

Керівник проекту
кандидат технічних наук
_____ Улічев О.С.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Кондратенко І.О.. Дослідження та програмно-апаратна реалізація комплексу відеоспостереження для виробничого підприємства з інтеграцією модуля розпізнавання обличчя. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2025.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для автоматизації відеоспостереження на підприємстві.

Об'єкт дослідження – адміністративна будівля, лабораторії та монтажні приміщення компанії НВО «S Beta».

Предмет дослідження – аналіз потреб компанії в системі відеоспостереження та проектування відповідної системи з інтеграцією програмного модуля постобробки відеопотоку.

Підставою для інтеграції в діючу локальну мережу сучасної системи відеоспостереження є те, що для підтримки статусу гаранта якості необхідно вести постійний контроль за якістю виконуваних робіт працівниками компанії.

Завдання полягає в тому, щоб спроектувати інформаційну систему відеоспостереження, надавши оптимальний вибір сучасного обладнання та програмного забезпечення з можливістю подальшої модернізації.

Мета роботи сформувати обґрунтовану пропозицію щодо оптимального вибору інформаційної системи відеоспостереження для НВО «S Beta» з застосуванням інноваційних методів проведення контролю, збору та обробки отриманих матеріалів відео інформації.

Програму розроблено в середовищі VisualStudioCode Python.

Ключові слова:відеоспостереження, технічні засоби захисту, нейронна мережа, розпізнавання облич.

ABSTRACT

Kondratenko I.O.. Research and implementation of a hardware-software complex for video surveillance for a manufacturing enterprise with integration of a face recognition module. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2025.

In this final qualification work for the second (master's) level of higher education, software has been developed that is intended for automating video surveillance at the enterprise.

The object of the research is the administrative building, laboratories and assembly premises of the company NPO "S Beta".

The subject of the research is an analysis of the company's needs in a video surveillance system and the design of a corresponding system with the integration of a software module for post-processing of the video stream.

The basis for integrating a modern video surveillance system into an existing local network is that in order to maintain the status of a quality guarantor, it is necessary to constantly monitor the quality of work performed by the company's employees.

The task is to design a video surveillance information system, providing the optimal choice of modern equipment and software with the possibility of further modernization.

The purpose of the work is to form a substantiated proposal for the optimal choice of a video surveillance information system for the NGO "S Beta" using innovative methods of monitoring, collecting and processing the received video information materials.

The program was developed in the VisualStudioCode Python environment.

Keywords: video surveillance, technical means of protection, neural network, face recognition.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ВМ	–	Віртуальна машина
ОС	–	Операційна система
ПЗ	–	Програмне забезпечення
СЗД	–	Система зберігання даних
ЦОД	–	Центр обробки даних
BIOS	–	Basic Input-Output System
DRaaS	–	Сервіс відновлення як послуга
LINQ	–	Language Integrated Query
RAID	–	Redundant Array of Inexpensive Disks

ВСТУП

Темою дослідження магістерської кваліфікаційної роботи є «Дослідження та програмно-апаратна реалізація комплексу відеоспостереження для виробничого підприємства з інтеграцією модуля розпізнавання обличчя».

Актуальність дослідження. Сучасні виробничі підприємства функціонують в умовах підвищених вимог до безпеки, контролю доступу та оперативного реагування на позаштатні ситуації. Зростання рівня автоматизації технологічних процесів, цінність матеріальних ресурсів, наявність спеціального обладнання, а також необхідність забезпечення охорони праці створюють комплекс факторів, що вимагають застосування сучасних систем відеоспостереження та інтелектуальних технологій аналізу відеоданих. Традиційні охоронні системи, які не мають можливості автоматичної ідентифікації осіб, часто є недостатньо ефективними в умовах великих промислових територій та складних цехових структур. Це підкреслює актуальність застосування програмно-апаратних комплексів відеоконтролю нового покоління з інтегрованими модулями розпізнавання облич.

В умовах зростання кількості інцидентів несанкціонованого доступу, внутрішніх загроз та виробничого травматизму підприємства змушені впроваджувати системи, які здатні не лише фіксувати події, але й проводити автоматизований аналіз відеопотоків у режимі реального часу. Інтелектуальні модулі на основі комп’ютерного зору забезпечують суттєве підвищення якості контролю без збільшення чисельності охоронного персоналу. Сучасні технології машинного навчання дозволяють точно ідентифікувати осіб, визначати їхні маршрути переміщення, контролювати відповідність доступу до конкретних виробничих зон, виявляти сторонніх людей та мінімізувати людський фактор у процесах безпеки.

Виробниче підприємство є об’єктом підвищеної небезпеки, що зумовлює потребу у використанні надійних та швидкодіючих засобів моніторингу. Наявність

зон з обмеженим доступом, спеціальних ділянок з небезпечним устаткуванням або хімічними речовинами, складів із матеріально-цінними запасами формує вимогу до автоматизованого контролю присутності персоналу. Розпізнавання облич дозволяє забезпечити ідентифікацію кожного працівника на вході та виході, а також у межах критично важливих локацій підприємства. Це сприяє удосконаленню пропускної системи, зниженню ризику проникнення сторонніх осіб і підвищенню дисципліни працівників.

Додатково, інтелектуальні системи відеоспостереження забезпечують підприємство можливістю створення архіву відеоданих із прив'язкою до конкретних користувачів, що є важливим для подальшого розслідування інцидентів, аудитів, розв'язання спірних ситуацій та аналізу порушень правил техніки безпеки. Впровадження розпізнавання облич дозволяє не лише фіксувати порушення, але й попереджати їх за рахунок перевірки доступу до небезпечних зон в режимі реального часу.

Окремої уваги потребує питання продуктивності та сумісності програмно-апаратних рішень. Підприємства часто мають розгалужену інфраструктуру та використовують обладнання різних поколінь, що потребує адаптивних систем, здатних інтегруватися з існуючими серверами відеоспостереження, мережевим обладнанням та системами контролю доступу. Розробка уніфікованого комплексу, який поєднує функції відеофіксації, інтелектуальної обробки даних та автоматизації процесів, є важливим завданням, що дозволяє уникнути надмірних витрат на модернізацію та забезпечити масштабованість системи.

Суттєвою перевагою застосування алгоритмів розпізнавання облич є можливість підвищення точності ідентифікації порівняно з традиційними картковими або кодовими системами контролю доступу. Використання біометричних даних унеможливлює передачу ідентифікатора стороннім особам, що часто трапляється у випадку з RFID-картами або пропусками. Це робить систему значно стійкішою до внутрішніх загроз і порушень режиму доступу.

На додаток, розвиток технологій штучного інтелекту, підвищення потужності мобільних і серверних пристроїв, а також удосконалення алгоритмів нейронних мереж сприяють тому, що інтелектуальні модулі стають доступнішими і надійнішими. Підприємства отримують можливість впроваджувати рішення, які ще кілька років тому були надто дорогими або вимагали спеціалізованого обладнання. Це зумовлює зростання попиту на програмно-апаратні комплекси відеоспостереження з функціями розпізнавання облич, а також потребу в дослідженні їх ефективності, оптимізації та адаптації до умов конкретних виробничих процесів.

Таким чином, актуальність дослідження полягає у необхідності створення інтегрованої системи відеомоніторингу нового покоління, яка поєднує апаратні та програмні компоненти, забезпечує високий рівень безпеки, автоматизує процес контролю доступу та мінімізує людський фактор. Розробка такого комплексу дозволить підприємствам забезпечити ефективний моніторинг території, оперативно реагувати на небезпечні ситуації, підвищити рівень охорони праці, оптимізувати ресурсні витрати та відповідати сучасним вимогам промислової безпеки.

Об'єкт дослідження – адміністративна будівля, лабораторії та монтажні приміщення компанії НВО «S Beta».

Предмет дослідження – аналіз потреб компанії в системі відеоспостереження та проектування відповідної системи з інтеграцією програмного модуля постобробки відеопотоку.

Підставою для інтеграції в діючу локальну мережу сучасної системи відеоспостереження є те, що для підтримки статусу гаранта якості необхідно вести постійний контроль за якістю виконуваних робіт працівниками компанії. Другим важливим фактором, що визначає необхідність впровадження відповідних систем відеоспостереження, є наявність в організації циркуляції конфіденційної інформації (фінансова звітність, науково-інженерні розробки компанії, данні пацієнтів). Останнє вимагає контролю доступу на об’єкт сторонніх осіб з метою

унеможливлення проникнення до інформаційних сховищ з метою подальшого викрадення чи порушення цілісності даних.

Інформаційна система відеоспостереження дозволить спостереження за роботою підприємства без відриву від виконання основних обов'язків керівника компанії чи окремої уповноваженої особи, що відповідає за безпеку компанії. Візуальні дані нададуть можливість аналізу технології виконання робіт, а також дотримання правил охорони праці. Особливу значущість наявності системи відеоспостереження дає при розслідуванні інцидентів.

Завдання полягає в тому, щоб спроектувати інформаційну систему відеоспостереження, надавши оптимальний вибір сучасного обладнання та програмного забезпечення з можливістю подальшої модернізації.

Мета роботи сформувати обґрунтовану пропозицію щодо оптимального вибору інформаційної системи відеоспостереження для НВО «S Beta» з застосуванням інноваційних методів проведення контролю, збору та обробки отриманих матеріалів відео інформації на центральному диспетчерському пункті підприємства для систематизації, аналізу або постобробки. Для формування пропозиції, щодо проектування системи відеоспостереження, необхідно дослідити різновиди систем відеоспостереження, побудованих із застосуванням аналогових та цифрових камер.

Для реалізації проекту необхідно:

- проаналізувати сучасні системи відеоспостереження;

- надати оптимальний вибір технічних засобів та рішень;

- запропонувати проект системи враховуючи особливості роботи компанії та архітектурні особливості будівлі;

- розробити та інтегрувати в систему програмний модуль для обробки зображення на предмет розпізнавання облич.

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

– запропоновано метод розпізнавання облич на основі контрольних маркерів та нейронної мережі;

– спроектовано структуру нейронної мережі для вирішення даної задачі;

– розроблено програмний модуль для інтеграції в систему відеоспостереження, з метою його застосування для пост обробки відеопотоку.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачу автоматизації контрольно-пропускної системи організації чи підприємства.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними підходами до розробки інформаційних моделей, а також відповідністю отриманих результатів результатам інших дослідників, які наведені у науковій літературі.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

НВО «S Beta» - організація заснована у 1998 році, і включала в початковому складі всього 5 осіб: директор (автор проекту та засновник), інженер з проектування електронних пристроїв, бухгалтер (що поєднує юридичні питання фірми) та дві особи – монтаж електронних плат.

За роки роботи організація дещо розширилася, але й сьогодні залишається невеликим колективом однодумців, сьогодні штат співробітників налічує 24 особи

Розвиток компанії базується на постійному вдосконаленні розробок, підвищення точності діагностики та розширенні набору додаткових функцій запропонованих пристроїв та супровідного програмного забезпечення.

Стратегія компанії полягає в нарощуванні конкуренції в сегменті діагностичного обладнання та залучення до партнерства великих медичних компаній, а також цільових споживачів продукції, що розробляється.

Спочатку організація займалася розробкою та дрібносерійним виробництвом діагностичної апаратури у сфері кардіології. До розроблених організацією приладів належать: холтер (реєстратор) добового тиску, холтер ЕКГ.

Холтерівська система (холтер) являє собою портативний реєстратор, що носиться ЕКГ сигналу (або ЕКГ + АТ), який носиться пацієнтом зазвичай протягом доби (або від 8 до 158 годин), при цьому пацієнт веде звичайний спосіб життя, заповнюючи щоденник пацієнта, що дозволяє лікарю отримати повну картину ЕКГ подій, які відбуваються з пацієнтом поза лікарнею.

Рисунок 1.1 – Приклади обладнання, що розробляється компанією

Розробникам організації вдалося спроектувати і реалізувати досить конкурентний пристрій, який досить якісно знімає сигнал, з урахуванням перешкод та зовнішніх наведень. Це дозволило конкурувати на ринку, як із іншими вітчизняними виробниками, так і із зарубіжними компаніями. Отримавши визнання в медичному секторі, і випробувавши пристрій у реальних умовах, вирішено було розробляти програмний комплекс для супроводу пристрою.

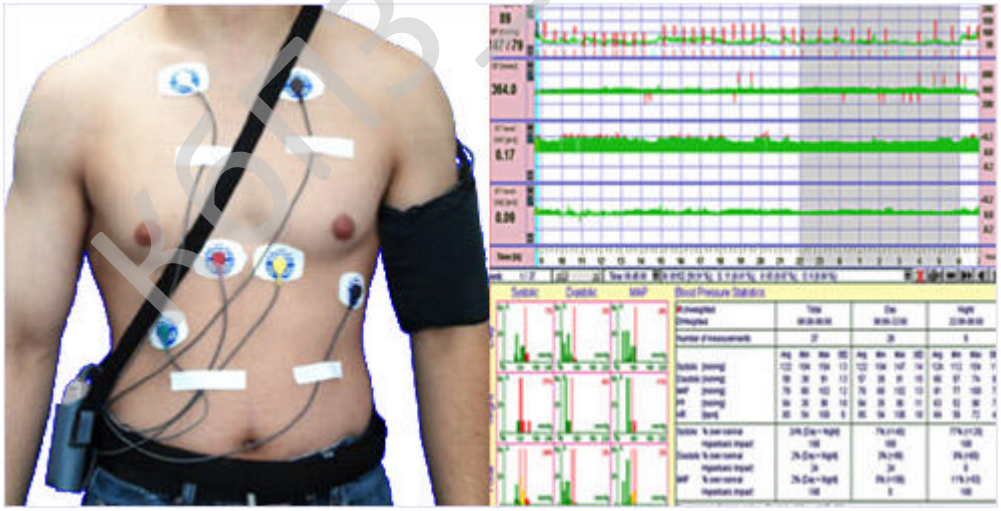

Рисунок 1.2 – Застосування обладнання для діагностики пацієнта

Наступні 18 років співробітники фірми оновлювали, покращували як апаратну частину системи, і програмну. В останні роки більше уваги було приділено саме програмній складовій. Оскільки програмна частина має і більший

потенціал розвитку та більш швидко застаріває щодо сучасних технологій та можливостей сучасних ПК.

Для досліджуваного підприємства основним чинником, що вимагає впровадження системи відеоспостереження, є запобігання витокам технічної інформації та захист інформаційних активів. Далі коротко розглянемо класифікацію даних активів та їх коротку характеристику.

Перелік видів, джерел та оцінки інформаційних активів підприємства

Основними джерелами інформації в організації є:

- Керівник організації;
- Посадові особи організації;
- Фахівці технічного відділу;
- Документи по столах та шафах;
- Демонстраційні прилади – продукція компанії
- Технічна документація;
- Електронні носії та бази даних компанії.

Таблиця 1.1 – Види, джерела та оцінка інформаційних активів підприємства

№ п/п	Вид інформації в кабінеті	Джерело	Максимальна ціна інформації	Місце знаходження джерела інформації в кабінеті інформації
1	Семантична документальна	документи	дуже висока	Сейф в кабінеті директора, бухгалтера, шафи технічного відділу
2	Семантична документальна (відкриті документи)	документи/електронні документи	низька	Сайт компанії, пакети документаційного супроводу продукції, шафи в приміщеннях компанії
3	Семантична мовна акустична	люди	висока	Кабінет директора/технічний відділ
4	Речові ознаки	Продукція компанії: пристрої	низька	Кабінет директора/технічний відділ
5	Електронні носії	Програмні коди, результати розробок, алгоритми	дуже висока	Комп'ютери технічного відділу, носії інформації в сейфі директора

1.2 Область застосування

Система відеомоніторингу та спостереження призначена для забезпечення комплексної безпеки науково-виробничого підприємства, контролю за технологічними процесами та дотриманням правил охорони праці. Її застосування охоплює як виробничі, так і адміністративно-господарські об’єкти підприємства.

Основні напрями застосування системи:

1. **Охорона периметру та об’єктів підприємства:**

- спостереження за вхідними групами, контрольно-пропускними пунктами, стоянками транспорту;
- виявлення несанкціонованого проникнення на територію;
- фіксація часу входу/виходу персоналу та відвідувачів.

2. **Контроль виробничих процесів:**

- дистанційне спостереження за роботою технологічного обладнання;
- моніторинг дотримання технологічних режимів;
- оперативний контроль за аварійними або позаштатними ситуаціями.

3. **Забезпечення охорони праці та техніки безпеки:**

- спостереження за дотриманням працівниками вимог безпеки;
- фіксація подій для подальшого розслідування нещасних випадків;
- навчальні та аналітичні цілі (аналіз типових помилок персоналу).

4. **Адміністративний та логістичний контроль:**

- моніторинг руху транспорту на території підприємства;
- контроль за роботою складських приміщень, зон відвантаження та прийому матеріалів;
- контроль доступу до службових і лабораторних приміщень.

5. **Інформаційно-аналітичне використання**

- накопичення архіву відеоданих для службових розслідувань;
- інтеграція з іншими системами безпеки (системою контролю доступу, пожежною сигналізацією, охоронною сигналізацією);

– формування аналітичних звітів для керівництва.

Таким чином, система відеомоніторингу та спостереження використовується як засіб забезпечення безпеки, ефективності виробничих процесів і контролю діяльності персоналу, що сприяє підвищенню загального рівня організаційної та технологічної дисципліни на підприємстві.

Дослідження об’єкту, інформаційний аудит

Для оцінки особливостей проектування та інтеграції системи відеоспостереження варто провести комплексний аналіз компанії. Основний акцент варто зробити на архітектурні особливості будівлі, аналіз інформаційних активів та приміщень де циркулює та зберігається інформація.

Обстеження приміщення стислий опис результатів його обстеження

Компанія займає двоповерхове приміщення з заднім огородженим заднім двором.

На першому поверсі розміщується: кабінет директора, кабінет гол. бухгалтера, приймальня, кімната для переговорів.

На другому поверсі розміщується: технічний відділ, серверна кімната, відділ монтажу, конференційна зала.

