

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)

Кафедра автоматики та телекомунікацій
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри автоматики та
телекомунікацій

_____ Іван ЛАКТИОНОВ
(підпис) (ім'я та прізвище)

«___» _____ 2022 р.

Випускна кваліфікаційна робота

_____ бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Розробка телекомунікаційної мережі офісної будівлі з інтеграцією
системи IP-відеоспостереження»

Виконав студент 4 курсу, групи ТКР-18 /
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

_____ Голдін Олексій Миколайович
(Прізвище, Ім'я та По-батькові) (підпис)

Керівник ст. викл. каф АТ _____ Гліб СТУПАК
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Рецензент зав. каф. ЕТ, д.т.н., проф. _____ Олександр ВОВНА
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Нормоконтроль:

_____ ас. Дар'я ЖУКОВСЬКА
(підпис)

*Засвідчую, що у цій дипломній
роботі немає запозичень з праць
інших авторів без відповідних
посилань.*

Студент _____
(підпис)

Луцьк – 2022 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)

Кафедра автоматики та телекомунікацій
(повна назва кафедри)

Захист відбувся _____
(дата)

з оцінкою _____

Секретар ЕК _____
(підпис)

Випускна кваліфікаційна робота бакалавра

Тема: «Розробка телекомунікаційної мережі офісної будівлі з інтеграцією системи IP-відеоспостереження»

Спецчастина: _____

Виконавець, студент

гр. ТКР-18

Олексій ГОЛДІН

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Керівник

Гліб СТУПАК

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Консультанти:

Іван ЛАКТИОНОВ

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Гліб СТУПАК

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Валерій ПОЦЕПАЄВ

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Нормоконтроль

Дар'я ЖУКОВСЬКА

(підпис, дата, Ім'я ПРІЗВИЩЕ)

**Державний вищий навчальний заклад
"Донецький національний технічний університет"**

Інститут, факультет Комп'ютерно-інформаційних технологій та автоматизації
Кафедра Автоматика та телекомунікації
Освітньо-кваліфікаційний рівень бакалавр
Галузі знань 17 Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри АТ
Іван ЛАКТИОНОВ

« » 2022 року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Голдін Олексій Миколайович

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розробка телекомунікаційної мережі офісної будівлі з інтеграцією системи IP-відеоспостереження

керівник проекту (роботи) Ступак Гліб Володимирович, ст. викл. каф. АТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від 06.05.2022 року № 180

2. Строк подання студентом проекту (роботи)_____

3. Вихідні дані до проекту (роботи)_____

_____Технічна документація та матеріали з переддипломної практики, схема

_____об'єкту, матеріали курсового проектування

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

- 1) Аналітичний огляд систем відеоспостереження
- 2) Аналітична частина
- 3) Апаратний синтез
- 4) Охорона праці

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
План об'єкта, зони відеоспостереження, структурна схема

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	ст. викл. каф. АТ Ступак Г.В.		
2	зав. каф. АТ, д.т.н., доц. Лактіонов І.С.		
3	к.т.н., доц. каф. АТ, доц. Поцєпаєв В.В.		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналітичний огляд систем відеоспостереження	25.04.2022	
2	Аналітична частина	07.05.2022	
3	Апаратний синтез	22.05.2022	
4	Додаток А – Охорона праці та безпека під час надзвичайних ситуацій на підприємстві	31.05.2022	
5	Оформлення	05.06.2022	

Студент

(підпис)

Олексій ГОЛДІН

(прізвище та ініціали)

Керівник роботи

(підпис)

Гліб СТУПАК

(прізвище та ініціали)

ЛИСТ ЗАУВАЖЕНЬ

Посада, Ім'я та ПРІЗВИЩЕ	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Голдін О.М. Розробка телекомунікаційної мережі офісної будівлі з інтеграцією системи IP-відеоспостереження / Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» зі спеціальності 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Покровськ, 2022.

Пояснювальна записка: 65 стор., 19 рис., 3 табл., 13 посилання.

У випускній кваліфікаційній роботі розроблена система відеоспостереження для офісної будівлі. Були сформульовані задачі для охоронної системи та визначенні вимоги до системи відеоспостереження. Виконано аналіз систем відеоспостереження. Вибрано оптимальний варіант побудови системи. Виконані розрахунок характеристик та вибір відповідного обладнання. Розроблено схему локальної мережі.

Ключові слова: ВІДЕОСПОСТЕРЕЖЕННЯ, КАМЕРА, ОБ'ЄКТИВ, ЗОНА ОГЛЯДУ, РОЗШИРЕННЯ, ІДЕНТИФІКАЦІЯ, МОДЕЛЮВАННЯ.

ЗМІСТ

ВСТУП.....	9
1 АНАЛІТИЧНИЙ ОГЛЯД СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ.....	11
1.1 Експлуатаційні вимоги до системи відеоспостереження.....	11
1.2 Стандарти відеонагляду.....	15
1.2.1 Стандартного розширення (PAL, NTSC).....	16
1.2.2 Аналогові стандарти високої чіткості AHD, HDCVI, TVI.....	17
1.2.3 Пакетна передача стислих кодованих даних	19
1.3 Кодеки відеонагляду.....	20
Висновки до розділу 1.....	22
2 АНАЛІТИЧНА ЧАСТИНА.....	23
2.1 Аналіз офісної будівлі	23
2.2 Зона огляду відеокамери.	24
2.3 Підбір об'єктива та матриці камери	27
2.4 Розрахунок кута обзору об'єктива	27
2.5 Необхідна роздільна здатність	28
2.6 Зона впевненого розпізнавання людини.....	29
2.7 Локальна мережа	34
2.8 Розрахунок трафіку.....	36
2.9 Вибір мережевих інтерфейсів	33
2.10 Вибір комутаторів.....	38
2.11 Розрахунок об'єму архіву запису	41
2.12 Відео-сервер та відеореєстратор	43
2.13 Програмне забезпечення для систем відеоспостереження.....	44
Висновки до розділу 2.....	45
3 АПАРАТНИЙ СИНТЕЗ.....	46
3.1 Вибір відеокамер.....	46

3.2 Розрахунок дискового простору для зберігання відеозаписів та вибір відеореєстратора.....	48
Висновки до розділу 3.....	52
ВИСНОВКИ.....	53
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	54
ДОДАТОК А – Охорона праці, безпека в надзвичайних ситуаціях.....	56

ВСТУП

Дипломний проект присвячений актуальній задачі – в ньому проводиться розробка системи відеонагляду для офісної будівлі парк Авеню в місті Київ.

Мережа, що розробляється в дипломному проекті надавати наступні послуги:

- Відеоспостереження;
- Контроль поведінки людей усередині будівлі;
- Корегування дій персоналу;
- Розслідування різноманітних інцидентів;
- Аналіз дій персоналу після інциденту (навчання персоналу при аналізі інциденту);
- Охорона об'єкту;

Для реалізації поставленої мети необхідно:

- Проаналізувати різні технології відеоспостереження та виявити їх переваги та недоліки;
- Здійснити обґрунтований вибір технології відеоспостереження, на якій будуватиметься майбутня система;
- Спроекувати систему відеоспостереження;
- Провести розрахунок основних характеристик обладнання та здійснити обґрунтований вибір.
- Провести комплекс заходів техніки безпеки та охорони праці .

Мета – підвищити привабливість для орендаторів через розробку мережі відеоспостереження.

Актуальність роботи полягає в потребі створення сучасної системи відеоспостереження для залучення нових орендаторів та підвищення рівня безпеки в бізнес-центрі.

Предмет – бізнес-центр «парк Авеню».

Об'єкт – Система відеонагляду.

Задачі:

- аналіз об'єкту проектування;
- аналітичне проектування;
- апаратний синтез;
- охорона праці.

Результатом дипломного проекту є пояснювальна записка, що містить проектні рішення, їх обґрунтування та опис. За схемами, що запропоновані в роботі та відповідним описом в подальшому можна розробити повноцінний комплект технічної документації для побудови та налаштування мережі в бізнес-центрі.

Методи дослідження – аналітичні методи, імітаційне моделювання.

Структура та обсяг роботи – 65 сторінки, 3 таблиць, 19 рисунків, 13 використаних джерел.

1 АНАЛІТИЧНИЙ ОГЛЯД СИСТЕМ ВІДЕОПОСТЕРЕЖЕННЯ

1.1 Експлуатаційні вимоги до системи відеоспостереження.

Планування системи відеонагляду має включати три ключові етапи показані на малюнку 1.1.

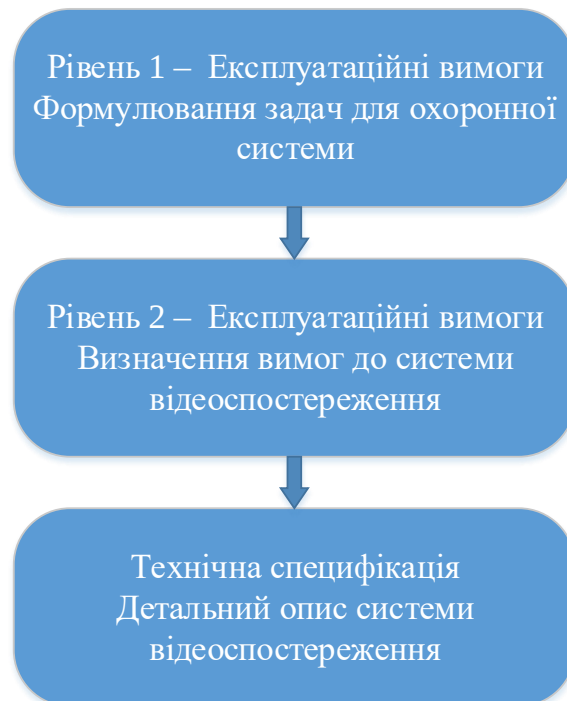


Рисунок.1.1 – Ключові етапи проектування системи відеоспостереження

Перший крок полягає у визначенні проблеми – це може бути безпосередня загроза безпеці об'єкта, якийсь із аспектів громадської безпеки або будь-яка інша вразливість. Зазвичай сформульовану проблему визначають як експлуатаційна вимога першого рівня. На цьому етапі необхідно з'ясувати, чи є установка системи відеонагляду найбільш підходящим вирішенням даної проблеми або існують інші, раціональніші шляхи її усунення.

Описуючи ясну картину всіх речей, що стосуються вирішення проблеми, варто звернути увагу на спеціалізовані аспекти, що стосуються виключно відеоспостереження. Вони становлять другий рівень експлуатаційних вимог.