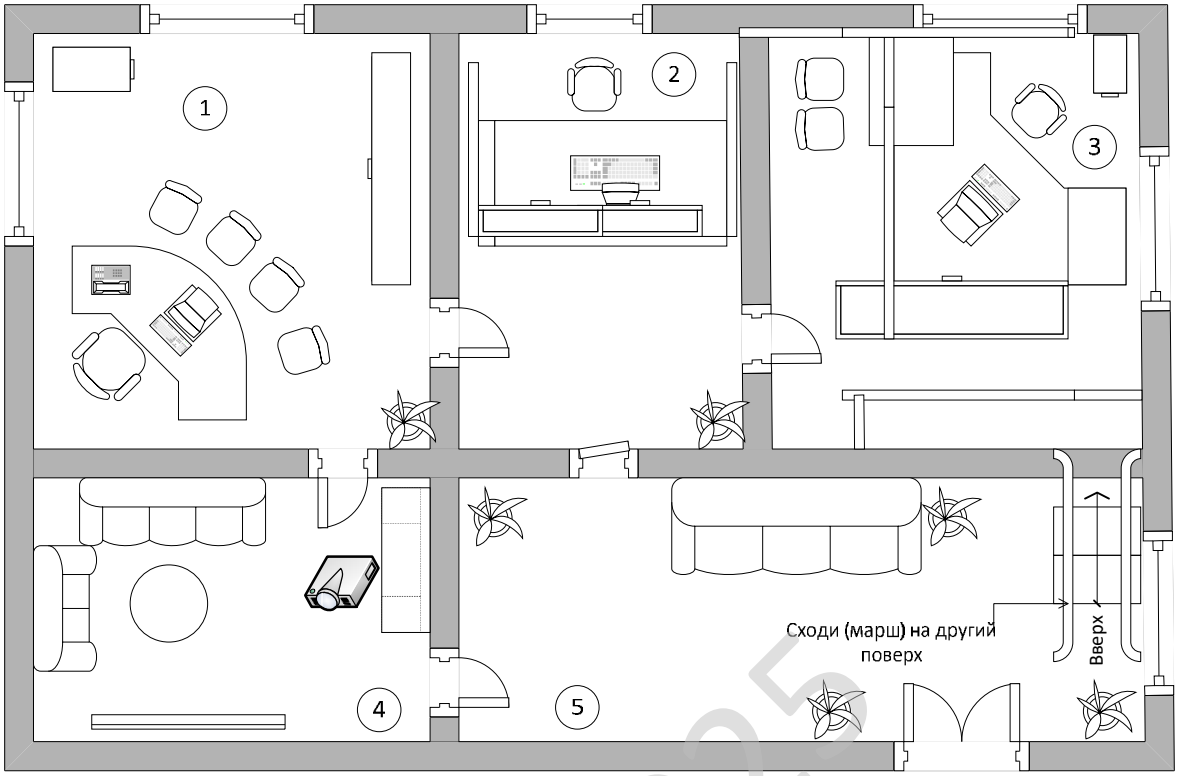

Рисунок 1.3 – План першого поверху

1 - кабінет директора

2 - приймальня

3 – кабінет бухгалтера

4 – кімната для перемовин

5 – хол

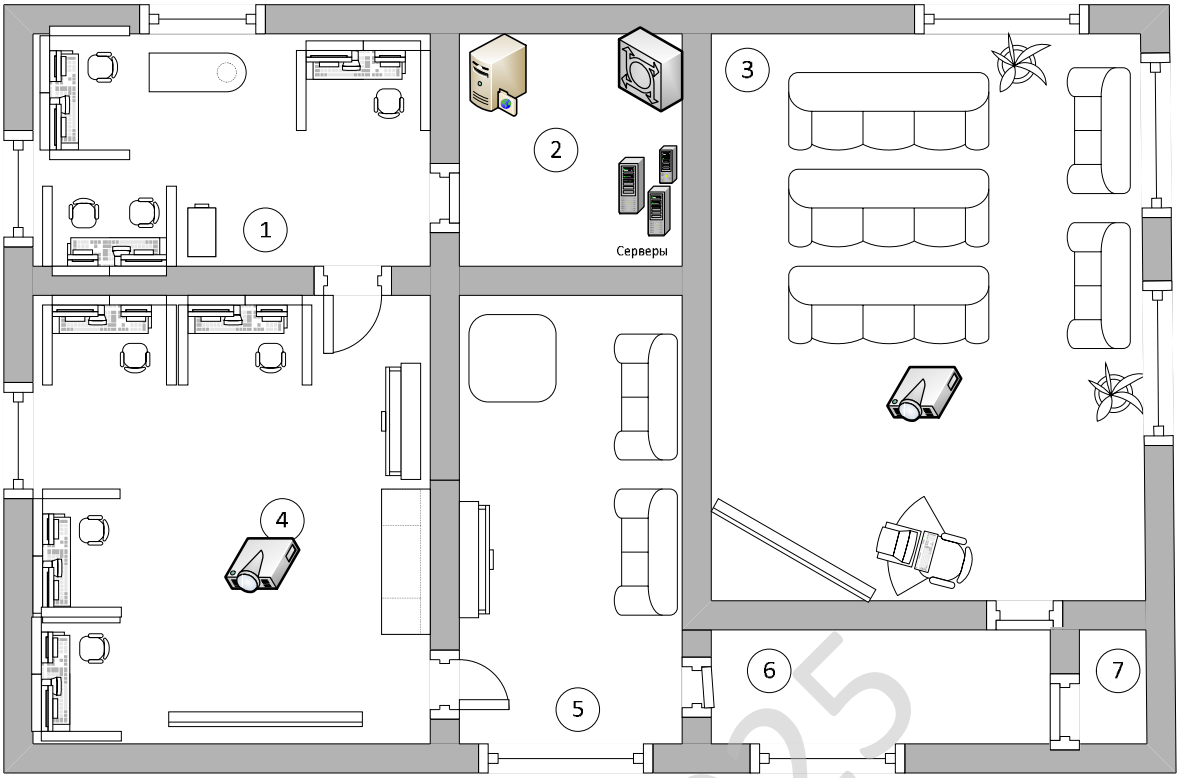

Рисунок 1.4 – План другого поверху

1 – відділ монтажу обладнання та підтримки

2 - серверна

3 – зал для нарад та конференцій

4 – відділ розробки

5 – кімната релаксу/кухня

6 – коридор

7 -- вбиральня

Таблиця 1.2 – Результати обстеження приміщення

№ п/п	Чинники впливу	Параметри	Примітка
1	2	3	4
1. Загальні характеристики приміщення			
1.1	Поверх	1	
	Площа	60 м2	
	Кімнат	5	
1.2	Поверх	2	
	Площа	90 м2	
	Кімнат	6	
2 Огорожі (границі приміщень)			
2.1	Стіни	зовнішня — цегляні 1200 мм внутрішні цегляні в 0,5 цеглини, обшиті гіпсокартоном з подвійною звукоізоляцією; опалення автономне електроконвектори; 3 вентиляційних отвори; суміжна з кабінетом директора - залізобетонна завтовшки 140 мм	
2.2	Стеля та перекриття між 1 та 2 поверхами	залізобетонна плита завтовшки 400 мм, покрита водоемульсійною фарбою	
2.3	Підлога		
	1 -поверх	Стяжка 20 см, армована, вкрита кахлями, в кабінетах вкрита поверх ковроліном	
	2- поверх	Стяжка по перекриттю 5 см, звуко та теплоізуюшуй шар, ламінат	
2.3	Вікна	Металополастик, 3-камерні, звукоізолюючі, товщина скла -4 мм. – 12 шт	
		Панорамні металопластикові - 2шт.: кабінет директора (1 шт.), вздовж маршу на другий поверх (1шт.)	
2.4	Двері	Вхідні двохстворчаті металопластикові, захищені зовні ролетом	
		1 поверх: деревяні (дуб) одностворчаті	
		2 поверх: поверх: дерев'яні одностворчаті (вбиральня), міжкімнатні (К5-К4, К4-К1) Металопластикові з автоматичним приводом: серверна, конференцзал, вхід в технічну зону (К6-К5)	
3. Предмети меблів і інтер'єру			
3.1	Дивани	10 шт.	
3.2	Сейф напольний	3 шт. електронні замки	
3.3	Дошки для демонстрацій	розмір 2000*1200 мм, з білого пласт., на якій можна малювати і використовувати як екран 3 шт. з хім фолокна, згортається в тубус, розмір 3500*2000, виключно для проектора 1 шт.	

Продовження таблиці 1.2			
№ п/п	Чинники впливу	Параметри	Примітка
3.4	Квіти (вазони)	12 шт.	
3.5	Робочі місця адміністрації (стіл, тумба, шафа, крісло)	3 шт.	
3.6	Робочі місця розробників (стіл, тумба, крісло)	8 шт.	
3.7	Робочі місця монтажників (стіл, тумба, крісло)	6 шт.	
3.8	Стіл круглий для перемовин	1 шт.	
3.9	Шафи	10 шт.	
3.10	Кухонне обладнання та посуд (набір)	1 шт.	
3.11	Буфет-бар	1 шт.	
4. Радіоелектронні засоби і електричні прилади			
4.1	Комп'ютер офісний	склад: системний блок, монітор, миша, клавіатура, 2 динаміки 8 шт.	
4.2	Комп'ютер розробника	склад: системний блок, монітор, миша, клавіатура, 2 динаміки 8 шт.	
4.3	Сервер	2 шт.	
4.4	Проектор	3 шт.	
4.5	Устаткування для монтажу (свердлільний станок, паяльні станції, місце слюсарної обробки)	1 шт.	
4.6	Телевізор	2 шт.	
4.8	Настільна лампа	10 шт.	
4.9	Люстри діодні (основне освітлення)	14 шт.	
4.10	Кавова машина	2 шт.	
4.11	Кондиціонер	6 шт.	
4.12	Конвектори опалення	14 шт.	
Засоби комунікацій			
5.1	Розетки електроживлення	40шт.	
5.2	Телефонні розетки	5 шт.	
5.3	Електропроводка прихована в стінах		
5.4	Кабелі телефонних ліній зовнішні		
5.5	Кабель локальної мережі ЕОМ вита пара, укріплена на стіні		
5.6	Шлейф пожежної сигналізації зовнішні, на стелі і стіні біля письмового столу		
5.7	Розетка телевізійної кабельної мережі	2 шт.	

Далі розглянемо перелік інформації в ІТС обраного підприємства, який містить перерахування відомостей, що в рамках даного підприємства мають конфіденційний характер (складають службову або комерційну таємницю), а також зазначимо перелік основних документів, що регламентують необхідність захисту інформації та електронних інформаційних ресурсів, що їх містять.

Таблиця 1.3 - Класифікація інформаційних активів НВО "S Beta".

№	Назва видів інформації	Категорія	Критичність захисту
1	Статут та установчі документи компанії	Службова	Критично
2	Договори з партнерами	Службова	Критично
3	Платіжні реквізити та платіжні документи	Службова	Критично
4	Облікові та реєстраційні дані співробітників та клієнтів.	Персональні данні	Критично
5	Анкетні та паспортні дані потенційних замовників та клієнтів тощо	Службова	Критично
6	Тестові дані пацієнтів	Данні досліджень і випробувань	Некритично
7	Схеми пристроїв	Результати розробок	Некритично
8	Алгоритми аналізу даних	Результати розробок	Критично
9	Вихідні коди програм обслуговування	Результати розробок	Критично
10	Технічна документація	Службова	Некритично
11	Інформація про діяльність підприємства, що оприлюднюється на сайті (вакансії та акційні пропозиції, інформація про напрямки роботи, інформація про Замовників, прайс-листи).	Публічна	Некритично

Прокоментуємо висновки критичності по деяким пунктам.

6 – «Тестові дані пацієнтів»: це файл з зафіксованими сигналами, але він безособовий, надається партнерами в тому випадку коли програмне забезпечення на ньому неадекватно відпрацювало, або коли сигнал містить дуже індивідуальні особливості. Використовується для аналізу і подальших досліджень. Отримання доступу до нього зловмисника може нести шкоду лише в ході дослідження (вилучення самого файлу або його модифікація), але дамп може бути легко відновлений по запиту до партнера, що його надіслав. Саме володіння даною інформацією зловмиснику ніяких переваг не дає.

7 – «Схеми пристроїв»: пристрій може бути купленим офіційно, його схема може бути проаналізована стороннім інженером. Копіювання схеми захищено патентом, виявлення копіювання з комерційною метою потягне за собою судові

наслідки в області захисту авторського права. Але сама по собі принципова схема пристрою не є секретною. Теж стосується і п.10. «Технічна документація» - документації немає в відкритому доступі, але вона надається замовнику при передачі пристроїв та програмного забезпечення. Доступ до неї зловмисника не має критичних наслідків.

Відповідальність, передбачена за порушення вимог нормативно-законодавчих актів України по захисту даного виду інформації (по Вашому варіанту) регламентується наступними законами:

- ЗУ «Про авторське право і суміжні права»;
- ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах»;
- ЗУ «Про захист персональних даних».

В якості об'єкту захисту розглядається підприємство НВО «S Beta». Приміщення має два поверхи: 1 – адміністративний, 2 – технічний відділ та відділ розробки.

Плани приміщень зображено на рис. 1.3-1.4

Розташування усіх ТЗПІ(технічний засіб(основні), призначений для витоку інформації) та ДТЗС(додаткові технічні засоби, призначені для витоку інформації) описано нижче на схемах.

До ТЗПІ засобів відносяться:

- телефони міської АТС
- внутрішні телефони (забезпечення внутрішнього зв'язку)
- звуко-підсилюючі пристрої (конференц-зал)
- засоби мережевої комутації (концентратори, роутери)
- мережеві пристрої друку
- засоби відео- трансляції (проектори).

До ДТЗС засобів відносяться:

- засоби і системи спеціальної охоронної сигналізації (загальна пультова сигналізація, датчики цілісності вікон);
- датчики пожежної сигналізації;

- засоби і системи кондиціонування (датчики температури, вологості, кондиціонери);

- засоби і системи електроосвітлення та побутового електрообладнання (світильники, люстри, настільні і стаціонарні вентилятори, електронагрівальні прилади, провідна мережа електроосвітлення);

- електронна та електрична оргтехніка

Кондиціонери та освітлювальні прибори розміщено у всіх кімнатах приміщення. На схемі не відображені з метою спрощення читання та сприйняття.

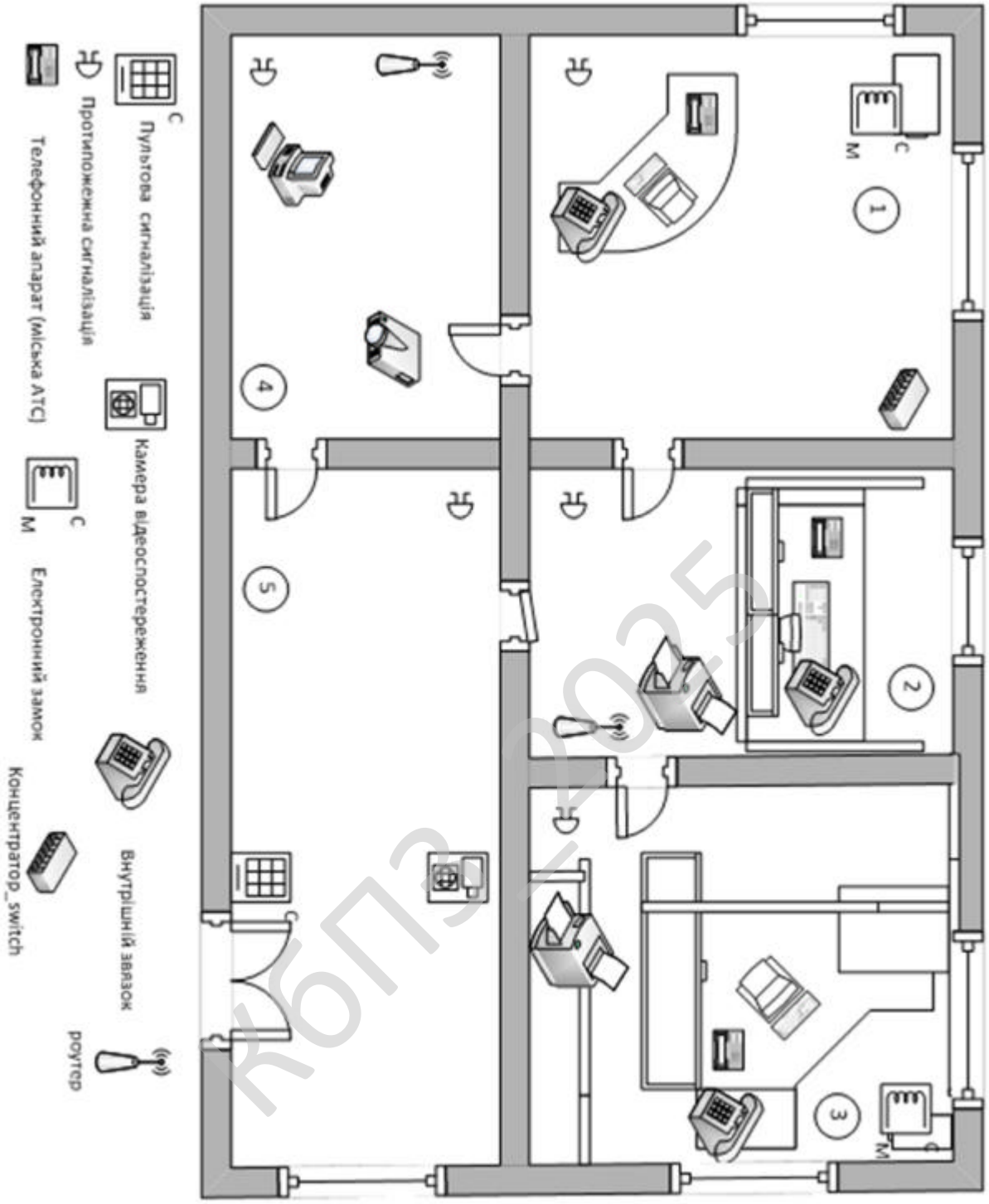

Рисунок 1.5 – Перший поверх, розміщення ТЗПІ та ДТЗС

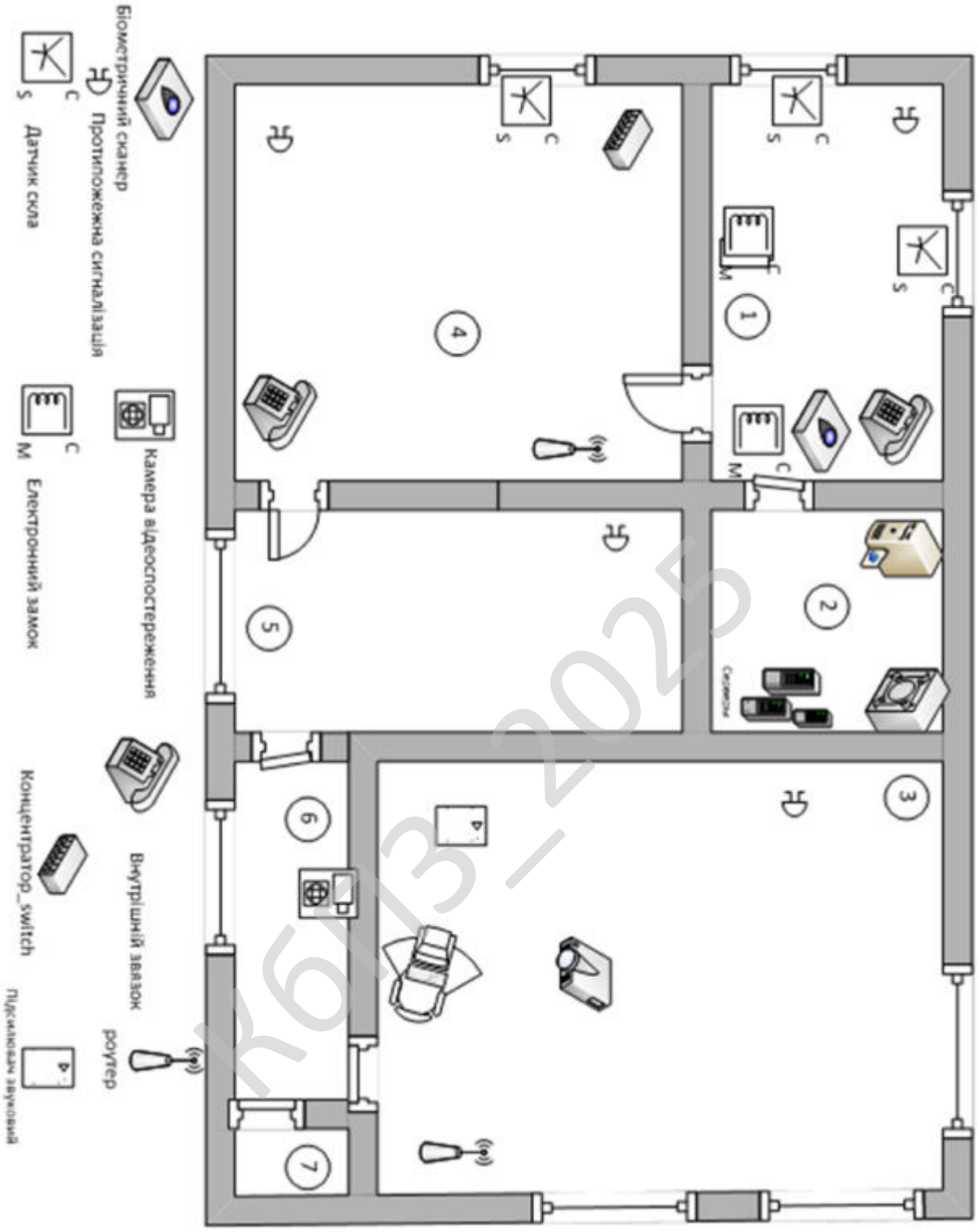

Рисунок 1.6 – Другий поверх, розміщення ТЗПІ та ДТЗС

Варто також проаналізувати кімнати приміщення, які можуть мати візуальний контакт з сусідніми будівлями.

Кімнати першого поверху хоч і мають вікна але більшість з них виходять в внутрішній двір, доступ до якого обмежений (див. рис. 1.7). Високий бетонний паркан перешкоджає видимості перекриваючи вікна.

На вулицю виходить два вікна:

- вікно холу (немає загроз – в даному приміщенні відсутня візуальна інформація, що може представляти інтерес для зловмисника)

- одне з вікон кабінету директора.

Вікно в кабінеті директора має захисне скло з односторонньою прозорістю

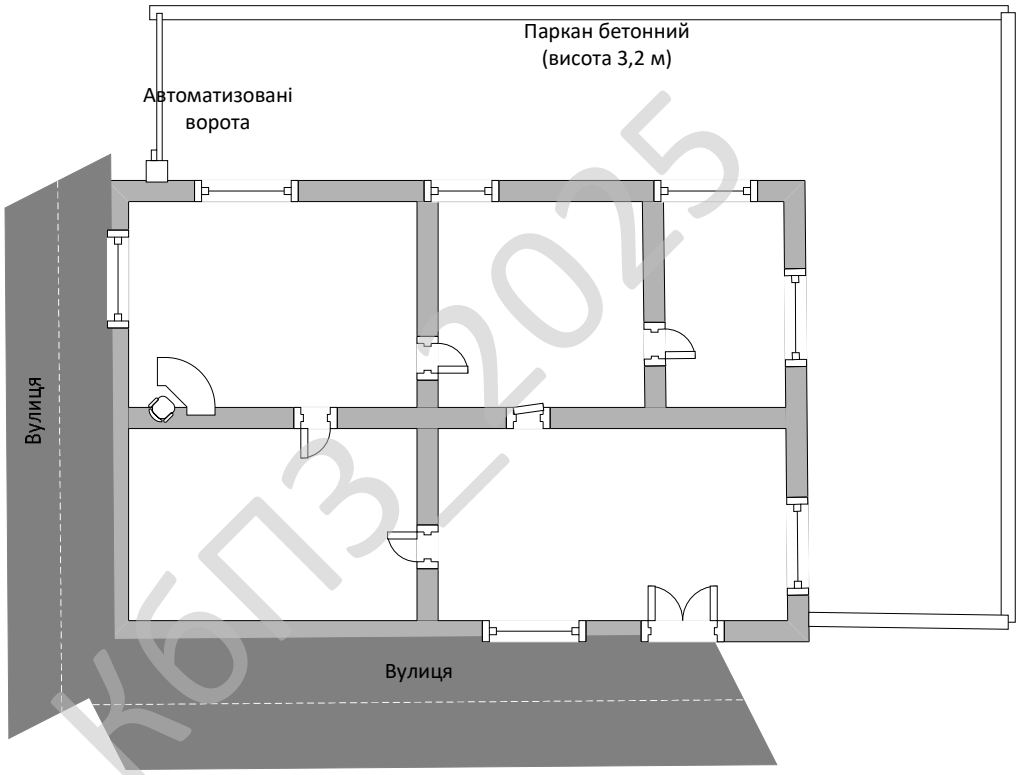

Рисунок 1.7 – Загальний план

Вікна приміщень другого поверху можуть проглядатись з навколишніх будівель.

Вікна захищені, мають жалюзі, що частково перешкоджає візуальному контролю та ускладнює можливість візуального моніторингу. Найбільш критичним є приміщення відділу розробки (К4 рис. 1.4). Зловмисники можуть отримувати данні за рахунок візуального спостереження, з використанням

спеціальної апаратури навіть читати інформацію з екранів. З огляду на це, всі робочі місця розташовані таким чином щоб монітори не потрапляли в кут огляду (див. план рис. 1.4 та рис. 1.8), також демонстраційний екран, на якому періодично транслюється інформація пов’язана з технологічними розробками організації в ході досліджень, розміщено поза кутом огляду.