Надалі їх опис допоможе кінцевому користувачеві розмежувати зони відповідальності співробітників, зрозуміти всі сторони процесу експлуатації системи, адекватно реагувати на ситуації, скласти найоптимальнішу конфігурацію системи відеоспостереження та приймати вірні управлінські рішення.

Третій етап – розробка більш детальної технічної специфікації системи відеоспостереження. Наприклад, сюди входить прийняття рішень про моделі камер, використовуваний алгоритм стиснення та розподіл обсягу жорстких дисків для зберігання відзнятого матеріалу.

Перед тим як зосередитися безпосередньо на системі відеоспостереження, корисно трохи замислитися над природою проблеми чи загрози, яку планується усунути за допомогою впровадження системи. Це осмислення вимог до безпеки об'єкта високому рівні абстракції і називається у документі упорядкуванням експлуатаційних вимог першого рівня. Простий алгоритм їх формулювання показаний на малюнку 1.2, і він повинен супроводжуватися складанням деяких записів, що пояснюють.

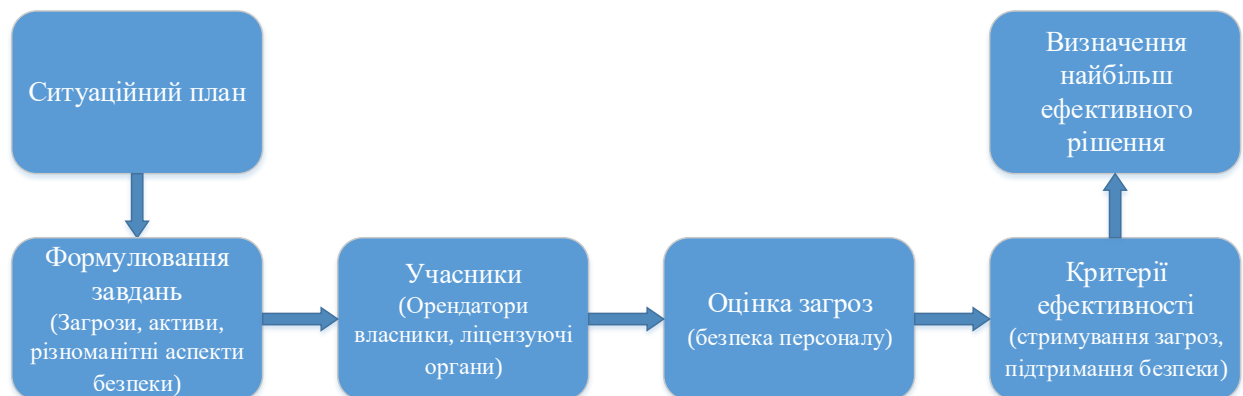
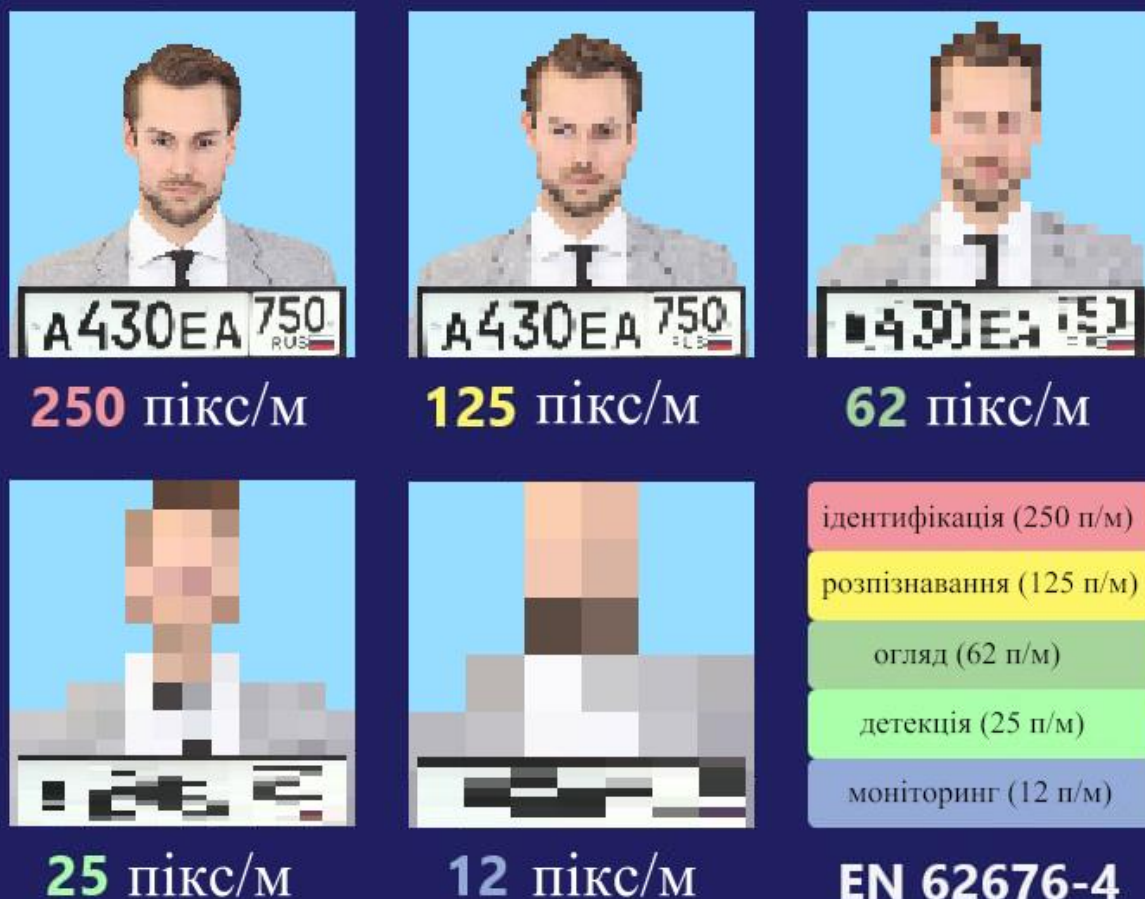