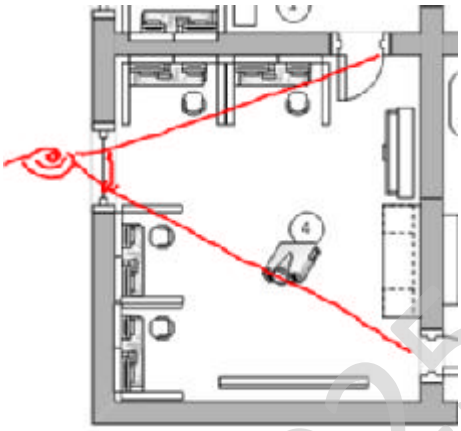

Рисунок 1.8 – Розміщення робочих зон, з урахуванням ускладнення візуального спостереження з зони поза контрольованим периметром

Види інформації, що циркулює на об’єкті, відштовхуючись від плану приміщення, представлені в таблиці 1.4.

Таблиця 1.4 – Розміщення інформаційних активів з урахуванням плану будівлі

№	Назва видів інформації	Розміщення, місце циркуляції	Примітка
1	Установчі документи компанії	Кабінет директора (1 поверх, К1)	Знаходиться в сейфі
2	Договори з партнерами	Кабінет директора, кабінет бухгалтера (1 поверх, К1, К3)	На комп'ютерах директора та бухгалтера
3	Облікові та реєстраційні дані співробітників та клієнтів.	Кабінет директора, кабінет бухгалтера (1 поверх, К1, К3)	На комп'ютерах директора та бухгалтера
4	Семантична мовна інформація, обговорення планів та стратегій, партнерських угод	Кабінет директора, кімната для перемовин (1 поверх, К1, К4)	
5	Семантична мовна інформація, обговорення підходів, алгоритмів	Приміщення відділу розробки (2 поверх, К4)	
6	Алгоритми аналізу даних візуальна текстова інформація	Комп'ютери відділу розробки, демонстраційна дошка	
7	Вихідні коди програм аналізу та обслуговування пристроїв	Комп'ютери відділу розробки, серверна, локальна мережа, комп'ютери відділу монтажу(2 поверх, К1, К2, К4)	
8	Технічна документація	Комп'ютери відділу розробки, серверна, локальна мережа, комп'ютери відділу монтажу, конференц-зал (2 поверх, К1, К2, К4, К3)	
9	Семантична мовна інформація, обговорення планів та стратегій, партнерських угод	Кабінет директора	Телефонний режим обговорення, наради з розробниками
10	Текстова та графічна інформація, що створена в ході досліджень	Приміщення відділу розробки (2 поверх, К4)	Проміжні варіанти на папері, чернетки і інші носії, що містять часткову інформацію, ідеї, елементи алгоритмів

Аналіз небезпечних фізичних сигналів, що можуть бути присутні на об'єкті

- Акустичний сигнал - опір пружного середовища, який виявляється у виникненні акустичних коливань різної форми і тривалості.

- Віброакустичний сигнал - передача акустичних коливань на природні мембрани (двері, вікна, інші інженерні та будівельні конструкції).

– Електромагнітне поле, що випромінюється ТЗС, а також електричні струми, що циркулюють в ланцюгах ТЗС.

Можливі канали витоку інформації, відштовхуючись від плану приміщення, можна охарактеризувати наступним чином.

Акустичний ТКВІ – може бути підслухана розмова в кабінеті директора чи кімнаті для перемовин (записана на підслуховуючий пристрій).

Віброакустичний ТКВІ – підслухати голосову інформацію можна знімаючи її за допомогою спеціальних пристроїв з природніх мембран.

Оптико-електронний (лазерний) ТКВІ утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких відображаючих поверхонь (скла вікон, картин, дзеркал і т. д.). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється по амплітуді і фазі (згідно із законом вібрації поверхні) і приймається приймачем оптичного (лазерного) випромінювання.

Оптичний ТКВІ – має найбільшу загрозу в приміщенні відділу розробки. Можуть бути застосовані пристрої відеозапису або фотофіксації. Для останнього необхідно проникнути в приміщення або мати інсайдера серед співробітників компанії.

Речовий ТКВІ – залишки інформації що залишилась на паперових носіях та потрапила до сміття, попередньо не знищена належним чином.

Найбільш ймовірний та небезпечний канал витоку пов’язаний зі зламом мережі компанії та отримання мережевого (дистанційного) доступу до електронних носіїв. Зламування мереж і витік інформації через інтернет відносяться до каналу витоку інформації «технічні засоби зв'язку та інформаційних систем». Цей канал пов'язаний з порушенням безпеки інформаційних систем, порушенням політик безпеки, і може відбуватися через зламування мережевих пристроїв, вразливість програмного забезпечення або неправильне налаштування мережевих конфігурацій. Він може призвести до витоку конфіденційних даних, таких як особисті дані користувачів, фінансові дані, комерційні секрети тощо. У

випадку досліджуваного об’єкту основними активами є програмні коди та алгоритми аналізу.

Природні канали пов’язані з природніми явищами та полями, фізичними процесами. До них варто віднести:

- Акустичний ТКВІ.
- Віброакустичний ТКВІ.
- Оптико-електронний ТКВІ.

Але якщо зловмисник використовує спеціальну апаратуру (наприклад для запису перемовин, долаючи перешкоди чи фільтруючи акустичний сигнал) то такий канал витоку варто віднести до штучних навмисно створених каналів. Також до штучних (ненавмисних) варто віднести речовий канал витоку.

Найбільш небезпечним є ТКВІ через злам технічних засобів зв’язку та інформаційних систем. Якщо зловмисник має такий канал – він отримує доступ практично до всієї інформації яка раніше була оцінена як критична, отримання такої інформації принесе максимальні збитки компанії аж до повного банкрутства (в залежності від об’ємів отриманої інформації та способів її зловмисного використання).

Електромагнітні канали витоку інформації - це канали, які використовують електромагнітні хвилі передачі інформації. Це можуть бути радіохвилі, мікрохвилі, інфрачервоні промені та інші типи електромагнітних хвиль, які можуть передаватися через повітря чи інші середовища. З огляду на аналіз пристроїв та циркуляцію інформації в компанії варто виділити наступні види ЕМК: Wi-Fi, Bluetooth, мобільний зв'язок.

Електромагнітні канали можуть використовуватися зловмисниками для перехоплення інформації, наприклад, зловмисник може використовувати радіопристрій, щоб перехоплювати сигнали, що надсилаються між бездротовим пристроєм і точкою доступу Wi-Fi.

Для захисту від електромагнітних каналів витоку інформації можна використовувати методи криптографії та фізичні заходи захисту.

Криптографія дозволяє захистити дані, що передаються через електромагнітні канали шляхом шифрування інформації.

Фізичні заходи захисту включають використання екранування, яке допомагає блокувати електромагнітні хвилі, а також розташування пристроїв у приміщенні, що знижує ймовірність перехоплення сигналів.

Криптографія безпосередньо не використовується в компанії для захисту, якщо не брати до уваги криптографію, що вже вбудована в певні пристрої та технології зв’язку (наприклад мобільний зв’язок)

З фізичних заходів варто порадити наступні методи:

- екранування стін: зменшить радіус розповсюдження сигналів за межі будівлі;

- розташування передаючих пристроїв в центрі будівлі: зменшить радіус розповсюдження сигналів за межі будівлі;

Також варто порадити ряд організаційних заходів:

- не використовувати відкриті мережі для передачі критично важливої інформації;

- періодично змінювати паролі доступу до бездротових мереж.

Аналіз технічних каналів витоку інформації через допоміжні технічні засоби і системи та сторонні провідники

Зв'язок між допоміжними технічними засобами, системами та сторонніми провідниками може бути здійснений за допомогою різних каналів передачі інформації. Основні канали передачі даних включають:

Канали зв'язку: ці канали використовуються для передачі інформації за допомогою телекомунікаційних мереж. До таких каналів можуть належати провідники, волоконно-оптичні лінії зв'язку.

Канали зберігання даних: ці канали використовуються для зберігання інформації в пам'яті комп'ютерів, серверів, зовнішніх жорстких дисків, флеш-накопичувачах тощо.

Канали передачі даних через хмарні сервіси: ці канали використовуються для передачі даних з одного пристрою на інший за допомогою хмарних сервісів, таких як Google Drive, Dropbox, OneDrive тощо.

Канали передачі даних через USB-порти: ці канали використовуються для передачі даних з одного пристрою на інший за допомогою USB-портів.

Далі розглянемо можливі методи запобігання витоку інформації технічними каналами витоку інформації через допоміжні технічні засоби і системи та сторонні провідники.

Запобігання витоку інформації через канали зв'язку: встанови спеціальне програмне забезпечення для моніторингу мережевої активності, встановити програмне забезпечення для запобігання вірусним атакам, обмежити коло співробітників, що мають доступ до сервера та ускладнити процеси авторизації/автентифікації.

Запобігання витоку інформації через канали зберігання даних: періодично проводити інформаційну ревізію на ПК розробників, обмежити доступ в мережу з ПК розробників, заборонити використання власних носії будь-яких форматів (лише корпоративні пристрої), фізично обмежити доступ до зовнішніх носіїв (зберігаються в спеціально призначеному захищеному місці, видаються та приймаються під запис)

Хмарні технології не використовуються компанією в виробничих процесах (окрім власного серверу з обмеженим доступом)

Канали електромагнітного випромінювання: при передачі даних по електричним лініям, таким як мережеві кабелі або шини внутрішнього комп'ютерного живлення, електромагнітні поля можуть випромінюватися з провідників і передавати інформацію з пристроїв на інші. Це може бути використано зловмисниками, щоб перехоплювати дані, які передаються по цим каналах.

Канали електричних сигналів на дротових мережах: якщо кількість електричного струму, який протікає через провідники мережі, залежить від

передаваної інформації, зловмисники можуть перехоплювати ці сигнали, щоб отримати доступ до інформації.

Канали витоку електричних сигналів на платі: на платах комп'ютерних пристроїв можуть бути провідники, які передають електричний сигнал. Зловмисники можуть сканувати ці провідники і вимірювати їх електричні властивості, щоб отримати інформацію, що передається по ним.

Щоб запобігти витоку інформації через електричні канали, необхідно використовувати захист електронної інформації, такий як криптографічні протоколи, екрановані кабелі і фільтри, щоб зменшити ефективність випромінювання електромагнітних хвиль і перешкод.

Параметричні канали витоку інформації можуть виникати в організаціях через недостатню захищеність пристроїв і систем від електромагнітного випромінювання, температурних і напругових змін, які можуть впливати на параметри електронних компонентів і забезпечити витік інформації. Деякі типові параметричні канали витоку інформації включають наступні:

Канали витоку напруги: відхилення напруги від звичайних значень може вказувати на те, що компоненти пристрою зазнали змін під впливом зовнішніх ефектів, таких як електромагнітне випромінювання або температурні зміни.

Канали витоку струму: зміни в струмі, який споживає пристрій, можуть свідчити про те, що його компоненти піддаються змінам в параметрах. Це може використовуватися зловмисниками для отримання інформації, що передається по системі.

Канали витоку тепла: збільшення температури пристрою може вказувати на вплив зовнішніх факторів, таких як радіаційне випромінювання або температурні зміни, на компоненти пристрою. Це може допомогти зловмисникам визначити відповідність між певними діями і змінами в системі.

Для досліджуваної організації та інформаційних потоків, що циркулюють в приміщеннях досліджуваного об’єкту параметричні канали витоку не актуальні або дуже мало інформативні.

Для запобігання витоку інформації через параметричні канали необхідно використовувати захист проти електромагнітного випромінювання та інших зовнішніх факторів, що можуть впливати на електронні компоненти. Також можна використовувати спеціальні методи аналізу для виявлення змін у параметрах та маскувати їх.

Наприклад, методом запобігання витокам інформації по тепловому каналу можна вважати теплоізоляцію та складну схему розподілу тепла та вентиліції, що дає змогу зменшити зовнішні прояви параметра та ускладнити їх фіксацію.

Для досліджуваної організації параметричні канали витоку не актуальні.

Акустичний ТКВІ – може бути підслухана розмова в кабінеті директора чи кімнаті для перемовин (записана на підслуховуючий пристрій). Окрім того підслуховування може бути здійснене з даху чи підвалу через вентиляційні канали.

Віброакустичний ТКВІ – підслухати голосову мовну інформацію можна знімаючи її за допомогою спеціальних пристроїв з природніх мембран.

Оптико-електронний (лазерний) ТКВІ утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких відбиваючих поверхонь (скла вікон, картин, дзеркал і т. д.). канал може бути використано для зняття мовної інформації з вікон кабінету директора.

Для запобігання витоку інформації акустичними каналами можна порадити наступні кроки.

Перенести всі важливі переговори з партнерами, обговорення стратегі та планів в спеціальну кімнату для перемовин. Її місце положення в будівлі та архітектурні особливості зменшують ризики витоку: кімната не має вікон, кімната розташована далеко від основних вентиляційних каналів (див схеми поверхів).

Додаткові методи:

1) Прибрати двері з холу в кімнату для перемовин і залишити вхід лише з кабінету директора;

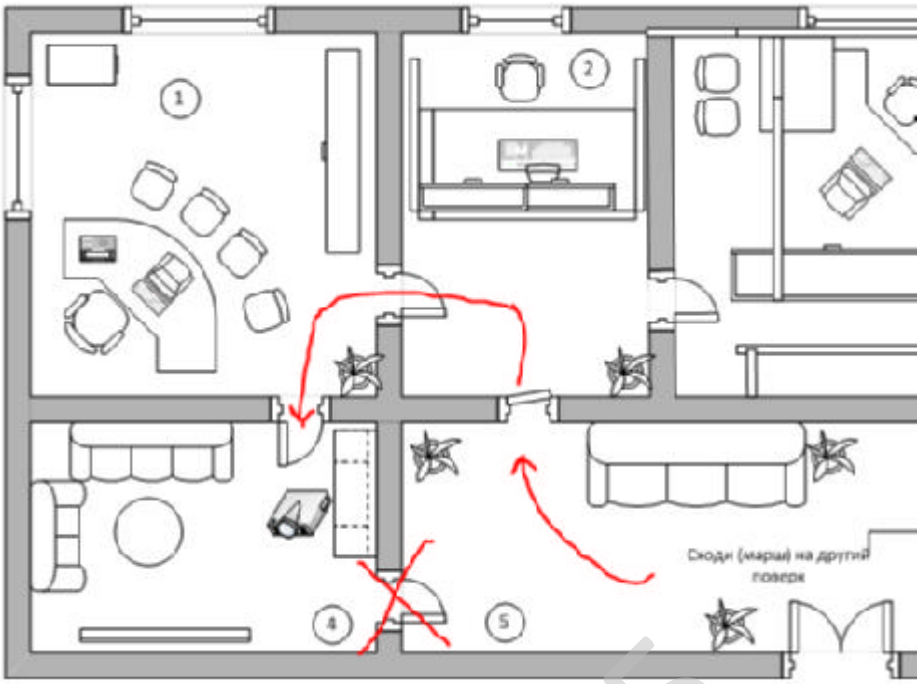

Рисунок 1.9 – Поради перепланування робочих зон

Початково таке планування робилося для зручності, інколи (окрім перемовин з партнерами) в цій кімнаті проходять важливі наради з технічними спеціалістами як штатними такі не штатними. Але з метою зниження ризику прослуховування їх варто прибрати.

2) Хоча при проектуванні внутрішні стіни приміщення включали звукоізоляційний шар, можна порекомендувати зробити в цій кімнаті додаткову звукоізоляцію

3) Обладнати кімнату детекторами прослуховуючих пристроїв та мікрофонів.

4) Вмикати в кабінеті директора голосну музику під час важливих перемовин в спец.кімнаті: музики не буде чути в кімнату за рахунок гарної звукоізоляції, а зовні музика (наприклад з колонок комп’ютера) буде виступати генератором шуму, що завадить підслуховуванню.

В якості об’єкту розглядається підприємство НВО "S Beta". Компанія займається розробкою та впровадженням систем діагностики та аналізу медичних показників в сфері кардіології. Компанія не є державною установою чи установою, що обробляє секретну державну інформацію. З огляду на це ІзОД, що циркулює в

організації, не підпадає під класифікацію та нормативну базу, яка врегульовує питання обмеження доступу та рівень секретності ІзОД в державному секторі. В той же час ІзОД присутня в інформаційному просторі організації й теж вимагає аналізу та впровадження комплексу технічного захисту інформації.

Основними носіями інформації є:

- Керівник організації;
- Посадові особи організації;
- Фахівці технічного відділу;
- Документи по столах та шафах;
- Демонстраційні прилади – продукція компанії
- Технічна документація;
- Електронні носії та бази даних компанії.

Приміщення де циркулює інформація з обмеженим доступом можна розділити на дві категорії. Категорії виключно стосуються організації, що розглядається, класифікація за категоріями здійснюється за критерієм виду інформації.

1 категорія – фінансова та стратегічна інформація компанії:

1.1 Кабінет директора

1.2 Кімната для перемовин

1.3 Кабінет бухгалтера

Всі приміщення 1-ї категорії розміщено на 1 –му поверсі будівлі (див рис. 1.10)

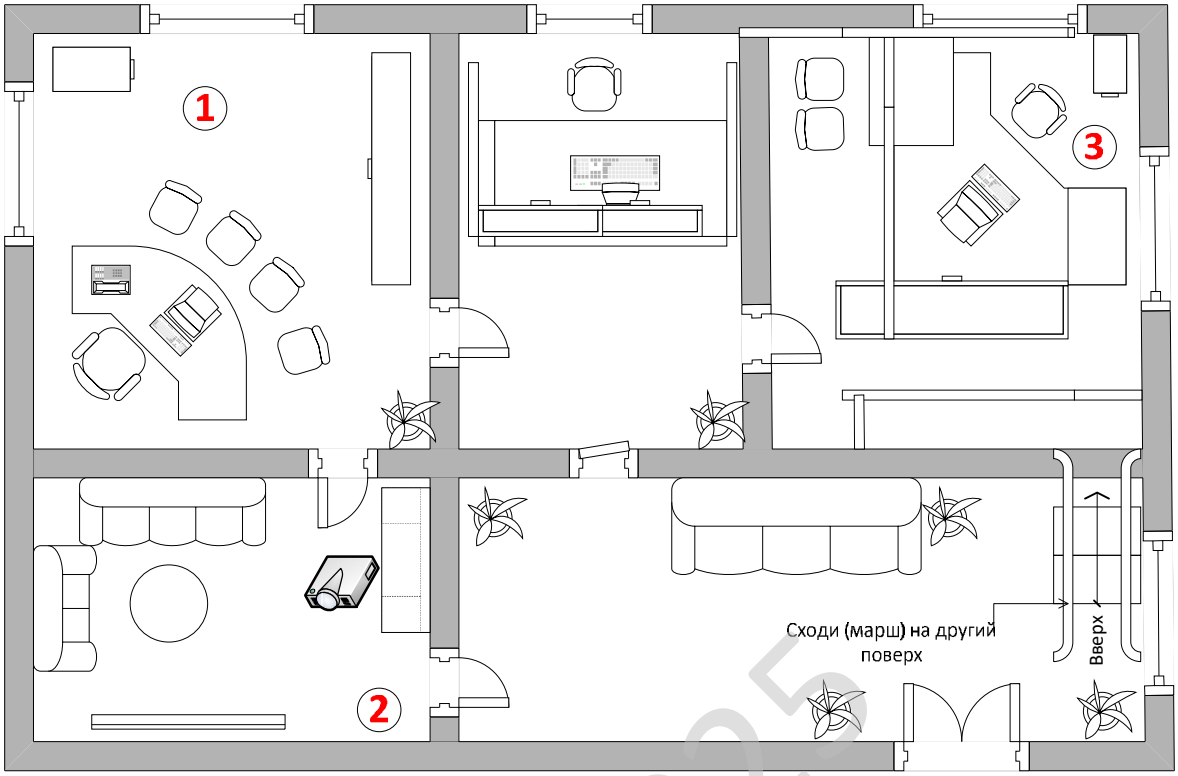

Рисунок 1.10 – Приміщення циркуляції ІзОД 1-ї категорії

Інформація озвучується та зберігається в приміщеннях : 1, 2, 3. В приміщенні 2 виключно озвучується, інформація зберігається та обробляється на ПК в приміщеннях: 1, 3.

2 категорія – технічна та проектна інформація:

2.1 Відділ монтажу обладнання та підтримки

2.2 Серверна кімната

2.3 Відділ розробки програмного забезпечення

Всі приміщення 2-ї категорії розміщено на 2 –му поверсі будівлі (див рис. 1.11)

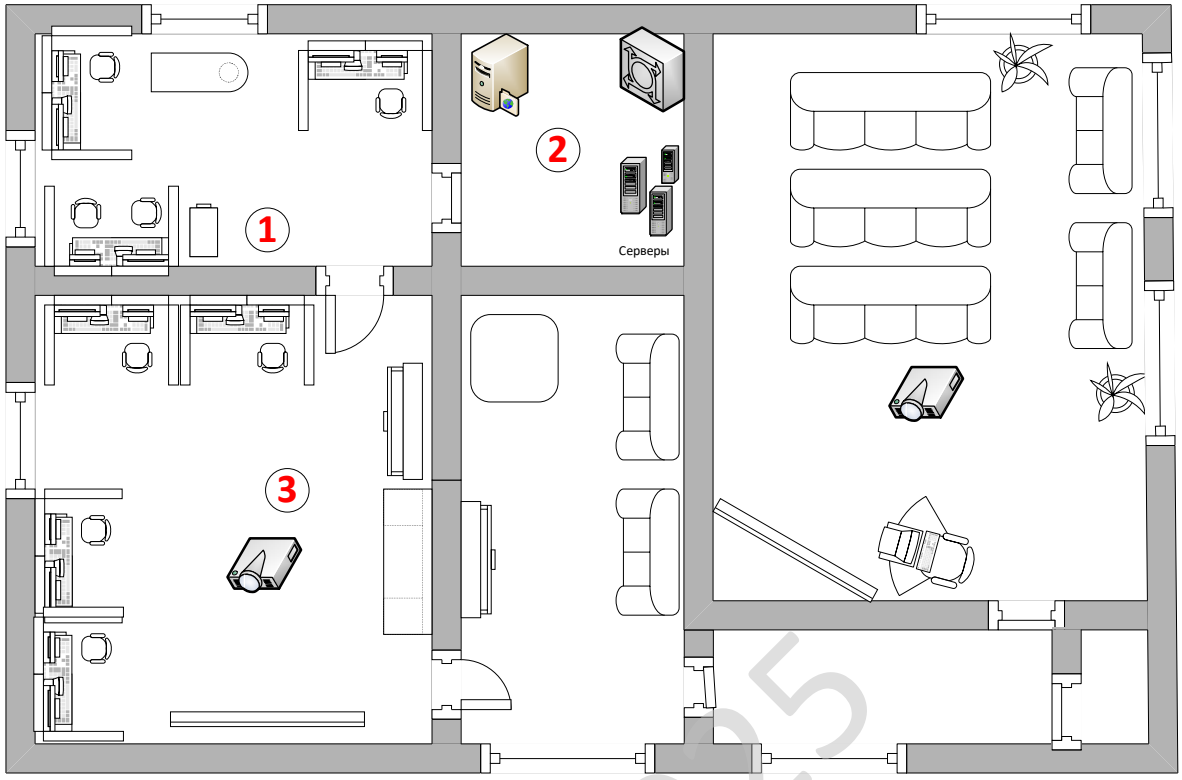

Рисунок 1.11 – Приміщення циркуляції ІзОД 2-ї категорії

Інформація озвучується в приміщеннях : 1, 3, інформація зберігається та обробляється на ПК в приміщеннях: 1, 2, 3.