Рисунок 1.2 – Складання переліку експлуатаційних вимог

Першочергове завдання щодо експлуатаційних вимог складання графічної схеми місця передбачуваного впровадження системи та виділення у ній зон, де потенційно можуть виникнути проблеми у сфері безпеки.

Щільність пікселів для різних цілей відеоспостереження



© ⓘ Ⓜ пікс/м - пікселів на метр

Рисунок 1.4 – Щільність пікселів для різних цілей відеоспостереження.

Моніторинг і контроль: фігура займає як мінімум 12 п/м, а сцена, що відображається, при цьому не перевантажується об'єктами. За такого рівня деталізації оператор зможе ознайомитися з кількістю, напрямом і швидкістю руху людей.

Детектування: фігура займає щонайменше 25 п/м. Після повідомлення оператор зможе, перемикаючись між камерами стеження, встановити, чи є людина в тому чи іншому місці.

Огляд: фігура повинна зайняти 62 п/м. При такому масштабі можуть бути видні характерні ознаки тієї чи іншої людини, наприклад, одяг. У той же час, поле огляду камери залишається досить широким для спостереження за ситуацією в цілому і виявлення інцидентів.

Розпізнавання: у разі фігура займає щонайменше 125 п/м. При цьому оператор з великою ймовірністю може сказати, чи бачив чи ні він цього чоловіка раніше.

Ідентифікація: якщо людська фігура займає щонайменше 250 п/м якість зображення та рівень деталей дозволить ідентифікувати особистість із зневажливо малою ймовірністю помилки.

1.2 Стандарти відеонагляду

Існує 2 стандарта сигналу CCTV :

Аналоговий :

- Стандартного розширення (PAL, NTSC)
- Високої чіткості (AHD, TVI, CVI)

Цифровий :

- Пакетна передача стиснутих кодованих даних (IP)
- Поточкова передача не стиснутих некодованих цифрових

відеосигналів (SDI)

Вибір того чи іншого стандарту відеоспостереження залежить від умов в яких буде побудована система відеоспостереження необхідно детально розглянути кожен стандарт відеонагляду щоб адекватно підібрати необхідне обладнання.

1.2.1 Стандартного розширення (PAL, NTSC).

Обидва стандарти прийшли в галузь відеонагляду с телебачення фактично в незмінному вигляді і мають багато недоліків :

Розширення картинки принципово обмежено и погано відповідає сучасним представленням о деталізації 704 на 576 точок при 25 к/с в PAL та 704 на 480 при 30 к/с в NTSC, в деяких випадках при використанні іншого процесора деталізація може бути збільшена 960 на 526 при 25 к/с в PAL та 960 на 480 при 30 к/с в NTSC.

Дані системи мають наступні переваги :

- низький рівень перехресних спотворень сигналів яскравості та кольоровості та висока помігозахищеність
- Якісне розділення сигналів яскравості та кольоровості.
- Простий запуск та обслуговування обладнання.
- Принципова відсутність затримок сигнала при перегляді живого відео локально.
- Теоретична можливість використовувати інфраструктуру систем колективного прийому телебачення при використовуванні телевізійного модуля. Тобто в колективну антену можна «підмішувати» сигнал PAL, NTSC та дивитися зображення з камер просто переключив на необхідний номер каналу.

Основним недоліком даної даної системи є її застарілість, а саме дуже погана якість зображення яка майже не дозволяє виконувати поставленні задачі.

У теперішній час PAL, NTSC майже не використовуються в системах сучасного відеонагляду так як недоліки суттєво переважають переваги, однак на ринку є багато застарілого та дешевого обладнання на базі якого можна побудувати хоч и обмежену, але дуже дешеву систему, тож для певних цілей дану технологію можливо використовувати і зараз наприклад в дешевих відеодомофонах або у приватному будинку.

1.2.2 Аналогові стандарти високої чіткості AHD, HDCVI, TVI.

Ці стандарти з'явилися у проміжок часу коли стандарти на основі IP технологій стали більш доступними та цікавими за технічними характеристиками, вирішувались проблеми з сумісністю обладнання та затримкою передачі сигналу тобто ір відеоспостереження ставало більш привабливим для практичного використання, а аналогові телевізійні стандарти вже вкрай застаріли. Єдиний перехід на IP відеонагляд був утруднений із за принципу передачі пакетів так і наявністю великої кількості об'єктів де була розгорнута кабельна інфраструктура на основі 75 Ом коаксіального кабелю. Отже заміна системи на більш сучасну IP систему означало для власника повну втрату всіх вкладів у систему безпеки. Потрібно було витратити кошти на закупку та монтаж нового обладнання, демонтаж старого та роботи на прокладання локально обчислювальної мережі для IP систем.

Компанія Dahua technology першою розробила стандарт HDCVI, стандарт високої якості заснований на коаксіальному кабелі. Сигнал передається при допомозі технології квадратурно-амплітудної модуляції тобто повністю розділяє сигнали яскравості та кольоровості що значною мірою усуває перехресні завади композитного сигналу та використовує функцію автоматичної корекції сигналу що зменшує спотворення первинного сигналу при передачі на великі відстані. Також підвищена частота модуляції до 44 МГц в порівнянні з 6 МГц стандарту PAL/NTSC.

HDTVІ розроблений компанією Hi sharp на відміну від стандартів PAL/NTSC використовується змінена технологія формування та передачі відео сигналу. Стандарт використовує повне розділення сигналів яскравості та кольоровості що дозволяє повністю уникнути накоплення завад для отримання більш чіткого зображення. Реалізований алгоритм попередньої обробки відеосигналу з подальшим використанням квадратурно-амплітудної модуляції для передачі по лініям зв'язку частота модуляції сигналу до 55МГц.

Недоліки стандартів високої якості.

По перше якість зображення залежить від відстані між камерою та відеореєстратором, відношення сигнал шум з кожним метром може лише зменшуватись тому й сигнал з кожним метром буде погіршуватись і не може бути відновлений до первозданного рівня.

Зі збільшенням довжини лінії відбувається збільшення рівня завад у коаксіальному кабелі у діапазоні 5-10 МГц із-за цього може скластися враження що найбільш вразливим буде стандарт АHD, але на практиці погіршення зображення аж до втрати кольоровості та появи завад відбувається у всіх HD стандартах, особливо сильно завади впливають на сигнал високого зображення 1080p і вище. Незважаючи на відмінності стандартів в частотній модуляції вони всі мають схожу завадостійкість і не можна сказати що один стандарт принципово переважає за якістю зображення інші.

Обладнання стандартів високої якості має обмежені можливості у резервуванні обладнання, по побудові відмовостійких систем.

Малий функціонал в порівнянні з IP камерами (функції відеоаналітики).

Переваги стандартів високої якості:

- можливість передавати по коаксіальному кабелю не тільки відеосигнал, а також живлення та сигнали управління поворотної камери.

- точна передача кольоровості.

- можливість використання існуючої коаксіальної інфраструктури.

- дальність передачі інформації від відеокамери до реєстратора досягає 600 метрів.

- гібридність відеореєстраторів, підтримка всіх аналогових стандартів та мають можливість підключення IP відеокамер.

Область застосування:

- невеликі системи без суттєвих потреб у відеоаналітиці .

- модернізація старих аналогових систем.

- великі відстані від реєстратора до камер.

1.2.3 Пакетна передача стислих кодованих даних (IP відеоспостереження)

На сьогодні IP відеонагляд це головний потік у розвитку систем відеоспостереження, бо IP відеоспостереження став одною з ІТ систем та розвивається неймовірними темпами, з'являються нові технології та нові можливості в тому числі по передачі, обробці даних та способу зберігання даних.

Мережеві пристрої відеоспостереження, що підтримують відкриті стандарти, можна легко інтегрувати майже в будь яку мережу. Крім того, відеосигнал з мережевих відеокамер може передаватися в інші системи безпеки, наприклад, систему охорони, систему контролю та управління доступом, POS-систему магазину.

Можна різними способами забезпечити безпеку мережевих пристроїв відеоспостереження і переданих відеопотоків. Зокрема, можна використовувати захист у вигляді імені користувача та пароля, списку дозволених мережних адрес, автентифікації за IEEE 802.1X та шифрування даних за HTTPS (SSL/TLS) або VPN. Аналогові відеокамери не передбачають можливості шифрування даних, що передаються, або використання імені користувача і пароля. Будь-який може приєднатися до лінії передачі відеосигналу або підмінити відеосигнал з аналогової відеокамери на інший відеосигнал.

Основним недоліком IP відеонагляду є саме пакетна передача даних, потоковий тип даних з відеокамери з деякими проблемами поєднується з принципом передачі даних пакетами.

І хоча дані проблеми частково вирішуються завдяки різноманітним стандартам стиснення для більш якісної роботи системи необхідно вводити даний трафік у VLAN, використовувати QOS, тобто маркувати трафік щоб призначити йому найбільший пріоритет.

1.3 Кодеки відеонагляду

MJPEG (Motion JPEG) - даний кодек використовує покадрову компресію. Головною перевагою даного кодека вважається простота алгоритму стиснення, що не вимагає високопродуктивного процесора.

Основним недоліком є високі вимоги до розмірів дискового простору для збереження інформації. Крім того, при реалізації можливості віддаленого доступу до відеоданих за допомогою Інтернет використання кодека MJPEG характеризується не раціональним використанням пропускного каналу зв'язку, так як при стисненні окремих кадрів не враховуються зміни в послідовності кадрів, що призводить до відправки зайвої (однаковою) інформації. Таким чином, кодек MJPEG залишається актуальний для бюджетних варіантів систем відеоспостереження, так як не пред'являє високих вимог до технічних характеристик комп'ютеризованої частини, однак для багатофункціональних систем моніторингу та камер з великою роздільною здатністю його використання є не раціональним.