Охарактеризуємо основні види ІзОД 1-ї та 2-ї категорії.

В таблиці 2.3 приводиться класифікація інформаційних активів організації та оцінка її критичності, виберемо лише ті види інформації, що є критичними з точки зору діяльності та конкретності організації. Саме ці ІзОД і підлягають особливому захисту.

1 категорія – фінансова та стратегічна інформація компанії:

Статут та установчі документи компанії – зареєстровані документи зберігаються в сейфі директора, матеріальний носій – папір. Не обговорюються і не обробляються в процесі діяльності компанії

Договори з партнерами – підписані договори зберігаються в сейфі директора, договори обговорюються з партнерами в кабінеті директора (П1, рис. 1.10) або кімнаті для перемовин(П2. рис. 1.10). Електроні копії договорів зберігаються на

ПК директора та головного бухгалтера. Електронні договори оброблюються в ході реалізації фінансових бізнес-процесів та аналізу економічної діяльності компанії.

Платіжні реквізити та платіжні документи – зберігаються на ПК головного бухгалтера, оброблюються в ході реалізації фінансових бізнес-процесів та аналізу економічної діяльності компанії.

Облікові та реєстраційні дані співробітників та клієнтів - зберігаються на ПК директора, оброблюються в ході реалізації організаційних бізнес-процесів, кадрової політики та менеджменту (прийом/звільнення/переведення співробітників).

2 категорія – технічна та проектна інформація:

Алгоритми аналізу даних – зберігаються на ПК керівника відділу розробки, оброблюються та інтегруються в програмні комплекси, що їх розробляє організація. Тимчасовий доступ мають всі співробітники відділу розробки за необхідності впровадження того чим іншого алгоритму.

Вихідні коди програм обслуговування - зберігаються на ПК керівника відділу розробки та на робочих місцях (ПК) розробників, вихідні коди та проектна документація зберігається на GitHub (сервер організації). Обговорюється під час мітингів та нарад з приводу стану проекту та вирішення конкретних проблем по проекту. В обговорені приймають участь: керівник відділу розробки, група розробників. Інколи до обговорення можуть залучатись співробітники відділу монтажу та підтримки, директор, замовники чи професійні консультанти.

Ступінь обмеження доступу визначимо у вигляді груп працівників, які можуть мати доступ до інформаційних активів наведено в наступній таблиці.

Таблиця 1.5 – Ступінь обмеження доступу до інформаційних ресурсів

Актив	Необмежений доступ	Обмежений/тимчасовий доступ	Доступ надається по запиту
Фінансова та стратегічна інформація			
Статут та установчі документи компанії	Директор	Головний бухгалтер	Співробітники компанії
Договори з партнерами	Директор Головний бухгалтер		
Платіжні реквізити та платіжні документи	Директор Головний бухгалтер		
Облікові та реєстраційні дані співробітників та клієнтів.	Директор Головний бухгалтер		Керівники відділів
Проектна та технічна інформація			
Алгоритми аналізу даних	Директор Керівник відділу розробки	Програмісти, що розробляли алгоритми	Програмісти, що працюють над проектом, де мають бути застосовані алгоритми
Вихідні коди програм обслуговування	Директор Керівник відділу розробки Задіяні в проекті розробники	Програмісти на етапі підтримки	Програмісти, за необхідністю використання кодів в подібних проектах

Проведений аналіз є підставою та обґрунтуванням при проектуванні системи відеоспостереження та конкретно визначає місця розміщення камер та вибір їх технічних характеристик.

Інтеграція модуля розпізнавання облич дає додаткові можливості при аналізі проникнення в приміщення з ІзОД несанкціонованих користувачів та подальшому розслідуванні інцидентів.

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

Сучасні системи відеоспостереження служать для віддаленого отримання відеоінформації про об'єкт спостереження і мають широке поширення. Залежно від виду застосовуваного обладнання системи відеоспостереження поділяють на аналогові та цифрові.

Аналогові системи відеоспостереження

Основоположники у розвитку відеоспостереження, але у зв'язку з інтенсивністю розвитку технологій рідко можна зустріти систему, побудовану виключно на аналогових камерах. І можна вже сміливо сказати, що аналогова система відеоспостереження – це минуле століття. Основу аналогових систем становили камери відеоспостереження оптичні прилади з ПЗЗ-матрицею(CCD), яка утворює відеосигнал із світлового потоку, одержуваного через об'єктив та лінзи пристрою. У перших реалізованих проектах запис із камер аналогових систем відеоспостереження велася на відеомагнітофон із виведенням на монітор. Для того, щоб переглянути архів, без переривання запису, оператору необхідно було встановити два відеомагнітофони для можливості перегляду запису на резервному пристрої, а при роздруківці необхідного кадру використовувати специфікований і досить дорогий принтер. До недоліків можна віднести так само і те, що система підтримує лише один канал аудіо запису та немає можливості розширення функціоналу системи.

Рисунок 2.1 – Аналогова система відеоспостереження

Комбінована система відеоспостереження

У ролі записуючого пристрою даної системи виступає цифровий відеореєстратор з можливістю встановлення жорсткого диска, аналогові роз'єми для підключення коаксіальних кабелів і монітора, Відеореєстратор - це модернізований відеомагнітофон, який веде запис не на магнітний носій, а на жорсткий диск. І нині знайшов широке застосування, у зв'язку з розширеними можливостями, на відміну його попередника. Функцію відеореєстратора, як пристрою, може виконувати комп'ютер із встановленою платою відеозахоплення і відповідним програмним забезпеченням.

Рисунок 2.2 – Комбінована система відеоспостереження

У наведених прикладах видно, що системи аналогового відеоспостереження від комбінованого один від одного, в цілому, нічим не відрізняються, наприклад, канал передачі даних здійснюється через коаксіальний кабель пристрій спостереження, в обох випадках є аналогова відеокамера.

При порівнянні комбінована система відеоспостереження має масу переваг перед аналоговою, а саме: висока якість відеозапису, відсутня необхідність у постійній зміні джерела зберігання даних, спрощений пошук та перегляд записаних подій. Крім того, якщо відеореєстратор має підтримку функції датчика руху, то система стає схожою, за рахунок функціонала, на цифрову систему відеоспостереження.

Недолік комбінованої системи в тому, що при проектуванні необхідно дороге обладнання і комплектуючі, такі як: коаксіальний кабель, з підтримкою передачі даних на 50 м., плата відео захоплення і відеореєстратор, з обмеженою кількістю аналогових роз'ємів, і конвертація аналогового сигналу в цифру і назад значно знижує якість зображення, що відображається на моніторі.

Комбіновані системи відеоспостереження, незважаючи на перелічені недоліки, знайшли широке застосування на невеликих об'єктах, таких як: магазини, заклади надання послуг, приватні будинки.

Гібридна система відеоспостереження

Застосовують на великих територіально-розподільчих об'єктах, де основним критерієм є безпека та охорона території. І з цими вимогами справляється гібридна система відеоспостереження за рахунок спільної роботи аналогового обладнання із цифровим. Робота системи організована через відеосервер або гібридний відеореєстратор, в яких передбачені порти підключення аналогових роз'ємів, так і цифрових. Вартість таких систем порівняно з комбінованими висока, але реалізуються через доцільне використання, без необґрунтованих витрат, наприклад, набагато дешевше буде встановити в приміщенні охорони аналогову відеокамеру, ніж цифрову.

В основі системи відеоспостереження лежить гібридний відеореєстратор, який може бути як готовий пристрій, так і комп'ютер з платою відеозахоплення, який дає можливість об'єднати в одну систему цифрові та аналогові відеокамери.

Гібридний відеореєстратор надає оператору можливість переглядати відеопотік не тільки через екран монітора, підключений безпосередньо до апарату реєстрації, а й через Інтернет. В останньому випадку для перегляду відео необхідно використовувати спеціальне програмне забезпечення або Web-браузер. Диспетчерські пункти або місця візуального контролю необхідно забезпечити засобами фізичного обмеження доступу з метою безпеки, в противному випадку несанкціоновані користувачі можуть отримати доступ до будь-якої відеокамери даної системи.

Недоліком даної системи є те, що зі збільшенням кількості камер виникає необхідність заміни обладнання. Оскільки розробки по розширенню функціоналу комплектуючих відеореєстраторів відстає від темпу розвитку комп'ютерних технологій, то використання даної системи доцільно тільки для певної кількості камер без можливості модернізації. Серед недоліків, через те, що до реєстратора є доступ з локальної мережі підприємства та з глобальної мережі Інтернет, можна відзначити можливість зараження вірусними програмами, внаслідок чого виникнення збою в роботі спеціалізованого програмного забезпечення відеореєстратора.

Рисунок 2.3 – Система з гібридними відеореєстраторами

Цифрова система відеоспостереження

Система ґрунтується на цифрових відеокамерах, які мають індивідуальну IP-адресу та вбудоване програмне забезпечення. Наявність даних функцій дозволяє їм працювати як автономні мережеві пристрої. Підключення всіх елементів системи цифрового відеоспостереження здійснюється як на основі локальної мережі Ethernet, так і безпосередньо, наприклад через модем, мобільний телефон, або бездротовий адаптер зв'язку. [1]

Як записуючий пристрій використовується мережевий відеореєстратор, який є стандартним комп'ютерним сервером із встановленим на нього програмним забезпеченням для відеозапису.

Можливість даного виду схеми організації відеоспостереження дає можливість проводити різноманітні модифікації, наприклад:

- - збільшення числа відеокамер у системі,
- - встановлення камер різних виробників,
- - модернізація сервера відеоспостереження, за рахунок заміни комплектуючих пристроїв (без придбання готового продукту).

Рисунок 2.4 – Цифрова система відеоспостереження

При розробці цифрових систем відеоспостереження все частіше приділяють рішенням важливих практичних завдань: детектування руху, відстеження траєкторій, пошук та розпізнавання об'єктів заданих класів, таких як людські обличчя, транспортні засоби, автомобільні номери, дим та вогонь. Велика увага приділяється проблемі пошуку різнопланової інформації у цифрових відеоархівах. Сучасний світ демонструє конвергенцію різних галузей діяльності. Ця тенденція дуже чітко простежується й у сфері відеоспостереження, куди дедалі інтенсивніше проникають інформаційні технології. Відеоспостереження запозичує різні

комп'ютерні та мережеві технології, на основі яких розробляються вже нові інтелектуальні алгоритми, що дозволяють розширити функціональність і підвищити ефективність систем відеоспостереження. Справа в тому, що інновації - це один з наріжних каменів, на яких збудовано з самого початку система інформаційне відеоспостереження. Справді, відеодетектори руху, автоматичне розпізнавання автомобільних номерів, відеодетектори залишених та віднесених предметів насамперед знаходять застосування у системах відеоспостереження.

Під час проведення проектування системи відеоспостереження для НВО «S Beta» було розглянуто найважливіші і актуальні методи з практичної погляду. Що дозволить надалі коректніше налаштовувати і, тим самим, ефективніше застосовувати на практиці інтелектуальні функції таких інформаційних систем відеоспостереження.

За останні роки значно зріс інтерес до цифрової обробки відеозображення, це пов'язано з різким зниженням ціни на цифрові телекамери, завдяки цьому вони стали загальнодоступними великому числу користувачів і почали широко впроваджуватись у багато сфер людської життєдіяльності, у тому числі і для вирішення завдань автономного контролю та відеоспостереження. Спочатку камери знайшли своє застосування в системах охоронного телебачення, але незабаром їх почали застосовувати у найрізноманітніших технологіях, таких як:

1. контроль і моніторинг на пропускних системах;
2. спостереження за об'єктами, що охороняються, за рухом і моніторингом транспортних засобів, що проїхали;
3. проведення дослідження контрольно-пропускного режиму;
4. виявлення перешкоди руху транспортних засобів;
5. підрахунок числа продукції, що надійшла і відпущеної.

І це далеко не повний перелік завдань, вирішення яких можна запропонувати на основі сучасних систем моніторингу та відеоспостереження.

Більш досконалі системи мають на увазі у своєму складі наявність інтелектуальних відеодетекторів руху (які для стислості ми надалі будемо також

називати просто детекторами руху), здатність яких передбачає можливість відрізняти пересування людини від, наприклад, тварини, транспорту або дерева, що гойдається на вітрі. На сьогодні небагато систем безпеки можуть похвалитися такими технічними можливостями, оскільки це суттєво веде до їх подорожчання, що відштовхує більшість користувачів. Детектування, сприяє приверненню увагу до певного монітора і автоматично реєструючи подію, що відбулася, що за наявності таких функцій в системі значно підвищують рівень безпеки об'єкта, що охороняється. Крім того, відеодетектори руху часто використовуються для інтелектуальної компресії, що дозволяє значно економити дисковий простір при архівуванні відео.

І вже в цьому виді це найважливіший аспект для систем безпеки, коли в охоронній зоні виключені будь-які рухи.

Підтримка функції детектування об'єктів, що рухаються, здатна попередити оператора системи про порушника через Інтернет або операторів стільникового зв'язку. Попереджаючи про те, що в полі зору камери відбувається якась подія. Наприклад, сповістити про особу, яка незаконно проникла на територію підприємства, тим самим сприятиме запобіганню розвитку неправомірних дій. За рахунок наявності даного модуля може попередити та сприяти у розслідуванні злочинів, а в результаті подальших незапланованих фінансових втрат.

У процесі проектування та впровадження інформаційних систем відеоспостереження є складність технологічних методів, що включають отримання цифрового відеозображення, як його обробку з можливістю виділення необхідної інформації, так і аналіз отриманої відеоінформації для вирішення певних завдань. У свою чергу, ідеальними видаються створення універсальних систем самонавчання, які в умовах можливих обмежень забезпечували б ефективний моніторинг об'єктів.

Незважаючи на те, що у світі створюється велика кількість систем, що мають різне призначення, послідовність обробки відеосигналу в них приблизно однакова. Понад те, аналіз різних систем показав, що у основі кожної їх лежать практично

одні й самі модулі. Умовно обробку відеозображень можна розділити на такі етапи:

- виділення переднього плану;
- виділення та класифікація руху об'єкта;
- спостереження траєкторією руху знайденого об'єкта;
- визначення та опис дії об'єкта.

Метод виділення переднього плану полягає у відокремлені фрагмента зображення, що рухається, від нерухомого, який називають фоновим або належить задньому плану. І від того, якою мірою акуратно і коректно було вирішено це завдання, залежить вся подальша обробка інформації, а також необхідна обчислювальна апаратура. У зв'язку з цим етап виділення переднього плану зображення та застосовуваним при цьому способам приділено особливий інтерес розробників. Проблема цього процесу обумовлений значною кількістю різноманітних чинників: власний шум камери, ступінь освітленості сцени, падіння тіней, тощо. На наступному етапі виділення і класифікації спочатку виробляють сегментацію зображення переднього плану, знаходять компактні області, які рухаються з однаковою швидкістю і вважаються об'єктами, що рухаються. Потім вони співвідносяться із заздалегідь визначеним класом: транспорт, людина, тварина тощо.

Наявність у цифрових системах модуля, здатного відрізнити статичний об'єкт від динамічного, дає велику перевагу перед аналоговими системами відеоспостереження. І з огляду на те, що в цеху вагонного депо недостатнє освітлення, а спеціалізований одяг і стаціонарні установки мають чорний колір, то при розслідуванні нещасних випадків допоможе у визначенні і знаходженні конкретного працівника в полі зору камери, так само ця функція виключає курйозні випадки у відео кадрі, наприклад, літаюча на повітрі.

Потім можливо перейти до наступного етапу - відстеження траєкторії певного об'єкта, що рухається (цей метод називається трекінгом - від англ. tracking). Для проведення трекінгу необхідно встановити взаємно-схожу

відповідність між виявленим об'єктом на наступних кадрах, для коректного проведення розрахунку та пошуку об'єкта, що цікавить, який був зафіксований камерами відеоспостереження.

Далі забезпечується тимчасова ідентифікація зазначених областей зображення та надходить відповідна інформація про об'єкт у зоні спостереження: траєкторія, швидкість та напрямок руху.

На останньому етапі при обробці зображення проходить розпізнавання та опис дії виділеного об'єкта. У найкращому разі система повинна буде видати повідомлення типу: «об'єкт пройшов до виходу та залишив територію» тощо.

Завдяки розвиненим мережевим технологіям можна створити як складну територіально-розподілену систему відеоспостереження, так і просту.

Доповнення до елементів цифрової системи відеоспостереження дозволяють розширити територіальне охоплення на основі існуючої комп'ютерної мережі, у тому числі через бездротові технології, які суттєво знижують витрати на монтаж.

Технології цифрового відеоспостереження дозволяють інтегрувати різноманітні платформи, що є основним вимогам, яким повинна відповідати система відеоспостереження. Наприклад, коли до діючої системи підключаються системи контролю доступу, охоронно-пожежної сигналізації, кондиціювання тощо.

Вбудовані функції дозволяють цифровій відеокамері самостійно приймати рішення про подавання тривожного сигналу, збільшення чіткості зображення, надсилання відео або оповіщення.

Численні приклади інтеграції систем на базі мережного відеоспостереження доводять, що вони є більш гідною альтернативою комбінованим та гібридним системам.

І все ж, при всіх численних перевагах цифрових систем, існує ряд факторів, які дещо стримують глобальну інтеграцію цифрового обладнання в області відеоспостереження. По-перше, багато користувачів відзначають тимчасову затримку відеосигналу, яка виникає при декомпресії та передачі потоку даних у мережу.

Мегапіксельні відеокамери здатні забезпечити відмінну якість зображення та велику площу огляду, що дозволяє заощаджувати на кількості камер у системі.

Насамкінець хочеться відзначити, що, незважаючи на деякі недоліки, судячи з порівняльних оцінок технічних характеристик цифрових, комбінованих і гібридних систем відеоспостереження, твердо сказати, що цифрова система відеоспостереження є на сьогодні найвигіднішим, і в той же час найбільш перспективним за функціональними можливостями візуального контролю.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Розробка програмно-апаратного комплексу відеоспостереження з інтегрованим модулем розпізнавання облич потребує використання сучасних, гнучких і продуктивних засобів програмування. Враховуючи специфіку завдань - обробку потокового відео, застосування алгоритмів комп'ютерного зору, машинного навчання та інтеграцію з апаратними засобами - до вибору інструментарію ставляться підвищені вимоги щодо надійності, масштабованості та підтримки широкого спектра бібліотек. У цьому контексті мову програмування **Python** обрано як основний інструмент для реалізації програмної частини системи.

Python є однією з найпоширеніших мов у сфері комп'ютерного зору, штучного інтелекту та розробки серверних систем завдяки своїй простоті, зрозумілому синтаксису та надзвичайно широкій екосистемі бібліотек. Його переваги особливо важливі в контексті побудови комплексних систем відеомоніторингу, де необхідно швидко інтегрувати обробку відеопотоків, модулі розпізнавання, аналітику та взаємодію з апаратними пристроями (IP-камерами, системами доступу тощо).

Рисунок 2.5 – Основний інструментарій розробки програмної частини проекту

Серед ключових причин вибору Python:

1) Велика кількість готових бібліотек для комп'ютерного зору. Мова має потужні засоби обробки зображень та відео (OpenCV, dlib, face_recognition), що дозволяють швидко реалізувати модуль розпізнавання облич.

2) Зручність інтеграції з нейронними мережами. Python є стандартом де-факто для роботи з глибоким навчанням через PyTorch, TensorFlow, Keras, що дозволяє розширювати функціонал системи (точніше розпізнавання, детекція небезпечної поведінки тощо).

3) Підтримка роботи з апаратними інтерфейсами. Завдяки бібліотекам для мережевої взаємодії та протоколів RTSP/HTTP Python легко підключається до IP-камер, відеореєстраторів та контролерів доступу.

4) Простота розгортання та масштабування. Python дозволяє створювати кросплатформні рішення, які можуть працювати як на окремих серверах, так і в розподіленій інфраструктурі підприємства.

5) Активна спільнота та стабільна підтримка. Python постійно оновлюється, а величезна спільнота забезпечує широкий вибір рішень, документації та прикладів.