H.264 - стандарт стиснення відеоданих, прийнятий Міжнародною організацією зі стандартизації (ISO). Головною відмінністю є те, що він не відправляє зайвої інформації. Він не відправляє як MJPEG ціле зображення, а відправляє тільки оновлення, тобто те, що змінилося в «основному» кадрі, це дозволяє домогтися значної економії дискового простору і зниження навантаження на смугу пропускання. У порівнянні з MJPEG при ідентичних показниках якості зображення кодек H.264 здатний зменшити розмір відео файлу більш ніж на 80 відсотків. Незважаючи на значну економію дискового простору та трафіку, в сучасних умовах при передачі такого відео вже виникає істотна проблема – а саме, нестача пропускної спроможності існуючих каналів зв'язку,

Сучасна IP камера з роздільною здатністю 4М при використанні кодека H.264 здатна передавати якісне 25 кадрів /с відео з бітрейтом близько 20-35 Мбіт/с. Звичайно, при порівнянні зі MJPEG-кодуванням, яке при аналогічному

дозволі транслює по мережі не відео, а слайд-шоу з частотою 1-4 кадрів/с – це чудовий результат. Домогтися від MJPEG адекватної передачі; живого відео з більш високою частотою кадрів рівня 25 кадрів /с і вище часто неможливо, адже в такому випадку відеопотік з камери в кілька разів перевищить пропускну здатність 100 Мбіт Ethernet мережі, і данні просто фізично не можуть бути передані по існуючій у багатьох місцях кабельній інфраструктурі. Однак пара-трійка IP камер високого дозволу навіть при використанні кодека H.264 здатні повністю поглинути пропускну здатність 100 Мбіт/с каналу. Проблема кодека H.264 якраз полягає в тому, що для відео надвисоких дозволів цей кодек вже не може забезпечити достатній ступінь стиснення, яка зберігала б прийнятною навантаження на канал передачі.

Стандарт компресії H.265, він же HEVC (High-Efficiency Video Coding) відеокодек, розроблений спільно Міжнародним союзом електрозв'язку ITU-T і ISO /IEC. Цей стандарт є логічним продовженням H.264. У той же час він характеризується використанням більш ресурсоемних, але зате і набагато більш ефективних алгоритмів стиснення. Кодек H.265 був розроблений, в тому числі, і з метою економного використання пропускну здатності каналів зв'язку. Використовуючи кодек H.265, в залежності від обраного режиму якості, вдається зменшити розмір переданих відеоданих і відповідно файлів, що зберігаються на 40-60% в порівнянні з кодеком H.264, за порівнянної якості зображення. Це дає можливість пропорційно знизити навантаження на мережу або ж встановити ще більш прогресивні засоби відеоспостереження при збереженні завантаженості мережі – адже стандарт H.265 передбачає роботу з відео дуже високих дозволів, аж до 8K (33,2 мегапікселя для формату 16: 9). Для потокової передачі 4K-відео, стисненого кодеком H.265, цілком достатньо пропускну здатності мережі на рівні 15-30 Мбіт /с. Це практично відповідає відеопотоку з роздільною здатністю 4М при використанні кодека H.264.

Таким чином, завдяки появі H.265 зникає важливий стримуючий фактор розвитку IP камер надвисоких дозволів, але стандарт H.265 пред'являє досить високі вимоги до обчислювальної потужності процесорів кодування і

декодування сигналу. Декодування відео H.265 вимагає до 10 разів більше ресурсів процесора, ніж декодуючи відео H.264 що означає значне збільшення вартості обладнання.

Висновки до розділу 1

В даному розділі були розглянуті теоретичні дані про основні моменти проектування відеоспостереження. Розглянуті ключові етапи проектування системи відеоспостереження, проаналізовані стандарти відеоспостереження та їх технічні особливості.

2 АНАЛІТИЧНА ЧАСТИНА

2.1 Аналіз офісної будівлі

Умовно весь ринок відеонагляду можна розділити на так звані вертикальні ринки замовники яких мають багато спільних та повторюваних проектних вимог (безпека, надійність, топологія мережі тощо).

Офісна будівля парк Авеню в місті Київ для якої розробляється мережа найбільш підходить до вертикального ринку SOHO (small office home office).

Основні задачі це:

- Моніторинг локацій для розслідування інцидентів що відбулися.
- Використання у маркетингових цілях покращення прозорості роботи (публічні трансляції на сайті компанії або доступ для окремих клієнтів).
- Віддалений контроль роботи працівників
- Ідентифікація клієнтів та робітників.
- Верифікація подій
- Наявність віддаленого онлайн трансляції архіва через мобільний додаток та веб-браузер.

Перш за все необхідно описати зони відеоспостереження в будівлі в залежності з тими задачами що поставив замовник.

Офіс можна розділити на декілька зон:

- прохідний пункт
- робоча зона
- склад/ серверна
- зона відпочинку

Для кожної з цих зон необхідно визначити задачі які буде виконувати система відеоспостереження.

Для робочої зони основною задачею є моніторинг процесів або локацій. А саме дотримання трудової дисципліни, стандартів обслуговування клієнтів або

за правилами приймання товару. Також можливо використовувати це як маркетинговий інструмент підвищення довіри споживача через трансляцію на різноманітні веб ресурси.

Розслідування інцидентів: збір доказової бази о протиправних діях зловмисників, клієнтів або персоналу для передачі правоохоронним органам і використання у судовому розгляді.

Створення чорних списків клієнтів.

Аналіз дій персоналу після інциденту (навчання персоналу при аналізі інциденту).