В якості середовища розробки обрано середовище Visual Studio Code. Під час інсталяції середовища необхідно обрати підтримку відповідної мови (рис. 2.6)

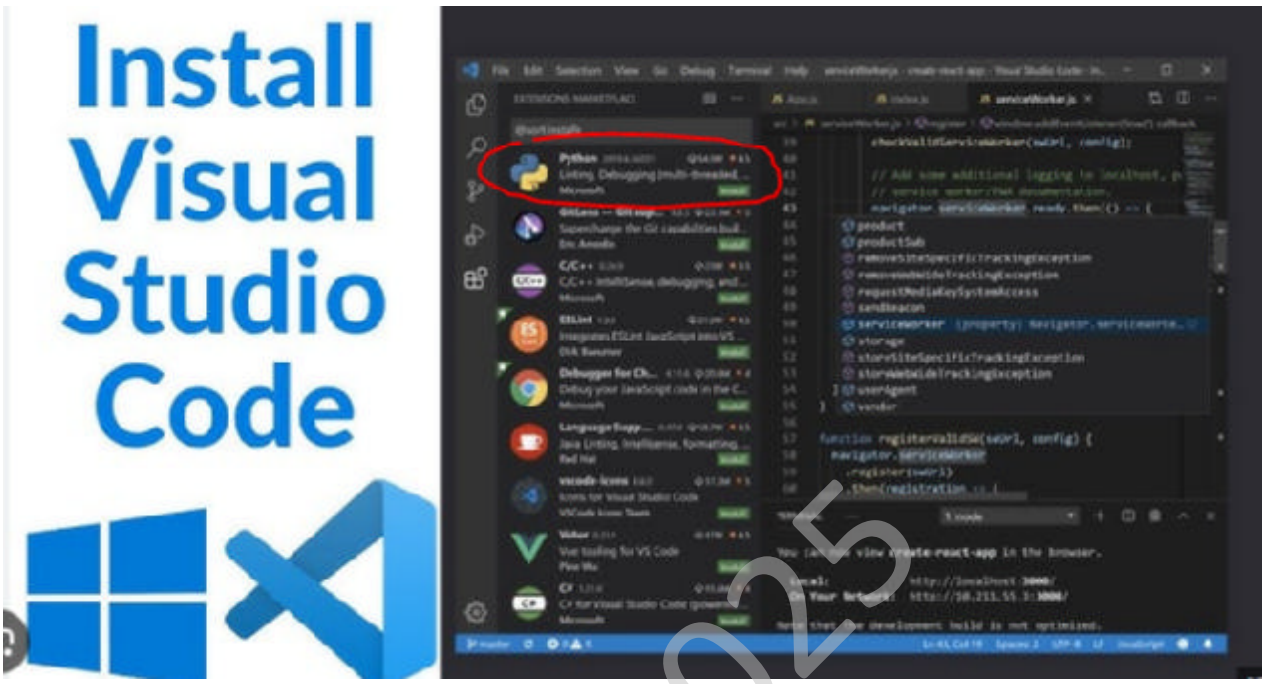

Рисунок 2.6 – Інсталяція IDE

Основні бібліотеки та фреймворки, обрані для реалізації

Для розробки програмно-апаратного комплексу обрано такі ключові програмні інструменти Python:

OpenCV

OpenCV є базовою бібліотекою комп'ютерного зору, яка забезпечує:

- роботу з потоковим відео та кадрами;
- конвертацію форматів зображень;
- детекцію об'єктів (облич, силуетів, руху);
- швидке опрацювання зображень в реальному часі.

Вона оптимізована для роботи з потоками RTSP, що робить її надзвичайно ефективною у системах відеоспостереження.

Dlib / face_recognition

Для реалізації розпізнавання облич використовуються:

- **dlib** — бібліотека, що містить високоточні алгоритми для детекції облич та визначення ключових точок;
- **face_recognition** — високорівнева обгортка над dlib, яка дозволяє:
- зчитувати біометричні ознаки облич;
- порівнювати їх з базою;
- виконувати ідентифікацію та верифікацію.

Ці бібліотеки демонструють стабільні результати навіть на середній потужності обладнання.

NumPy та SciPy

Служать для ефективних математичних операцій над масивами даних, що є критичним при обробці відеопотоку.

PyTorch / TensorFlow (опційно)

У разі необхідності реалізації більш складних алгоритмів:

- глибокі нейронні мережі для класифікації облич;
- моделі аналізу поведінки (наприклад, падіння працівника);
- виявлення небезпечних situацій.

Ці фреймворки забезпечують GPU-прискорення та можливість навчання моделей.

Flask / FastAPI

Для реалізації API-сервісу, який взаємодіє з:

- клієнтськими застосунками;
- веб-інтерфейсом моніторингу;
- базою даних із біометричними профілями.

FastAPI забезпечує швидку роботу, асинхронність та високу продуктивність, що важливо для обробки потокових запитів.

SQLite / PostgreSQL

Для зберігання даних:

- біометричних шаблонів облич;
- журналів доступу;
- архівів подій;

– метаданих відеозаписів.

PostgreSQL рекомендовано через масштабованість та можливість обробки великих обсягів логів.

Взаємодія Python зі стороннім обладнанням

Для інтеграції Python із програмно-апаратним комплексом застосовуються:

RTSP/ONVIF-протоколи: Дозволяють отримувати відеопотоки з IP-камер у реальному часі.

Requests, aiohttp: Для взаємодії з мережею, веб-сервісами, модулями доступу та внутрішнім API підприємства.

Бібліотеки для Raspberry Pi / NVIDIA Jetson (опційно): Якщо частина обчислень переноситься на периферійні пристрої (edge computing).

Переваги екосистеми Python у контексті даного проекту

Швидка розробка прототипів дозволяє оперативно створити робочу модель, протестувати її на реальних відеопотоках та адаптувати. Масштабованість Python підтримує розподілені системи, що важливо для розширення мережі камер. Інтеграція з різними ОС надає можливість запуску сервера відеоаналітики на Windows, Linux або хмарних платформах.

Для пришвидшення реалізації окремих частин та автоматизації написання коду використовувались інструменти ШІ (рис. 2.7). конкретно було використано пакет - The open source AI code editor.

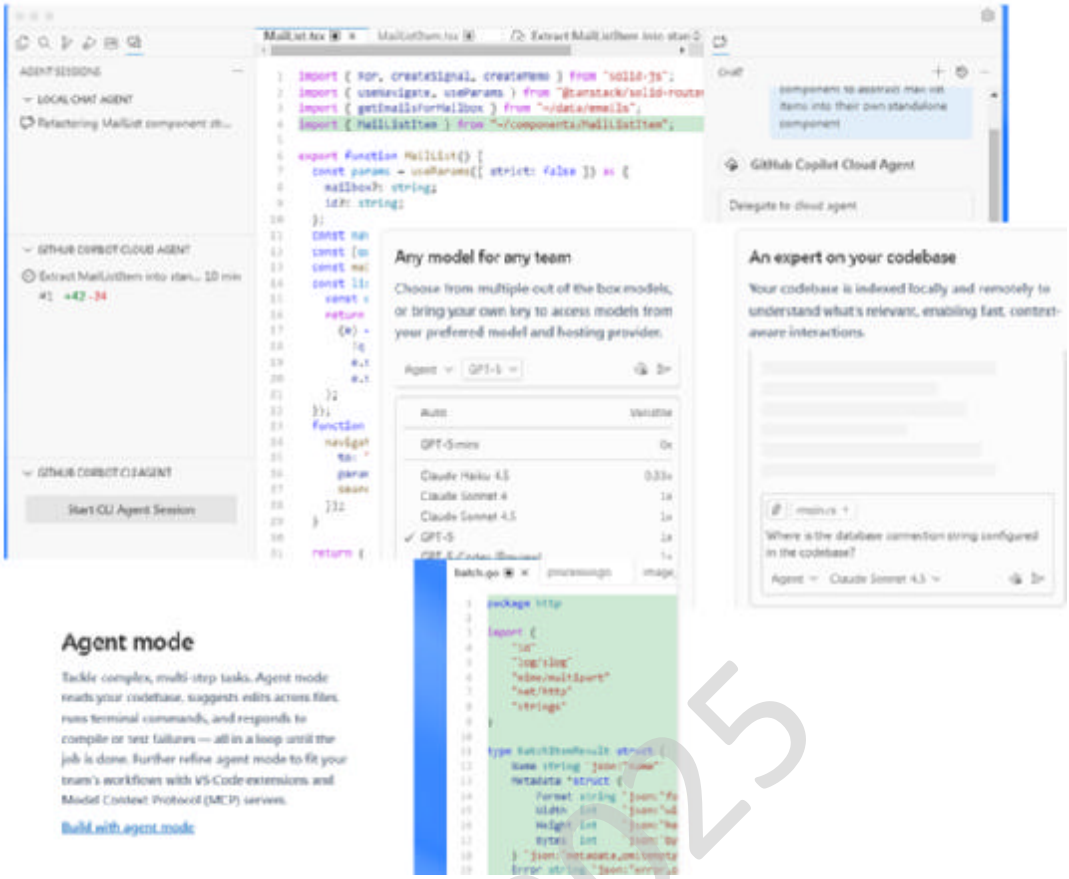

Рисунок 2.7 – Інтегровані інтелектуальні інструменти розробки

Використання Python як основного інструменту для розробки програмно-апаратного комплексу відеоспостереження є оптимальним рішенням, оскільки мова забезпечує:

- потужний набір бібліотек для аналізу відео та розпізнавання облич;
- легку інтеграцію з апаратними пристроями підприємства;
- можливість створення гнучкої, масштабованої та продуктивної системи;
- мінімальні витрати часу на розробку та тестування.

Завдяки гнучкості та потужності Python, комплекс отримує потенціал для подальшого розвитку: від удосконалення алгоритмів розпізнавання до впровадження нових модулів інтелектуальної аналітики, що робить його універсальним та перспективним рішенням для промислових підприємств.

2.3 Розгорнута постановка завдання

Загальні положення

Проектування системи відеоспостереження здійснюється з метою підвищення рівня технічної та інформаційної безпеки науково-виробничого підприємства, забезпечення контролю за діяльністю персоналу, дотриманням технологічних процесів, а також запобігання несанкціонованому доступу до об’єктів підприємства.

Система повинна бути частиною комплексної системи безпеки підприємства та інтегруватися з іншими підсистемами (охоронною сигналізацією, системою контролю доступу, пожежною сигналізацією, мережею передачі даних).

Мета проектування

Розробка технічного рішення, що забезпечує:

- цілодобовий відеоконтроль за ключовими зонами підприємства;

- оперативне виявлення порушень режиму безпеки, аварійних або позаштатних ситуацій;

- реєстрацію та архівування відеоінформації для подальшого аналізу;

- аналітичну обробку відеоданих з можливістю пошуку подій, розпізнавання об’єктів, часу та осіб;

- захист даних і розмежування прав доступу користувачів.

Об’єкти спостереження

Система охоплює наступні категорії об’єктів:

Територія підприємства - огорожа, в’їзди, КПП, автостоянки, склади, лабораторні та виробничі приміщення, згідно аналізу, проведеного в П. 2.3.

Виробничі приміщення – приміщення збору обладнання та монтажу, лабораторії, ділянки з обладнанням підвищеної небезпеки, експериментальні стенди.

Адміністративні приміщення - хол, рецепція, коридори, архіви, кабінети керівництва.

Складські та експедиційні зони - місця зберігання сировини, готової продукції, завантаження і розвантаження.

Основні функціональні вимоги до системи

Безперервний моніторинг і запис відеоінформації у реальному часі.

Віддалений доступ до системи через захищений веб- або клієнтський інтерфейс.

Ідентифікація подій та руху в кадрі з можливістю автоматичних сповіщень.

Розпізнавання та фіксація руху осіб по території на основі інтеграції програмного модуля та бази даних облич співробітників компанії.

Архівування відео з можливістю швидкого пошуку за часом, подіями або камерою.

Розмежування доступу операторів, адміністраторів та керівництва.

Масштабованість системи — можливість розширення кількості камер без суттєвої зміни інфраструктури.

Інтеграція з існуючими мережевими, охоронними та інформаційними системами підприємства.

Захист каналів передавання даних шляхом використання шифрування та авторизації користувачів.

Надійність та безперебійність роботи — забезпечення резервного живлення та дублювання критичних вузлів.

Технічні умови та середовище експлуатації

Система експлуатується в умовах промислових приміщень та зовнішніх об’єктів із температурним діапазоном від –30°C до +50°C.

Джерела живлення — основна електромережа 220 В, резервне живлення від UPS. Система повинна підтримувати мережеву архітектуру на базі IP-технологій, з можливістю централізованого керування. Відеодані зберігаються не менше 30 діб у централізованому архіві.

Очікувані результати проектування

У результаті проектування повинно бути створено:

- технічне рішення з вибором оптимальної конфігурації обладнання (камери, сервери, комутатори, сховище);

- структурна та принципова схема системи відеоспостереження;

- специфікація компонентів;

- рекомендації щодо розміщення відеокамер та кабельних трас;

-розрахунок необхідного об’єму сховища даних;

- опис програмного забезпечення та налаштування системи доступу;

- інструкції з експлуатації та технічного обслуговування.

Очікуваний ефект від впровадження

Впровадження системи відеоспостереження дозволить:

- підвищити рівень фізичної та інформаційної безпеки підприємства;
- знизити ризики втрати матеріальних цінностей;
- забезпечити контроль за дотриманням технологічних процесів та трудової дисципліни;
- створити доказову базу для службових розслідувань;
- оптимізувати роботу служби безпеки та чергового персоналу;
- сформувати умови для подальшого розвитку «розумної» системи моніторингу на основі аналітики відеоданих.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Система відеоспостереження, розроблена відповідно до вимог підприємства, є інтегрованим апаратно-програмним комплексом, який забезпечує безперервний збір, передавання, обробку, аналіз та зберігання відеоінформації з контрольованих об’єктів. Її функціонування ґрунтується на взаємодії мережевих IP-камер, серверного обладнання, програмних модулів відеоаналітики, підсистеми зберігання даних та інтерфейсів доступу користувачів.

Збір відеоданих

Усі зони, визначені як критичні для спостереження (периметр, КПП, склади, виробничі дільниці, адміністративні приміщення), оснащуються IP-камерами різних типів - купольними, корпусними, поворотними, тепловізійними залежно від умов експлуатації.

Функціонування цього етапу включає:

- Безперервну зйомку у режимі 24/7 з автоматичною адаптацією до умов освітлення.
- Локальну попередню обробку (компенсація шумів, HDR, детекція руху на рівні камери).
- Передавання відеопотоку в центральну мережу підприємства через закриті VLAN або окремий фізичний сегмент.

Камери підтримують протоколи RTSP/ONVIF, що забезпечує їх сумісність із програмним забезпеченням системи.

Передача та маршрутизація даних

Усі відеопотоки надходять через мережеве комутаційне обладнання (PoE-комутатори, маршрутизатори безпеки) до центрального серверного вузла.

Функціонування на цьому рівні передбачає:

– Шифрування трафіку (TLS, SRTP) для запобігання перехопленню даних.

– Відокремлення потоків відеоданих від загальної корпоративної мережі через VLAN або окремий сегмент, що зменшує навантаження та ризики кібератак.

– Резервування каналів зв’язку для забезпечення безперервності роботи у випадку відмови обладнання.

Обробка та управління відеоданими

Основна обробка виконується на сервері відеоспостереження (NVR/VMS-сервер). Програмне забезпечення системи реалізує такі процеси:

1) Централізований моніторинг

У реальному часі оператори мають доступ до живого відео з будь-якої камери. Доступ здійснюється:

– через веб-інтерфейс у захищеному каналі,

– через робочу станцію з клієнтським ПЗ,

– через мобільний клієнт (за наявності відповідних прав доступу).

2) Детекція подій і відеоаналітика

Програмна підсистема забезпечує:

– детекцію руху, перетину лінії, входу в зону, залишених предметів тощо;

– автоматичне формування подій та інцидентів у системному журналі;

– розпізнавання облич персоналу на основі інтеграції модуля співставлення з базою даних співробітників;

– супровід об’єктів у кадрі;

– класифікацію подій (тривога, інформаційна подія, системне повідомлення).

Виявлені події можуть автоматично передаватися в підсистеми охоронної сигналізації, систему контролю доступу або службу охорони.

3) Система сповіщень

При фіксації порушень система генерує:

– звукові та візуальні оповіщення оператору,

– push-повідомлення на мобільні пристрої відповідальних осіб,

- автоматичні e-mail/SMS-сповіщення (за конфігурацією).

Зберігання та архівування відеоінформації

Система архівування працює на виділеному сховищі (NAS/SAN) або сервері з великою ємністю. Її функціонування передбачає: безперервний запис відео, стиснення відео, зберігання архіву на визначений конфігурацією термін (зазвичай не менше 14 днів), можливість резервного дублювання.

Архів підтримує фільтри пошуку:

- за часом,
- за подією,
- за камерою,
- за виявленою особою,
- за типом інциденту.

Інтерфейси та доступ користувачів

Система має багаторівневу модель доступу:

Оператор - перегляд відео та подій у реальному часі.

Адміністратор - налаштування камер, серверів, користувачів.

Керівництво - доступ до архіву, аналітичних звітів, ключових камер.

Аутентифікація виконується через:

- локальні облікові записи,
- корпоративний домен (Active Directory),
- двофакторну авторизацію.

Доступ до відео передбачає застосування політик шифрування та журналювання дій користувачів.

Інтеграція з іншими підсистемами підприємства

Система відеоспостереження функціонує як частина комплексної системи безпеки, що взаємодіє з іншими структурними елементами системи безпеки:

- охоронною сигналізацією (звірка подій із відео),
- системою контролю доступу (фіксація входу співробітників),
- пожежною сигналізацією (відеопідтвердження пожежних подій),

– мережею передачі даних підприємства (для централізованого керування).

Через стандартизовані протоколи (ONVIF, REST API) система може передавати інциденти іншим службам або приймати команди.

Забезпечення надійності та безперебійності

Безперервне функціонування системи забезпечується через використання допоміжних технічних засобів. В першу чергу до таких варто віднести резервне живлення та дублювання критичної інформації.

Перше особливо актуально з урахуванням поточної ситуації з енергомережами в країні. Класично резервне живлення базується або на автономному генераторі або на альтернативних джерелах живлення на основі акумуляторних батарей.

Друге (резервне копіювання) може реалізуватись на основі створення копій на відокремленому сервері чи використання різних технологій дублювання даних, наприклад на основі рейд-масиву.

У випадку відмови окремої камери система фіксує інцидент та сповіщає адміністратора.

У комплексі система забезпечує повний контроль над ключовими зонами організації. Дозволяє здійснювати постобробку даних, аналітичну обробку відеоданих для виявлення порушень або несанкціонованих дій. Наявність відеоматеріалів може виступати доказовою базою або використовуватись як допоміжні матеріали при розслідуванні інцидентів.

3.2 Розробка функціональної схеми

На основі опису функціонування системи можна запропонувати наступну функціональну схему (схема представлена на рис. 3.1).

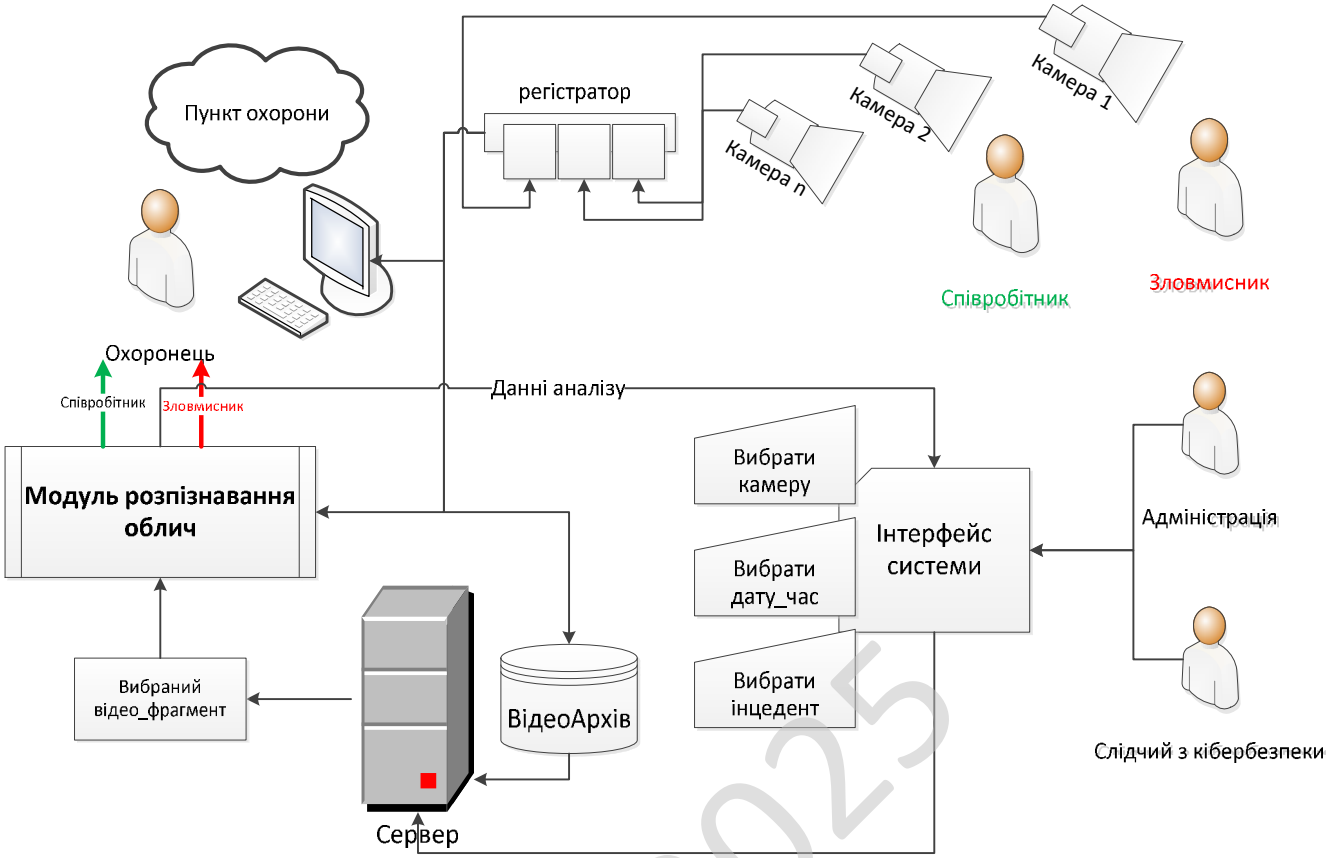

Рисунок 3.1 – Функціональна схема комплексу

Основним користувачем системи є охоронець, що несе варту на охоронному пункті. Камери розпізнають обличчя людей, що потрапляють в їх поле зору. У випадку якщо камера фіксує сторонню людину, чи співробітника, що намагається проникнути в закриту, недоступну для нього, зону (лабораторії, спеціальні приміщення, кабінети керівництва), система автоматично попереджає охоронця та вносить відповідний запис до журналу подій.

Система також може використовуватись адміністрацією. Наприклад – при виникненні підозр, щодо окремого працівника. Або ж у випадку розслідування інцидентів, відеоматеріали можуть слугувати додатковими матеріалами слідства чи доказами.

3.3 Розробка структурної схеми

В цьому пункті розглянемо структурну схему комплексу(рис. 3.2).

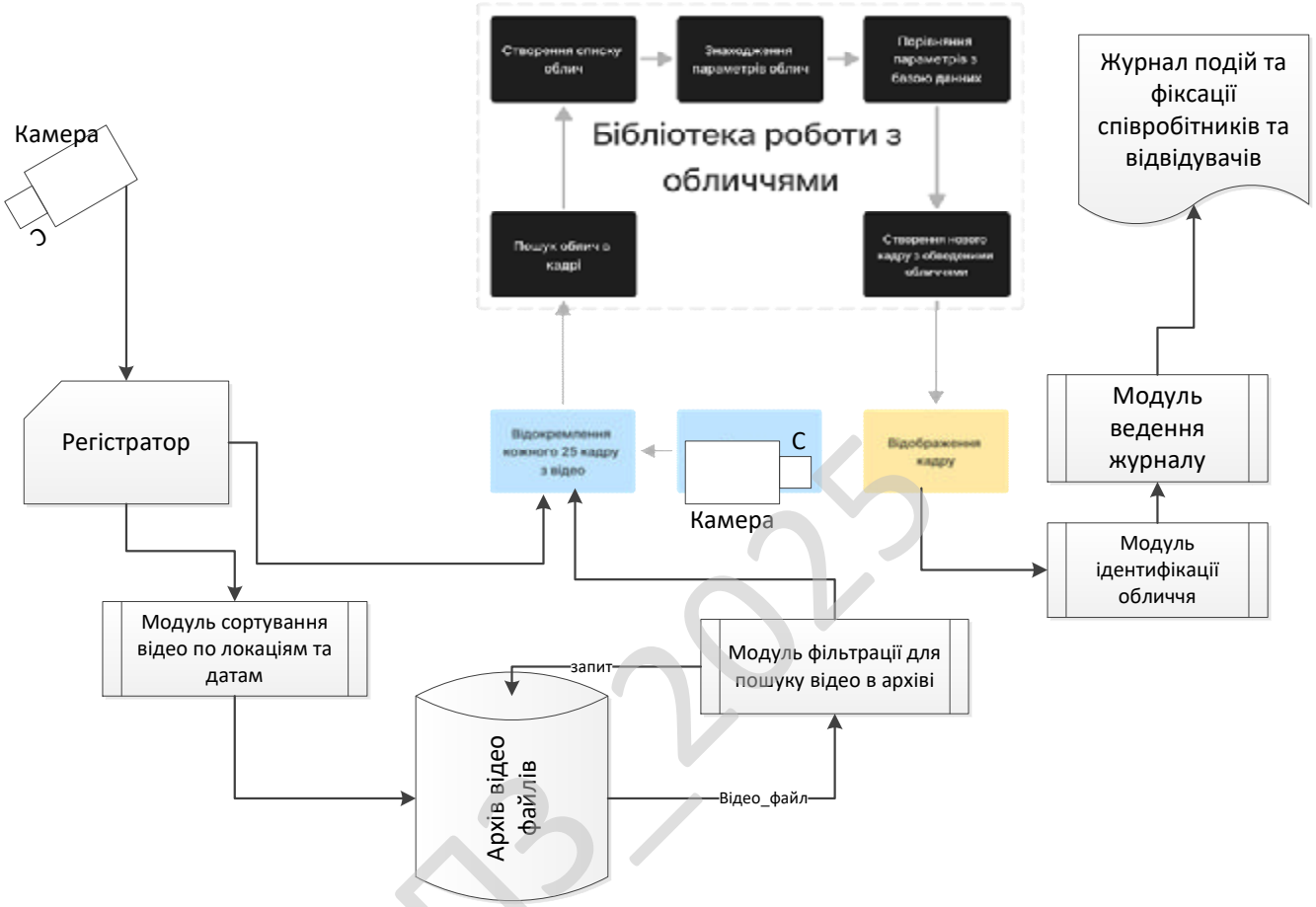

Рисунок 3.2 – Структурна схема комплексу

Представлена блок-схема відображає логічну структуру та взаємодію компонентів програмно-апаратного комплексу відеоспостереження, що включає реєстрацію відеопотоку, архівування, фільтрацію, модулі роботи з обличчями, а також систему журналювання подій. Основна мета - забезпечити автоматизовану ідентифікацію персоналу та відвідувачів на підприємстві та формування історії подій.

В якості джерела відеосигналу виступають камери (у випадку досліджуваного об’єкту 5 шт.), але на схемі умовно відображено лише дві камери.

Реєстратор - апаратний пристрій для прийому, обробки та збереження відео.

Реєстратор виконує наступні функції: приймає відеопотік від камер,

формує відеофайли, передає відео в архів відеофайлів, забезпечує доступ до потокового відео для подальшого аналізу.

Інші компоненти схеми відносяться до програмної складової системи і представллені у вигляді окремих модулів.

Модуль обробки кадрів (виділення кожного 25-го кадру) - програмний компонент, який отримує з потоку окремі кадри для подальшого аналізу.

Архів відеофайлів є центральним елементом зберігання історичних відеоданих. У ньому накопичуються файли, які надходять від реєстратора.

Взаємодія архіву з іншими модулями:

Модуль сортування відео по локаціям та датам - структуризація файлів за місцем розташування камер і часом запису.

Модуль фільтрації для пошуку відео в архіві - обробляє запити користувача на вибірку відео та повертає відповідні файли.

Функція модулів — оптимізувати пошук відео за критеріями часу, місця, події, типу інциденту тощо.

Блок **«Відокремлення кожного 25 кадру з відео»** отримує відеопотік безпосередньо від камери. Його основні функції: періодичний аналіз відео та отримання ключових кадрів, передача цих кадрів у бібліотеку роботи з обличчями**.**

Це оптимізує ресурси: розпізнавання відбувається на вибіркових кадрах, а не на всьому відеопотоці.

Бібліотека роботи з обличчями є центральним модулем системи розпізнавання, який включає кілька послідовних етапів:

1. Створення списку облич - формування масиву еталонних зображень осіб, допущених до підприємства (співробітники, відвідувачі, контрагенти).

2. Знаходження параметрів облич - має на увазі алгоритмічну нормалізацію та обчислення ознак:

- векторизація,
- формування біометричних ключів,

– видалення шумів і фонової інформації.

3. Порівняння параметрів з базою даних - одуль виконує зіставлення знайденого у кадрі обличчя з еталонами.

4. Пошук облич у кадрі - аналіз окремого кадру на предмет наявності облич та визначення їх координат.

5. Створення нової моделі обличчя. Якщо система не знаходить збігів - створюється новий шаблон (опціонально, залежно від політики підприємства). Результат передається у модуль ідентифікації.

Модуль ідентифікації облич - отримує результат порівняння від бібліотеки та визначає:

– чи належить обличчя певній особі,

– ступінь достовірності співпадіння,

– статус особи (зареєстрований співробітник, гість, невідома людина).

Дані передаються у модуль ведення журналу.

Модуль ведення журналу. Модуль відповідає за запис даних:

– час виявлення особи,

– місце розташування камери,

– результат ідентифікації,

– подія (вхід, вихід, доступ у зону).

Представлена структура програмно-апаратного комплексу відеоспостереження описує повний цикл обробки інформації — від моменту отримання відеопотоку камерами до фіксації результатів ідентифікації в журналі подій. У роботі системи поєднано апаратні та програмні модулі, що забезпечує не лише запис відеоархіву, але й можливість інтелектуального аналізу зображень у режимі реального часу. Така архітектура забезпечує підвищений рівень безпеки підприємства завдяки автоматизованому контролю входу співробітників, моніторингу переміщень та аналізу відвідуваності.

Загалом, схема відображає логічно завершену модель функціонування системи відеоспостереження з розпізнаванням облич, яка об’єднує апаратні засоби

збору відеоінформації, програмні модулі для обробки та аналізу зображень, інструменти зберігання та пошуку, а також підсистему формування журналу подій. Усі елементи взаємодіють у єдиному інформаційному середовищі, забезпечуючи високу точність ідентифікації та надійний моніторинг ситуації на підприємстві. Така архітектура підвищує ефективність засобів безпеки, мінімізує потребу в ручній перевірці персоналу та забезпечує можливість оперативного реагування на нестандартні ситуації.

3.4 Розробка діаграми процесів

Діаграма процесів це одна з діаграм в ході проектування системи, що деталізує окремі аспекти системи. В нашому випадку така діаграма буде певною мірою доповнювати та деталізувати функціональну схему в частині взаємодії користувача та програми, а також внутрішньо-модульні обміни даними в середині самої програми.

Діаграма процесів представлена на рис. 3.3

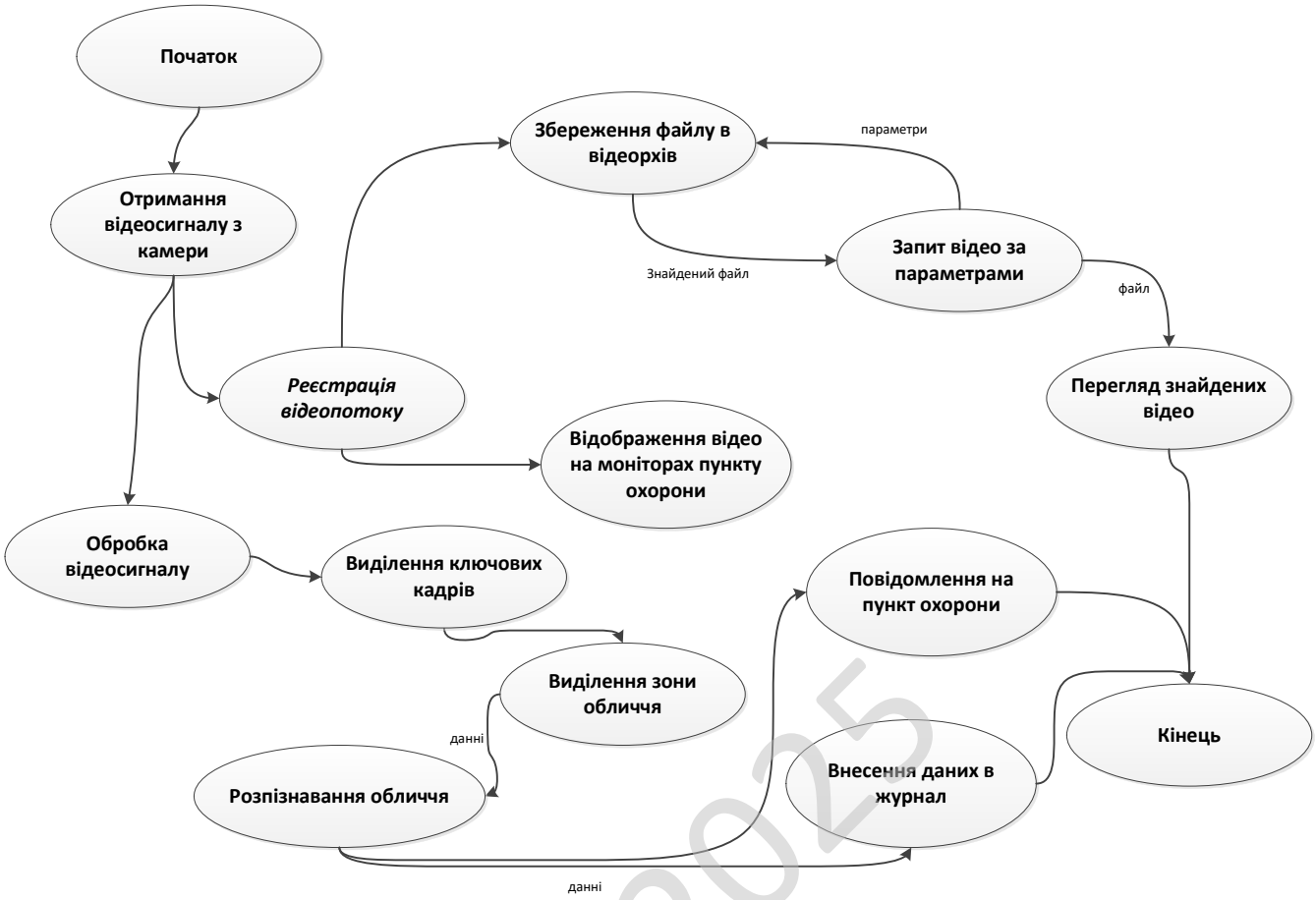

Рисунок 3.3 – Діаграма процесів

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

Традиційні методи розпізнавання облич включають розпізнавання облич на основі геометричних ознак, розпізнавання облич на основі рис обличчя та методи, засновані на прихованих марковських моделях. У розпізнаванні облич на основі геометричних ознак геометричними ознаками можуть бути очі, ніс, рот та інші форми та геометричні зв'язки між ними (наприклад, їхня відстань одна від одної). В конкретній реалізації використовувався алгоритм AdaBoost, що базується на геометричних ознаках обличчя (маркерах).

Мережа розпізнавання базується на w1 − w6, що представляє шість спільних ваг, які обчислюються вперед у прямому шарі, і вихідне значення ht прямого прихованого шару від часу 1 до часу t отримується в ході алгоритму та зберігається. У зворотному шарі виконується зворотне обчислення для отримання вихідного значення ht′ зворотного прихованого шару від часу t до часу 1, і воно теж зберігається.

Нарешті, об'єднавши вихідний результат відповідного моменту прямого шару та зворотного шару, отримується кінцевий вихід O_t, вираз якого наступний:

$$\begin{aligned} h_t &= \mathrm{f}(w_1 \mathrm{x}_t + w_2 \mathrm{h}_{t-1}), \\ h'_t &= \mathrm{f}(w_3 \mathrm{x}_t + w_5 h'_{t-1}), \\ O_t &= \mathrm{f}(w_4 \mathrm{x}_t + w_6 h'_t) \end{aligned} \tag{4.1}$$

Структура мережі представлена на рис. 4.1

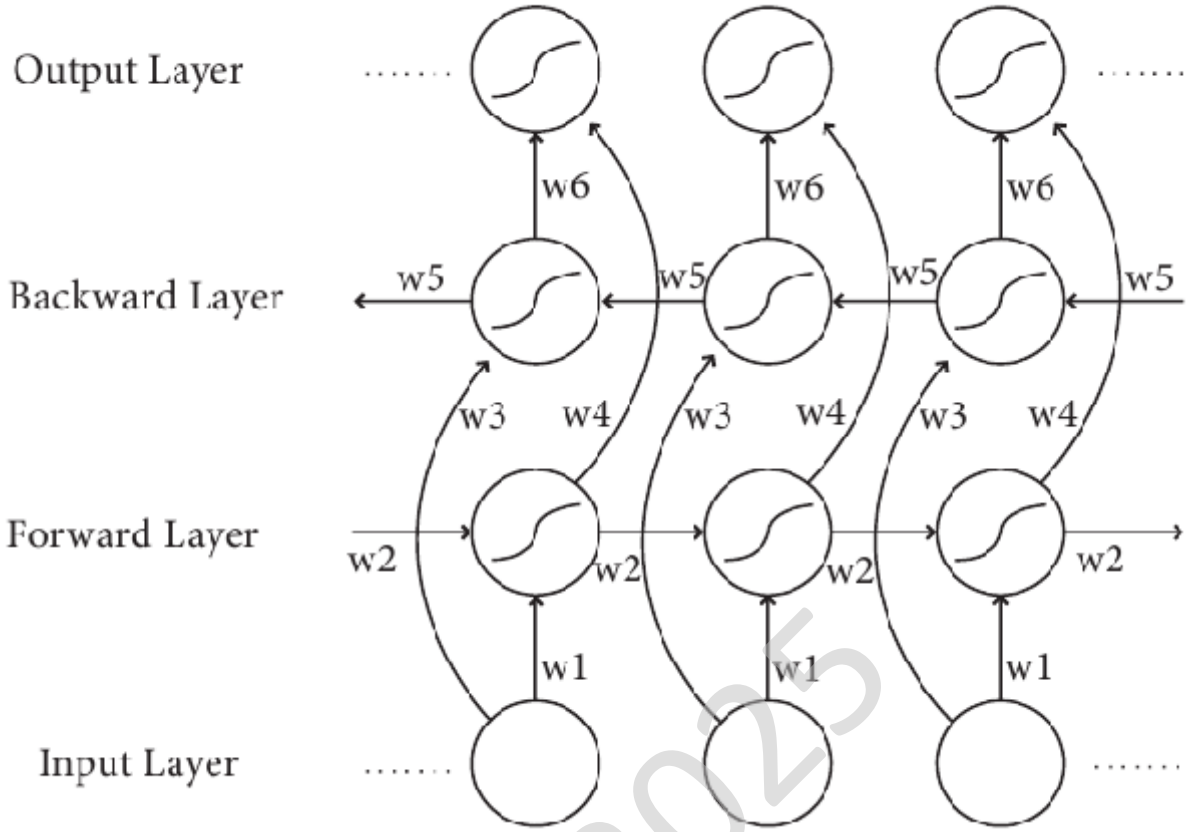

Рисунок 4.1 – Структура мережі для розпізнавання

Розглянемо окремі алгоритмічні аспекти реалізації.

Для розпізнавання необхідно створити базу облич та внести до неї всіх співробітників, для того щоб система могла ідентифікувати та розрізняти обличчя за принципом «свій-чужий».

Процес передбачає наступні кроки

1) Внесення даних про особу

На початковому етапі користувач заповнює інформацію про людину, для якої формується база зображень (наприклад, ім’я, унікальний ідентифікатор та інші дані).

2) Активування камери

Система вмикає камеру та готує її до отримання серії знімків обличчя.

3) Процес зйомки (цикл i = 1…100)

Подальша робота здійснюється в циклі, у межах якого виконується збирання 100 зображень обличчя:

Пауза 1 секунда: коротка затримка перед фіксуванням наступного кадру;

Отримання кадру: камера робить чергове фото;

Виявлення обличчя: алгоритм проводить пошук та визначення обличчя на знімку;

Збереження зображення: вирізаний фрагмент із обличчям записується у файл формату *name.i.png*, де *i* — номер знімка.

4) Оброблення отриманих фотографій

Після завершення циклу виконується аналіз усіх збережених зображень.

5) Формування ідентифікатора обличчя

Для кожного зображення генерується унікальний ID, який у подальшому зберігається в базі даних та використовується як еталонний ідентифікатор для цієї особи.

Блок-схема процесу представлена на рис. 4.2

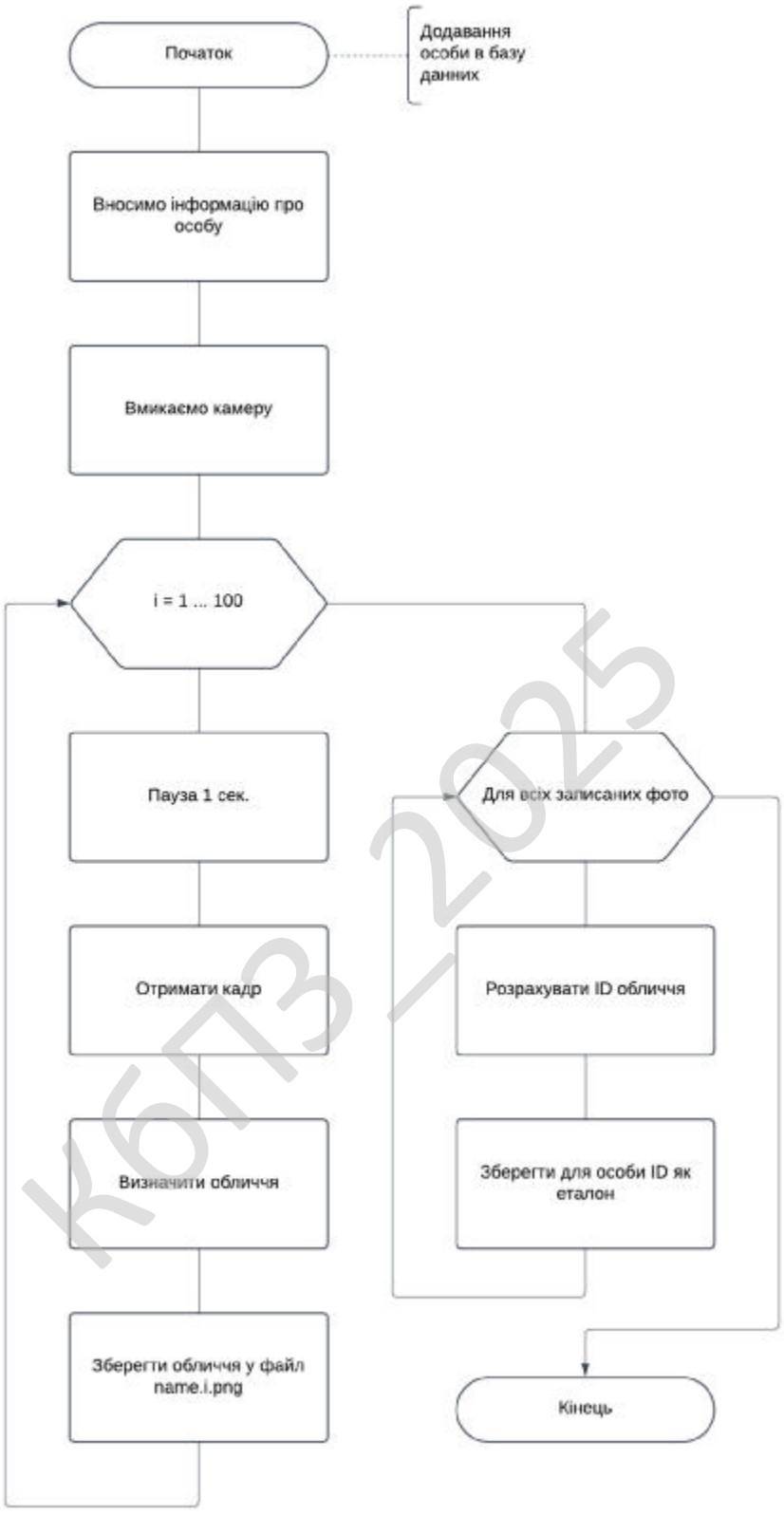

Рисунок 4.2 – Блок-схема алгоритму додавання осіб до бази даних

Безпосередньо програма, що розпізнає обличчя в потоковому режимі працює в нескінченному циклі (поки не буде завершена оператором або не

вимкнеться живлення). Блок-схема основної програми представлена на рис. 4.3.