Підготовка відео-кейсів для корпоративних тренінгів, корегування дій персоналу, для навчання нових співробітників чи зміна регламенту обслуговування клієнтів.

Верифікація подій, підтвердження спрацювання охоронних чи пожежних систем .

Для прохідного пункту основною задачею є :

Верифікація подій. Підтвердження проходу співробітника через систему управлінням доступу (проходження через турнікет). Автоматичний підрахунок відвідувачів . Ідентифікація людини та надання прав доступу.

Для прохідного пункту основною задачею є моніторинг процесів або локацій та розслідування інцидентів.

Для складу це виявлення та ідентифікація (запис за датчиком руху).

2.2 Зона огляду відеокамери

Зона огляду це тривимірна геометрична фігура у формі піраміди з вершиною що виходить з об'єктива відеокамери, усі предмети або їх частини що потраплять в межі цієї піраміди будуть зображені на екрані монітора, але тільки якщо предмети не затіняються іншими предметами.

Значно зручніше проектувати не у тривимірному просторі а у звичному

для людини двовимірному просторі при вигляді зверху це значно швидше та зручніше тому необхідно цю тривимірну зону огляду у вигляді деякої двовимірної фігури, тобто зробити горизонтальну проекцію зони огляду на план місцевості, при цьому частіше за все нас цікавить не вся зона огляду, а тільки її частина в певному діапазоні висот.

Якщо задача полягає в тому щоб виявити появу людини то очевидно що зріст людини обмежен як зверху так і знизу, отже важливі наступні параметри огляду.

- висота нижньої границі зони огляду
- висота верхньої границі зони огляду
- відстань до верхньої границі зони огляду.

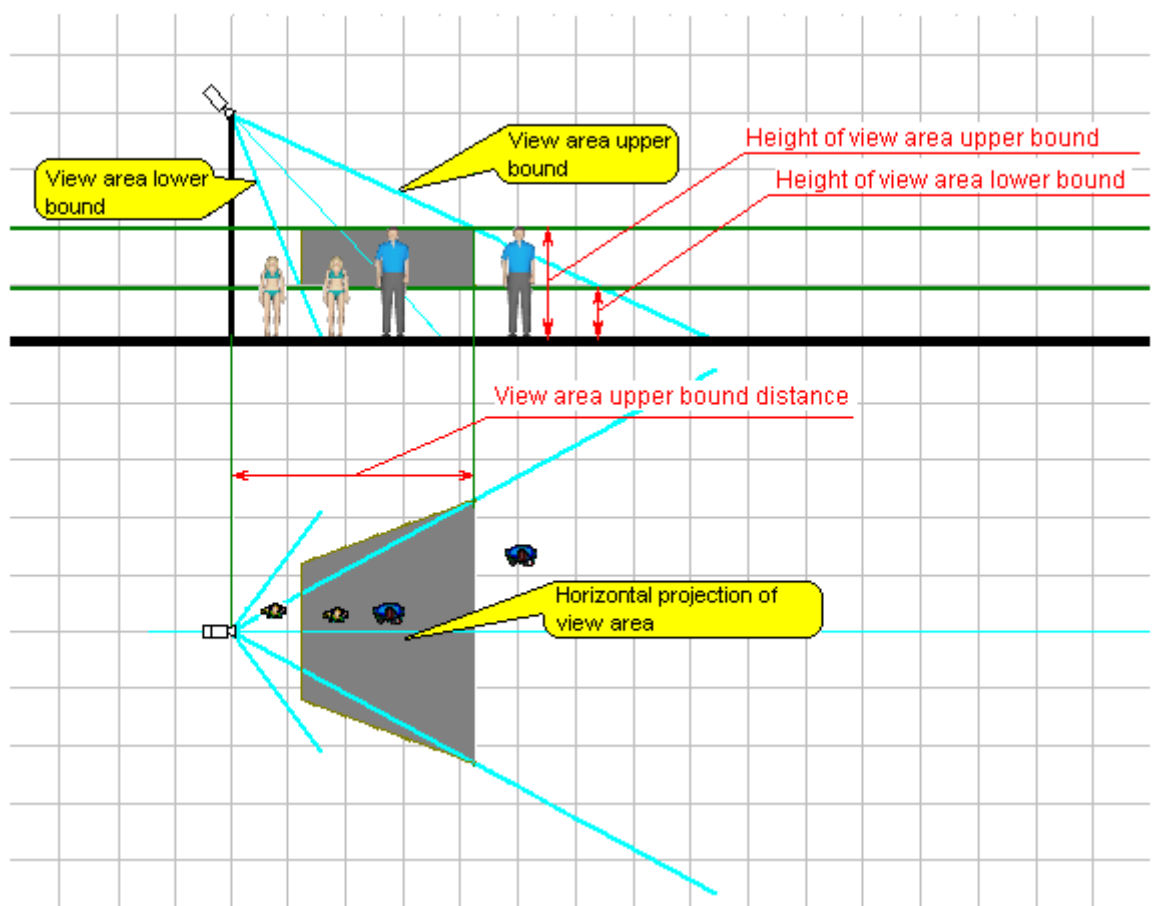


Рисунок.2.2 – Проекції області огляду камери.

На рис. 2.2 ми бачимо значення наступних параметрів: верхня межа

висоти області огляду та нижня межа висоти області огляду. Змінюючи значення цих висот, ми отримаємо різні розміри проекції, і будь-який об'єкт, який знаходиться на висоті між цими межами і на горизонтальній площині в межах горизонтальної проекції області огляду, буде видно на екрані, коли він не затінений іншими об'єктами на сцені.