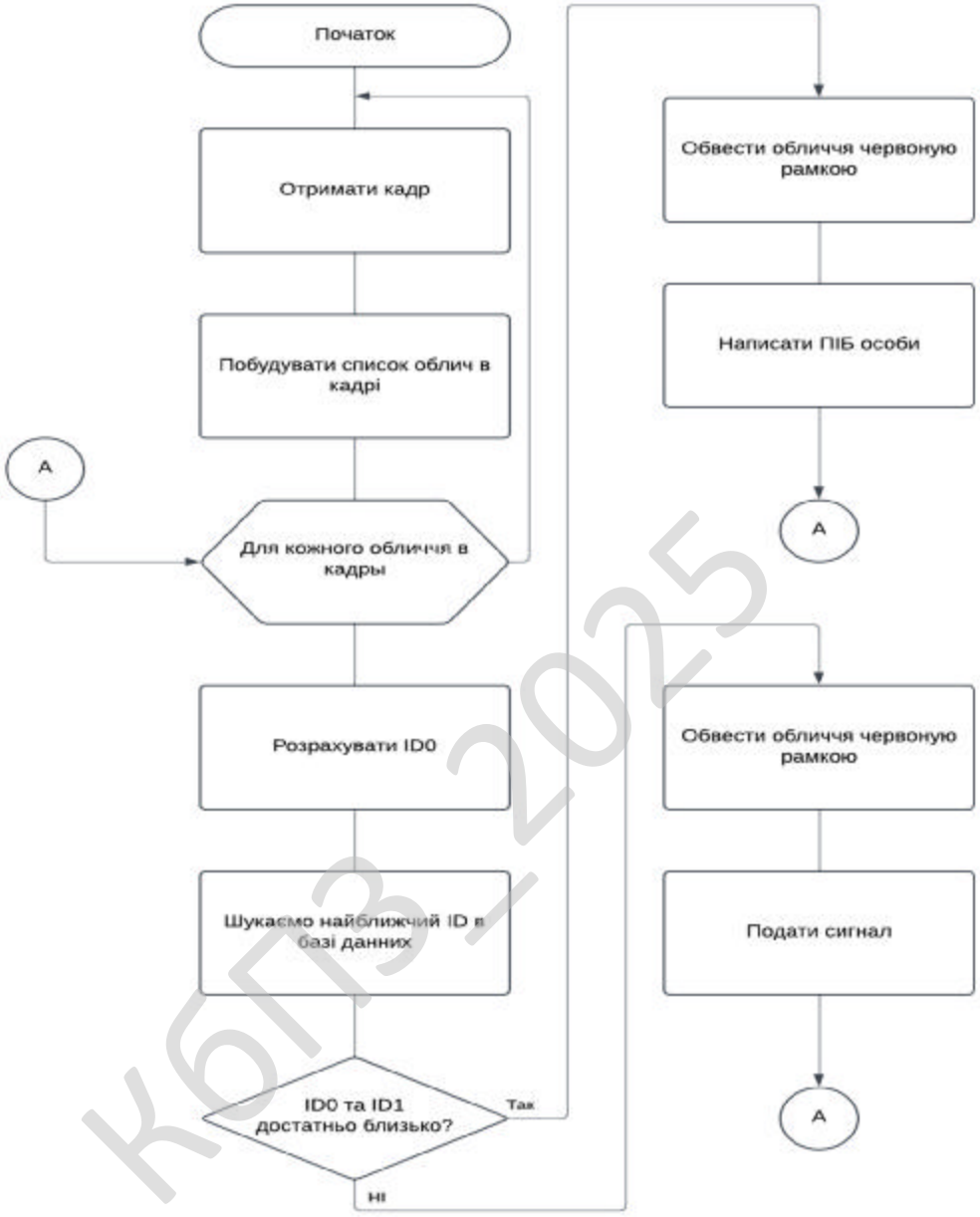

Рисунок 4.3 – Блок-схема основної програми

Програма працює в нескінченому циклі до вимкнення живлення. Розглянемо послідовність дій, які показано на рис. 4.3:

Отримання кадру: система захоплює зображення за допомогою підключеної камери.

Побудова списку облич у кадрі: алгоритм визначає всі обличчя, які присутні на отриманому зображенні, і створює їх список для подальшої обробки.

Обробка кожного обличчя у списку - для кожного обличчя зі списку виконується наступне:

- Розрахунок ID0: Генерується унікальний ідентифікатор (ID) на основі біометричних даних обличчя.
- Пошук у базі даних: Система знаходить найближчий ID (ID1) у базі даних, щоб порівняти його з розрахованим ID0.
- Перевірка збігу.

Якщо ID0 та ID1 знаходяться на достатньо близькій відстані (збіг), виконується наступне:

- Обведення обличчя червоною рамкою: Система вказує знайдене обличчя на зображенні.
- Виведення ПІБ особи: На екрані або у звіті виводиться ім’я, прізвище або інші дані, пов’язані з ID1.

Якщо збігу немає, виконується наступне:

- Обведення обличчя червоною рамкою: Вказується обличчя, яке не вдалося розпізнати.
- Подання сигналу: Генерується сигнал або сповіщення про невпізнану особу.

Після завершення обробки всіх облич модуль повертається до отримання нового кадру, і процес повторюється.

4.2 Захист розробленого програмного забезпечення

Так як в проекті активно використовується мережа одним з основних засобів захисту є мережевий захист на основі брендмауера.

Основним механізмом, що застосовується під час створення брандмауерів, є фільтрація пакетів. Пакетний фільтр, взаємодіючи з відповідним програмним

забезпеченням, фактично унеможливлює проходження несанкціонованих пакетів через проксі-сервер на шляху між мережами. Він перевіряє заголовки кожного пакета, а адміністратор визначає правила, які саме пакети можуть бути пропущені, а які - заблоковані.

Окрім IP-адрес, фільтр може аналізувати протокол, за яким передається пакет, а також служби високого рівня, з якими він пов'язаний. Наприклад, адміністратор може встановити заборону на весь WWW-трафік і дозволити передавання лише електронної пошти.

Типова структура брандмауера Internet включає три фільтри:

- один контролює пакети, що надходять з Інтернету;
- другий — ті, що виходять у зовнішню мережу;
- третій забезпечує роботу прикладного програмного забезпечення.

Захищений хост розташовується у виділеному сегменті мережі та фактично знаходиться між двома пакетними фільтрами. Перший фільтр блокує всі вхідні пакети, окрім тих, які надходять від спеціальних сервісних програм захищеного хоста. Другий аналогічно обмежує вихідні пакети — пропускаються лише ті, що призначені для спеціальних додатків цього хоста. Таким чином, увесь обмін даними між комп'ютерами організації та зовнішніми ресурсами Інтернету здійснюється через захищений хост.

На цьому хості працює спеціалізоване ПЗ - шлюзи прикладного рівня (proxy-сервери). Наприклад, при запиті користувача на отримання файлу через FTP, клієнтська програма зв'язується з FTP-проксі на захищеному хості. Proxy перевіряє дозвіл на запит, отримує файл з Інтернету, перевіряє його на віруси та лише після цього передає користувачу. Також ведеться журнал запитів для подальшого аналізу.

Першим важливим завданням адміністратора проксі-сервера є ідентифікація та авторизація користувачів. Підтримка схем NTLM, MSNT, SMB, LDAP значно спрощує цей процес, особливо коли потрібен аудит або детальна фільтрація трафіку.

Як основний каналоутворюючий протокол використовується IPSec — набір стандартних механізмів для створення VPN, що визначає методи аутентифікації, шифрування та управління ключами між вузлами IP-мережі. IPSec забезпечує:

- аутентифікацію кінцевих точок при встановленні з'єднання;
- шифрування та перевірку цілісності передаваних даних;
- автоматичний обмін секретними ключами.

Для цього IPSec застосовує три типи протоколів:

IKE (Internet Key Exchange) — ініціалізація з'єднання, вибір параметрів та обмін ключами;

AH (Authentication Header) — цілісність даних та аутентифікація джерела;

ESP (Encapsulation Security Payload) — шифрування та захист переданої інформації.

У межах однієї SA (Security Association) використовується один із протоколів — AH або ESP. Захист може працювати у транспортному або тунельному режимі. Для шифрування застосовуються DES, 3DES або AES, а для хешування — MD5 або SHA-1. У цьому випадку рекомендується використання **SHA-1**.

Для шифрування даних обрано алгоритм **3DES** — модернізовану версію DES, що усуває його основний недолік - короткий 56-бітний ключ. 3DES виконує послідовне шифрування блоків даних трьома ключами, забезпечуючи загальну довжину ключа 168 біт. Це значно підвищує стійкість до перебору.

Цілісність передаваних даних забезпечують **HMAC-коди**, які формуються шляхом обчислення хешу з секретним ключем. Це дозволяє однозначно визначити, чи був змінений пакет під час передавання.

Для обміну ключами в IPSec використовується протокол **IKE**, що базується на протоколах ISAKMP, Oakley та SKEME. Аутентифікація сторін може виконуватися за хеш-функцією або через сертифікати стандарту X.509. Після цього використовується **алгоритм Діффі–Геллмана**, який дозволяє сторонам згенерувати спільний секретний ключ, навіть обмінюючись даними незахищеним

каналом. Стійкість алгоритму базується на складності задачі дискретного логарифмування.

На завершення, для забезпечення фізичної безпеки рекомендується проводити візуальний огляд приміщень перед і після робочих нарад, звертаючи увагу на місця, де можуть бути приховано встановлені закладні пристрої. Для захисту ліній електроживлення доцільно мати власну підстанцію на території підприємства, що унеможливить витік інформації через цей канал.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Методика впровадження системи повинна передбачати в подальшому сумісність, надійність, зручність використання та забезпечувати цільову безпеку.

Подання проекту на рівні етапів (див. рис. 5.1)

Розробку програмного забезпечення можна розділити на окремі стадії, у кожній з яких у свою чергу, можна виділити окремі етапи та роботи. Відповідно до ДСТУ, зазвичай виділяють такі стадії розробки програмного забезпечення:

1. технічне завдання;
2. ескізний проект;
3. технічний проект;
4. робочий проект;
5. впровадження в експлуатацію.

У роботі раніше вже розглянуто елементи ескізного проектування, моделювання системи та елементи робочого проекту (програмна реалізація). Технічне завдання представлене в додатку А.

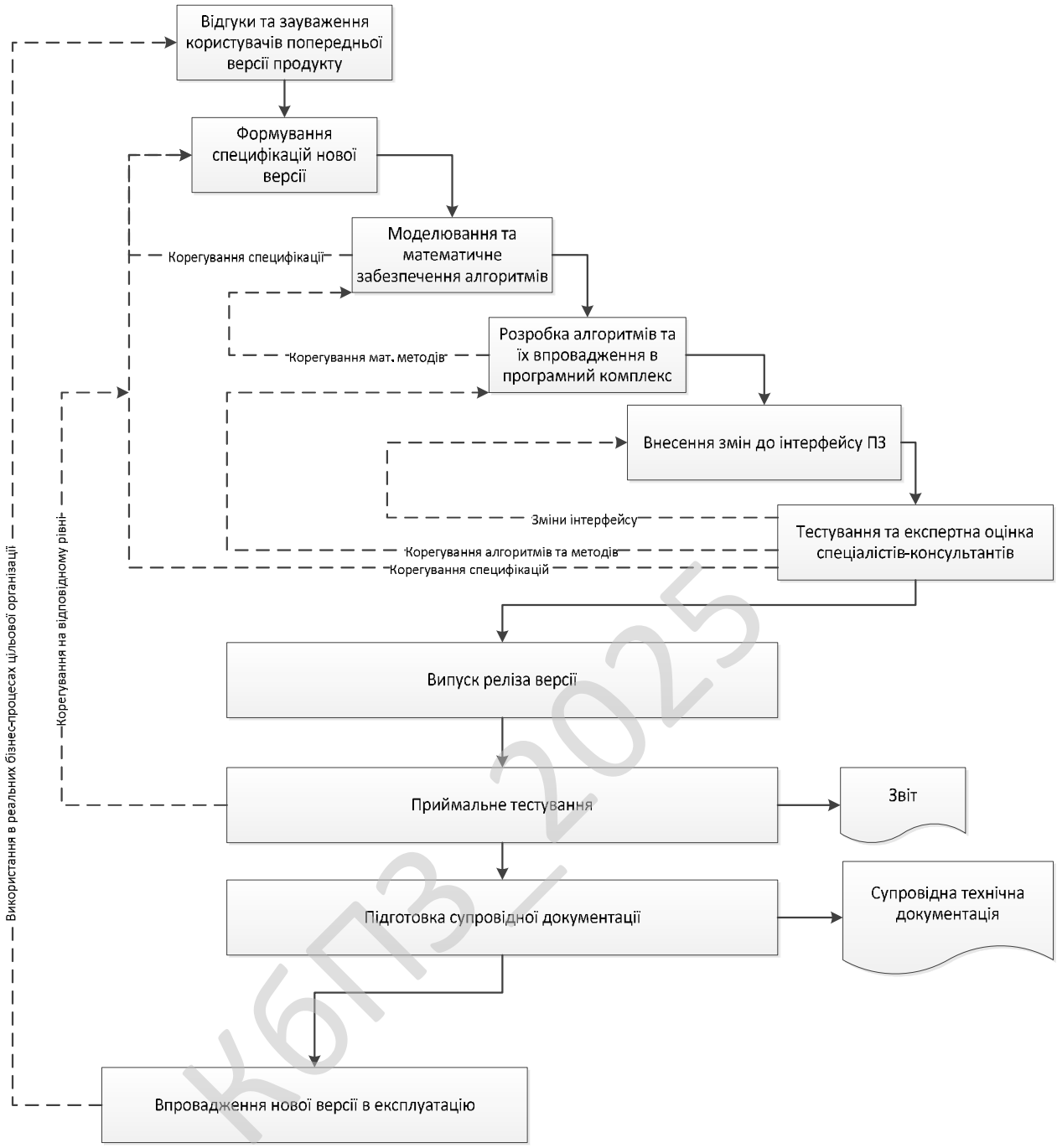

Рисунок 5.1 – Етапи реалізації проекту [23]

На першій ітерації (коли ще немає попередніх версій) перший блок замінюється на: "Результати інтерв'ювання та набір очікуваних замовником функцій". Окрім того підставами та впливаючими факторами є результати аудиту безпеки, окремі положення якого представлено в першому розділі роботи. Результати інтерв'ювання слугують основою написання постановки завдання

(технічного завдання), які описують специфікації майбутнього програмного продукту.

Далі розглянемо методику впровадження програмного комплексу.

Призначення та умови застосування

Для ініціалізації роботи системи необхідно під'єднати відеокамеру до робочої станції та переконатися у коректності її розпізнавання операційною системою. Після активації відеопотоку виконується початковий етап збору вихідних даних — здійснюється серія фотографувань співробітника, який має бути зареєстрований у системі. Для підвищення стійкості алгоритмів ідентифікації рекомендується отримувати зображення під різними кутами огляду, при зміні освітлення та з різними варіаціями міміки, що дозволяє сформувати репрезентативну вибірку.

Після завершення процесу зйомки створюється окрема директорія, якій надається уніфікована назва у форматі "прізвище-ім'я-працівника". Така структура найменування забезпечує систематизацію матеріалів та спрощує подальшу навігацію в наборі даних. До створеної директорії переміщуються всі отримані зображення обличчя, що дає змогу формувати коректний вхідний набір для наступних етапів оброблення.

Далі сформовану директорію необхідно розмістити в системній папці "faces", яка функціонує як централізоване сховище усіх базових наборів зображень персоналу підприємства. Після перенесення даних система отримує можливість виконувати автоматизовану обробку кожного зображення.

На завершальному етапі здійснюється запуск первинного модуля оброблення даних - **collect_data.py**. Даний модуль виконує комплекс функцій: детекцію облич на кожному знімку, вилучення векторизованих ознак (face embeddings), формування унікального ідентифікатора працівника та занесення його до внутрішньої бази даних системи. Таким чином завершується процес первинної реєстрації співробітника, що створює основу для подальших процедур автоматизованої ідентифікації та контролю доступу на підприємстві.

Для оптимальної роботи програмного засобу рекомендується використовувати комп'ютер із такими характеристиками:

1. процесор AMD Ryzen 7 6800H with Radeon, ядер: 8, логічних процесорів: 16;
2. оперативна пам'ять 16,00 ГБ;
3. тип системи 64-розрядна оперативна система;
4. операційна система Windows 11 Pro;
5. 5,53 ГБ оперативна пам'ятка (ОЗУ);
6. відеокарта на 4 ГБ;
7. 26,2 MB вільного дискового простору;
8. монітор з роздільною здатністю 1920 x 1080.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти проведено аналіз потреб компанії в системі відеоспостереження, обрано технічні складові та спроектовано саму систему. Окремою складовою системи є модуль розпізнавання облич.

Об'єкт дослідження – адміністративна будівля, лабораторії та монтажні приміщення компанії НВО «S Beta».

Предмет дослідження – аналіз потреб компанії в системі відеоспостереження та проектування відповідної системи з інтеграцією програмного модуля постобробки відеопотоку.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах штучного інтелекту та нейронних мереж, методах розробки програмного забезпечення.

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

– запропоновано метод розпізнавання облич на основі контрольних маркерів та нейронної мережі;

– спроектовано структуру нейронної мережі для вирішення даної задачі;

– розроблено програмний модуль для інтеграції в систему відеоспостереження, з метою його застосування для пост обробки відеопотоку.

7 МАРКЕТИНГОВЕ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ІТ-ПРОЄКТУ

7.1 Визначення цільової аудиторії кінцевого готового продукту

Результати такого дослідження можуть бути цікавими власникам і керівникам виробничих підприємств, тому що саме вони найбільше відчувають потребу в підвищенні безпеки та скороченні втрат. Для них система відеоспостереження з розпізнаванням облич стає не просто технічним інструментом, а реальним способом контролювати ситуацію на виробництві й запобігати проблемам, які раніше залишалися непомітними.

Служба охорони також отримає значний інтерес до такого рішення, адже воно дозволяє автоматизувати частину їхньої роботи. Завдяки системі їм легше контролювати великі території, стежити за переміщенням працівників та швидше реагувати на інциденти, що робить їхню роботу менш стресовою та ефективнішою.

Інженери з охорони праці знайдуть у цій системі можливість зменшити кількість нещасних випадків, бо вони зможуть точно визначати, хто має доступ до небезпечних зон і чи всі працюють згідно з правилами. Якщо раніше контроль був переважно документальним, то тепер він стає автоматичним і набагато точнішим.

HR-відділу така система теж буде корисною, бо вона допоможе в контролі робочого часу. Розпізнавання облич виключає ситуації, коли хтось може «відмітити» колегу чи маніпулювати системою обліку, що є частою проблемою у великих колективах.

Окрім цього, інтерес може виникнути у страховиків та аудиторських компаній, оскільки наявність системи знижує ризики підприємства. Вони краще розуміють, як зміни у внутрішньому контролі впливають на збитки, і можуть коригувати політики або навіть знижувати страховий тариф.

7.2 Оцінка привабливості шляхом застосування методів експертних оцінок

Щоб оцінити привабливість цього проєкту, я б залучив фахівців із різних сфер — кібербезпеки, відеоспостереження, управління підприємствами та права. Кожен із них дивиться на систему під іншим кутом, і саме такий різнобічний підхід дозволяє отримати більш реалістичну картину. Можна було б організувати анонімне оцінювання, щоб уникнути впливу інших думок.

Експертам запропонував би визначити, наскільки система може знизити збитки, підвищити дисципліну персоналу чи зменшити кількість інцидентів. Вони оцінювали б кожен критерій у числовому форматі, наприклад, за десятибальною шкалою, що дозволяє легко порівнювати результати між собою та між експертами.

Після того як усі оцінки зібрані, можна порахувати середнє значення кожного показника та виявити ключові сильні сторони проєкту. Наприклад, експерти можуть високо оцінити потенційне зменшення крадіжок або зниження витрат на охорону, але нижче — складність впровадження. Це допомагає побачити реальні перспективи.

Окрему увагу варто приділити коментарям експертів, тому що вони можуть вказати на нюанси, які команда розробників могла не врахувати. Наприклад, хтось може застерегти про юридичні обмеження щодо зберігання біометричних даних, і це вплине на бачення системи.

У результаті формується структурований підсумок, на основі якого вже можна обґрунтувати доцільність інвестицій у впровадження проєкту. Така експертна оцінка підвищує довіру до всього дослідження та допомагає знайти оптимальні підходи до реалізації.

7.3 Вибір методу оцінки вартості ПЗ

У випадку впровадження системи відеоспостереження з розпізнаванням облич найдоцільнішим буде витратний метод оцінки. Він дозволяє об’єктивно визначити всі витрати на обладнання, програмне забезпечення, монтаж, навчання персоналу й технічну підтримку. Це важливо, бо проєкт складається з багатьох компонентів і не можна пропустити жоден із них.

Проте я би не відкидав і дохідний підхід. Він дозволяє оцінити, яку фінансову вигоду принесе система підприємству. Наприклад, якщо прогнозоване скорочення крадіжок або зменшення витрат на охорону перевищує витрати на розробку, це дозволяє краще зрозуміти окупність інвестицій. Такий підхід робить оцінку більш гнучкою.

Ринковий підхід теж можна врахувати, але він менш точний, бо системи з розпізнаванням облич можуть сильно відрізнятися за функціональністю та складністю. Однак аналіз конкурентних рішень дозволяє визначити, чи не є проєкт занадто дорогим або, навпаки, недооціненим.

Комбінований підхід був би найефективнішим, тому що він враховує і витрати, і потенційний прибуток. Таке рішення дає повнішу картину й допомагає обґрунтувати інвестиції перед керівництвом.

У підсумку для цього проєкту я б використовував саме витратний метод у поєднанні з прогнозом економічного ефекту — це дозволить отримати реалістичні та переконливі цифри.

7.4 Розрахунок економічної ефективності від впровадження реалізованого ПЗ як фактору його привабливості

На типовому виробничому підприємстві система безпеки здебільшого складається з камер спостереження старого зразка, пунктів охорони, журналів відвідування та фрагментарної IT-інфраструктури. Така модель роботи вже не

відповідає сучасним викликам: дані зберігаються у різних джерелах, розслідування інцидентів займає години або дні, а недисциплінованість персоналу й внутрішні крадіжки залишаються основними причинами фінансових втрат.

Впровадження програмно-апаратного комплексу відеоспостереження з модулем розпізнавання облич дозволяє централізувати контроль за всіма входами, виробничими зонами та складськими приміщеннями. Алгоритми ідентифікації співробітників автоматично фіксують присутність, порушення, спроби доступу до заборонених зон і підозрілу активність. У той же час система зберігає всі записи у єдиному захищеному сховищі та забезпечує можливість миттєвого пошуку кадрів за обличчям.

Таке рішення суттєво зменшує кількість інцидентів, скорочує витрати на охорону та пришвидшує реагування на будь-які відхилення у поведінці персоналу. Воно усуває «людський фактор», який часто стає причиною помилок або навмисних порушень. Окремо важливим є посилення дисципліни працівників, адже прозорість контролю різко знижує запізнення, прогули та небезпечні дії.

Підприємство також отримує перевагу в управлінні ризиками: система вчасно попереджає про спроби доступу до потенційно аварійних зон, запобігаючи дорогим технічним збиткам. Інтеграція з ERP або системою доступу дозволяє автоматизувати контроль відвідуваності й створює єдину аналітичну платформу.

Вхідні дані для розрахунку економічного ефекту зведено у таблиці 7.1.

Таблиця 7.1 – Потенційні економічні вигоди

Показник	До впровадження	Після впровадження	Економічний ефект
Кількість виробничих об’єктів у системі	1	1	—
Середні річні витрати на фізичну охорону підприємства	1 200 000 грн	700 000 грн	–500 000 грн
Кількість інцидентів на рік (крадіжки, проникнення, порушення дисципліни)	45	12	–73 %
Витрати на усунення наслідків інцидентів	900 000 грн	250 000 грн	–650 000 грн
Річні втрати від несанкціонованих доступів і простоїв	600 000 грн	150 000 грн	–450 000 грн
Річне обслуговування IT-системи безпеки	300 000 грн	180 000 грн	–120 000 грн
Початкові інвестиції у впровадження (обладнання, ПЗ, монтаж, навчання)	—	—	1 270 000 грн

Розрахунок економічного ефекту дає наступні результати: поточні витрати системи безпеки без програмно-апаратного комплексу - 3000000 грн/рік, нові витрати після впровадження комплексу - 1280000 грн/рік, річна економія - 1720000 грн/рік , чистий економічний ефект у перший рік - 450000 грн, термін окупності - 0.74 року, окупність – приблизно 9 місяців, рентабельність інвестицій ≈135%

Додаткові нефінансові вигоди: зниження внутрішніх крадіжок і покращення дисципліни — завдяки автоматичному контролю персоналу значно зменшується кількість зловживань, а працівники відчувають більшу відповідальність за свої дії, підвищення рівня безпеки — система блокує доступ до небезпечних зон для осіб без відповідного дозволу, що зменшує ризик аварій та травм на виробництві, покращення якості розслідувань — завдяки розпізнаванню облич та централізованому відеоархіву час аналізу інциденту скорочується з годин до хвилин, прозорість процесів — керівництво отримує аналітику щодо відвідуваності, руху персоналу, пікових навантажень і зон ризику, репутаційний ефект — наявність сучасної системи безпеки підвищує інвестиційну привабливість підприємства та довіру партнерів.

7.5 Пропозиція алгоритму просування проєкту розробки ПЗ

Першим кроком я б створив чітку презентацію, яка демонструє, як працює система, які проблеми вона вирішує та які фінансові вигоди приносить. Людям важливо розуміти не тільки технічну складність, але й реальну користь, тому акцент робив би саме на практичних результатах.

Далі я б визначив ключові підприємства, які можуть бути зацікавлені системою. Це можуть бути виробничі компанії, склади, логістичні центри й навіть торговельні мережі. З ними я б проводив індивідуальні презентації, показуючи демо-систему та реальні кейси.

Паралельно працював би над створенням цифрової присутності - сайт, відеопрезентації, демонстраційні ролики. Це дозволило б залучати компанії, які самі шукають подібні рішення, і формувати довіру до продукту ще до першої зустрічі.

Також було б ефективно брати участь у галузевих виставках та форумах, де можна презентувати систему широкій аудиторії й отримувати нові контакти. Люди охочіше довіряють продуктам, які бачать у дії.

І нарешті, після появи перших успішних впроваджень варто формувати кейси й публікувати їх. Реальні приклади економії та ефективності завжди переконують краще за будь-які презентації.

7.6 Оптимізація каналів збуту та шляхів реалізації ПЗ

Щоб оптимізувати канали збуту, я б почав із розділення потенційних клієнтів на групи: великі підприємства, середні компанії та малі виробництва. Кожна з них має свій бюджет і свої вимоги, тому пропозиції повинні бути адаптованими під кожен сегмент.

Для великих підприємств підходить модель індивідуальних продажів - з виїзними демонстраціями та персональними зустрічами. Це довше, але приносить великі контракти і забезпечує хорошу стабільність.

Для середнього бізнесу краще запропонувати систему підписки - щоб вони могли користуватися технологією без великих початкових інвестицій. Це розширює потенційну аудиторію та робить продукт доступнішим.

Для невеликих компаній важливо мати готові пакети рішень «під ключ». Простота - їхня ключова потреба, тому краще пропонувати легкі в установці та недорогі комплекти.

Важливо також використовувати партнерські продажі, наприклад, через компанії, які займаються встановленням систем безпеки чи автоматизації. Вони вже мають доступ до клієнтів, які готові до технологічних рішень.

Онлайн-канали - сайт, реклама, SEO - забезпечать постійний потік клієнтів, які самі шукають подібні рішення. Це значно здешевлює продажі та дозволяє швидше масштабувати проєкт.

7.7 Визначення ключових факторів успіху конкретного проєкту

Одним із головних факторів успіху є точність і швидкість розпізнавання облич. Якщо система працює без збоїв і не допускає помилок у критичних ситуаціях, вона створює довіру у підприємства та стає незамінним елементом їхньої безпеки.

Не менш важливою є простота інтеграції та налаштування. Якщо система швидко встановлюється й не вимагає значного втручання у вже існуючу інфраструктуру, це значно збільшує шанси на її впровадження.

Ключову роль відіграє і якість технічної підтримки. Клієнти цінують, коли вони можуть легко отримати допомогу у випадку несправностей або питань. Це створює відчуття стабільності й підсилює лояльність до продукту.

Репутація компанії-розробника також визначає успіх. Якщо вона відома професіоналізмом, дотриманням строків та відкритістю до співпраці, клієнти легше приймають рішення щодо інвестицій у систему.

Нарешті, масштабованість проєкту дозволяє охоплювати нові ринки та різні типи підприємств. Чим гнучкіше рішення підлаштовується під вимоги замовників, тим більший потенціал для розвитку й довготривалого успіху воно має.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1. Вступ

Аналізуючи умови працівників ІТ-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 ІТ-індустрії, можна виявити ряд факторів які будуть мати негативний сплив на стан охорони праці, та на самого ІТ-фахівця зокрема. 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 ІТ-фахівця є врахування його психологічних можливостей (швидкість реакції, особливості пам'яті та уваги, емоційний стан тощо). Для того, щоб забезпечити ефективну роботу ІТ-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 ІТ-індустрії. Завданнями для даного розділу є: аналіз умов праці на робочому місці фахівця ІТ-індустрії, розробка конкретних рекомендацій щодо покрашення умов праці фахівців ІТ-індустрії, огляд пожежної безпеки на ІТ-підприємстві та розрахунок системи загального штучного освітлення виробничого приміщення де працюють ІТ - фахівці.

8.2. Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Розглянемо умови праці у приміщенні, в якому працюють програмісти. Геометричні розміри приміщення наведено у таблиці 8.1.

Таблиця 8.1 - Розміри приміщення

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

Таблиця 8.2 - 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. 8.1, та табл. 8.2, 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 року Головного державного санітарного лікаря України робота, що виконується 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 8.3 наведено оптимальні та фактичні значення параметрів мікроклімату як для категорії ваги робіт Іа, так і для розглянутого приміщення. У приміщеннях, де встановлено ЕОМ, рекомендується застосування тільки оптимальних значень показників мікроклімату.

Таблиця 8.3 - 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

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

В літню пору застосовується кондиціонер.

Для боротьби з пилом робляться регулярні провітрювання та вологі прибирання у 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 повинне бути освітлено достатньо рівномірно - це основна гігієнічна вимога. Оскільки яскраве світло на ділянці периферійного 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.

8.3. 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.

8.4. 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].

8.5. Розрахункова частина

Система освітлення робочого місця користувача ПК має відповідати наступним вимогам (рис. 8.1).

Рисунок 8.1 - 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.

К - 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 К = 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:

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

де S - площа приміщення, S = 53,1 м^2;

h - розрахункова висота підвісу, h = 3,2 м. (співпадає з висотою стелі, т.я. 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, знаходимо n = 0,46 (з табличних даних коефіцієнтів використання світлового потоку n світильників з відповідним типом лампам) [8]. Підставимо всі значення у формулу та обчислимо 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 кількість світильників

$$N = 57161,7/ 7200 = 7,9 \text{ шт.}$$

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.

9 ОСНОВНІ ВИСНОВКИ

Система відеоспостереження є невід'ємним елементом системи безпеки будь-якої сучасної організації.

Проектування системи відеоспостереження базується на аудиті інформаційної безпеки компанії. Розміщення камер повинно враховувати покриття зон та присутність камер в важливих, з точки зору інформаційної безпеки, приміщеннях будівлі.

Основну увагу було зосереджено на дослідженні архітектурних особливостей будівлі компанії, для якої проектується системи відеоспостереження. Також розглянуто інформаційні активи компанії, місце розташування та перелік осіб, що мають санкціонований доступ до даної інформації. Отримані в ході аналізу результати складають основу для проектування ефективної системи відеоспостереження.

В окремому розділі проаналізовано типи систем відеоспостереження за критеріями технічної основи реалізації та використовуваних технологій.

У ході роботи над проектом було проведено детальний аналіз предметної галузі. Вивчення існуючих аналогів дозволило нам виявити основні функції та потреби ринку. На основі цього аналізу формуються основні вимоги до системи:

- технічний склад;
- кількість та характеристики камер;
- план розміщення камер та структура мережі;
- функціональні вимоги до системи;
- склад програмного забезпечення та налаштування сервера для накопичення та обробки відео.

Далі було проведено логічний аналіз та вибір відповідних інструментів розробки, так як окремим завданням є реалізація програмного модуля ідентифікації суб'єктів на основі розпізнавання облич. Аналіз задач та

функціональні вимоги до проекту схиляють в бік мови програмування Python. Дана мова має широкий вибір готових компонентів для реалізації нейронних мереж, які вирішено використовувати для реалізації поставленого завдання.

Процес розробки включав не лише технічну частину, а й тестування: після завершення роботи над усіма модулями було проведено комплексне тестування, спрямоване на виявлення як позитивних, так і негативних сторін комп'ютерного застосунку. Усі функції були успішно протестовані та показали хороші результати.

Результати, отримані в ході виконання магістерської роботи, мають конкретне практичне значення. На основі проведеного аналізу та використовуючи отримані результати, можна розгорнути систему відеоспостереження не лише на об’єкті, що безпосередньо аналізувався в роботі, а й на будь-якому іншому об’єкті співрозмірного масштабу, з мінімальними корективами в проекті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Advanced Video-Based Surveillance Systems / Carlo S. Regazzoni, Gianni Fabri, Gianni Vernazza (Eds.). Springer, 2019. SpringerLink

2. A Review of Video Surveillance Systems / Omar Elharrouss, Noor Almaadeed, Somaya Al-Maadeed. Journal of Visual Communication & Image Representation, 2021.

3. A Study on Implementation of Real-Time Intelligent Video Surveillance System Based on Embedded Module / EURASIP Journal on Image and Video Processing, 2021.

4. Caputo A. C. *Digital Video Surveillance and Security*. – 2nd ed. – Amsterdam : Elsevier / Academic Press, 2017. – 460 p.

5. CCTV Surveillance: Video Practices and Technology / Herman Kruegle. Elsevier Butterworth-Heinemann, 2022. openlibrary.org

6. Digital Video Surveillance and Security / Anthony C. Caputo. 2nd Edition, Elsevier/O'Reilly, 2017. oreilly.com

7. *ECR Loss Prevention Report 2023: Video Analytics and Retail Security* [Електронний ресурс]. – Режим доступу: https://www.ecr-shrink-group.com (дата звернення: 24.10.2025).

8. Elharrouss O., Almaadeed N., Al-Maadeed S. A review of video surveillance systems // *Journal of Visual Communication and Image Representation*. – 2021. – Vol. 78. – Art. 103145.

9. Foresti G. L., Mähönen P., Regazzoni C. S. (eds.). *Multimedia Video-Based Surveillance Systems: Requirements, Issues and Solutions*. – Boston : Springer, 2000. – 302 p.

10. IEC 62676 (серія стандартів). *Video Surveillance Systems for Use in Security Applications*. – Geneva : IEC, 2014–2024.

11. *Importance of Video Surveillance in the Manufacturing Industry* // *SSPro Online Journal*, 2024 [Електронний ресурс]. – Режим доступу: https://sspro.com (дата звернення: 24.10.2025).

12. *Intelligent Network Video: Understanding Modern Video Surveillance Systems*. – 2nd ed. – Oxford : Elsevier, 2014. – 424 p.

13. Intelligent Video Surveillance: Systems and Technology / Yunqian Ma, Gang Qian (Eds.). CRC Press, 2010. Routledge

14. Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission, and Analytics / Wei Qi Yan. Springer, 2019. SpringerLink+1

15. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. – Київ: ДП "УкрНДНЦ", 200.335. – 60 с.

16. ISO/IEC 30137-1:2019. *Use of Biometrics in Video Surveillance Systems – Performance Testing and Reporting*. – Geneva : ISO, 2019.

17. Israfilov A., Sitnikov P. R. та ін. Security analysis of urban video surveillance systems: vulnerabilities and protection strategies // *Transportation & Information Technologies in Russia*. – 2024. – Vol. 14, No. 2. – P. 45 – 56.

18. Kruegle H. *CCTV Surveillance: Video Practices and Technology*. – 2nd ed. – Oxford : Butterworth-Heinemann, 2006. – 648 p.

19. Li H., Xiezhang T., Yang C., Deng L., Yi P. Secure video surveillance framework in smart city // *Sensors*. – 2021. – Vol. 21, No. 13. – Art. 4419.

20. Milesight. *Industrial Video Surveillance Solutions* [Електронний ресурс]. – Режим доступу: https://www.milesight.com (дата звернення: 24.10.2025).

21. MindScope. *Як вибрати систему відеоспостереження для підприємства* [Електронний ресурс]. – Режим доступу: https://mindscope.biz.ua (дата звернення: 24.10.2025).

22. Multimedia Video-Based Surveillance Systems: Requirements, Issues and Solutions / Gian Luca Foresti, Petri Mähönen, Carlo S. Regazzoni (Eds.). Springer, 2000. SpringerLink

23. Pelco. *Real-time Video Surveillance Solutions for Manufacturing* [Електронний ресурс]. – Режим доступу: https://www.pelco.com (дата звернення: 24.10.2025).

24. Regazzoni C. S., Foresti G. L., Vernazza G. (eds.). *Advanced Video-Based Surveillance Systems*. – Boston : Springer, 1999. – 250 p.

25. Remagnino P., Jones G. A., Paragios N., Regazzoni C. S. (eds.). *Video-Based Surveillance Systems: Computer Vision and Distributed Processing*. – Boston : Springer, 2002. – 332 p.

26. Sánchez J., Benet G., Simó J. E. Video sensor architecture for surveillance applications // *Sensors*. – 2012. – Vol. 12, No. 2. – P. 1509 – 1528.

27. SDM Magazine. *State of the Market: Video Surveillance 2024* [Електронний ресурс]. – Режим доступу: https://www.sdmmag.com (дата звернення: 24.10.2025).

28. Secure Video Surveillance Framework in Smart City / Hao Li, Tianhao Xiezhang, Cheng Yang, Lianbing Deng, Peng Yi. Sensors, 2021. MDPI

29. Security Analysis of Urban Video Surveillance Systems: Vulnerabilities and Protection Strategies / A. Israfilov, P.R. Sitnikov et al. Transportation & Information Technologies in Russia, Vol.14 No.2 (2024). RCSI Journals Platform

30. Shidik G. F., Noersasongko E., Nugraha A., Andono P. N., Kusuma E. J. A systematic review of intelligent video surveillance: trends, techniques, frameworks, and datasets // *IEEE Access*. – 2019. – Vol. 7. – P. 170 – 198.

31. Video Sensor Architecture for Surveillance Applications / Jordi Sánchez, Ginés Benet, José E. Simó. Sensors, 2012. MDPI

32. *Video Surveillance Techniques and Technologies*. – Hershey, PA : IGI Global, 2013. – 370 p.

33. Video-Based Surveillance Systems: Computer Vision and Distributed Processing / Paolo Remagnino, Graeme A. Jones, Nikos Paragios, Carlo S. Regazzoni (Eds.). Springer, 2002. SpringerLink

34. Yan W. Q. *Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission, and Analytics*. – Cham : Springer, 2019. – 382 p.

35. *Використання систем відеоспостереження на промислових підприємствах України* // *Таврійський науковий вісник*. – 2024. – Вип. 15. – С. 98 – 104.

36. ДСТУ EN IEC 62676-4:2017. *Системи відеоспостереження. Частина 4. Правила застосування (EN IEC 62676-4:2015, IDT)*. – Київ : ДП «УкрНДНЦ», 2017. – 49 с.

37. ДСТУ EN IEC 62676-5:2019. *Системи відеоспостереження. Частина 5. Характеристики даних та якості зображення камер (EN IEC 62676-5:2018, IDT)*. – Київ : ДП «УкрНДНЦ», 2019. – 72 с.

38. Скачек Л. М. ЦІННІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ [Текст] / Л. М. Скачек. // Інформаційна безпека. – 200.333. – №0.33(9). – С. 0.3352–0.3354.

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

40. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T),* Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.

41. 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.

42. 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.

43. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358.

44. 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.

45. 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.

46. Smirnov A.A., Kuzne tsov 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.

47. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління,* № 2(70). 2022. С. 28-37.

48. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

49. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Конопліцька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. Кібербезпека: освіта, наука, техніка. – Том 3 № 3. – Київ: КУ ім. Бориса Грінченка. – 2019. – С. 63-87.

50. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

51. Смірнов О.А., Смірнов С.А., Дідик А.К. Метод безпечної маршрутизації метаданих у хмарні антивірусні системи. Системи озброєння та військова техніка. – Випуск 2 (46) – Х.: ХУПС – 2016. – С. 146-149.

52. Державні будівельні норми України: ДБН В.2.5-28:2018. - Режим доступу до ресурсу: https://goo.su/9AkQ

53. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин: ДСанПІН 3.3.2-007-98. - Режим доступу до ресурсу: https://zakon.rada.gov.ua/rada/show/v0007282-98

54. Закон України «Про охорону праці» від 14.10.1992 р. № 2694-XII. - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2694-12 (дата звернення 19.10.22).

55. Зеркалов Д. В. Охорона праці в галузі: Загальні вимоги: навч. посіб. Київ: Основа. 2011. 551 с.

56. Наказ Міністерства соціальної політики України 14.02.2018 № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0508

57. Постанова № 42 від 01.12.1999 Головного державного санітарного лікаря України «Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99. - Режим доступу до ресурсу: https://zakon.rada.gov.ua/rada/show/va042282-99

58. Оришака, О. В. Основи охорони праці: навч. посіб. / О. В. Оришака, Г. П. Горбачова, К. М. Марченко; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. - Кропивницький : ЦНТУ, 2022. - 175 с. – Режим доступу до ресурсу: http://dspace.kntu.kr.ua/jspui/handle/123456789/12161

59. Оришака О.В. Охорона праці в галузі та цивільний захист / О.В Оришака, Г.П. Горбачова, О.М. Мезенцева , К.М. Марченко, К.О. Буравченко; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. - Кропивницький: Видавець Лисенко В.Ф., 2019. − 226 с. – Режим доступу до ресурсу: http://dspace.kntu.kr.ua/jspui/handle/123456789/9258

60. Методичні рекомендації до виконання розділу "Заходи з охорони праці та техніки безпеки" випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти для здобувачів вищої освіти спеціальностей 123 "Комп'ютерна інженерія" та 122 "Комп'ютерні науки" / М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т, каф. кібербезпеки та програм. забезпечення; [укл. О.В. Оришака, К.М. Марченко]. - Кропивницький: ЦНТУ, 2022. - 19 с. [Електронний ресурс]. – Режим доступу: http://dspace.kntu.kr.ua/jspui/handle/123456789/12240

61. Розрахунки з електробезпеки. Розрахунок захисного заземлення. Режим доступу: https://cpo.stu.cn.ua/Oksana/rozrah_rozd_OP_DP_bak_spec_mag