Наприклад, якщо нас цікавить спостереження за людьми, які не намагаються сховатися від спостереження, достатньо встановити 1 м нижньої межі області огляду та 2 м висоти області огляду зверху. Якщо можливо що людина проповзе через перетин контрольованої зони, то нижню межу слід знизити до нуля.

Останній параметр, який ми повинні визначити, - це відстань верхньої межі області перегляду. З рис. 2.2 видно, що це проекція на горизонтальну площину відстані від камери до перетину верхньої межі області перегляду з верхньою межею висоти області огляду, яку ми встановили раніше.

Хоча область огляду може бути нескінченною, як правило, нас цікавить спостереження не тільки в діапазоні висот від нижньої межі до верхньої межі області огляду, а й до заданої відстані. Ця відстань є верхньою межею області перегляду в цьому конкретному положенні камери.

Таким чином, щоб отримати розміри та положення проекції області огляду по відношенню до камери, необхідно задати наступні параметри :

- Формат датчика зображення та фокусна відстань об'єктива.
- Висота установки камери.
- Висоти верхньої та нижньої межі області огляду.
- Відстань до верхньої межі області огляду

За допомогою цих параметрів значно зручніше визначити всі інші параметри проекції області огляду.

2.3 Підбір об'єктива та матриці камери.

Підбір об'єктива та матриці камери відеоспостереження відбувається виходячи з параметрів місця монтажу камери, геометричних розмірів спостерігаемого об'єкта та типу задачі спостереження.

Важливо вибрати розмір об'єктива для матриці камери. Якщо об'єктив призначений для матриці меншого розміру, ніж та, яка встановлена в камері, зображення буде затемнено по кутах.

Якщо об'єктив призначений для матриці більшого розміру, ніж та, яка встановлена в камері, то отримане поле огляду буде менше того, на яке розрахований об'єктив, оскільки частина зображення опиниться за межами датчика і буде втрачена. У цій ситуації виникає ефект телеоб'єктиву, оскільки зображення здається збільшеним, як при використанні зуму.

Чим більше розмір відеосенсора (матриці) тим більше кут огляду відеокамери та навпаки чим менше розмір відеосенсора тим менше кут огляду відеокамери . розмір відеосенсора вимірюється у дюймах $\frac{1}{2}$ " (по діагоналі), або у міліметрах, (Нмм*Vмм).

2.4 Розрахунок кута обзору об'єктива.

Розрахунок кута обзору об'єктива виконується по формулі:

$$\lambda = 2\arctg\left(\frac{d}{2F}\right) \quad (2.4)$$

λ - кут огляду об'єктива

d - діаметр світлочутливого елемента

F – ефективна фокусна відстань.

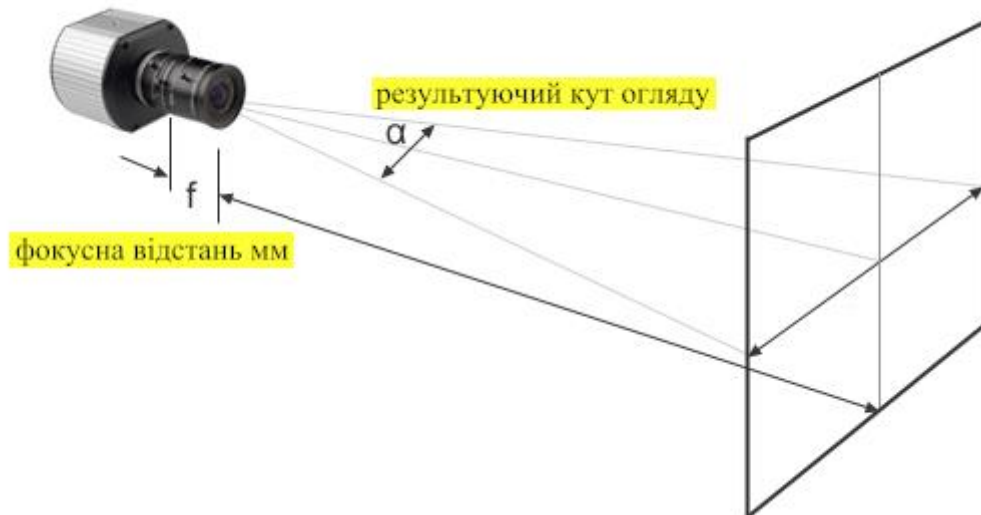


Рисунок 2.4 – Кут обзору об'єктива.

Фокусна відстань — один із параметрів об'єктива, що визначає кут огляду камери відеоспостереження. Фокусна відстань вимірюється в міліметрах і зазвичай позначається латинською літерою f (f , мм).

Чим менша фокусна відстань тим більше кут огляду відеокамери та навпаки чим більша фокусна відстань тим менше кут огляду відеокамери. Фокусна відстань записується як $f = \dots \text{мм}$.

2.5. Необхідна роздільна здатність

Раніше в аналоговому відеоспостереженні роздільна здатність була стандартною та не дуже високою, але з появою IP відеокамер та з розвитком аналогових стандартів високої якості роздільна здатність зображення може бути практично будь якою.

Традиційно у аналогових системах відеоспостереження вимоги до роздільної здатності формували на основі того яку долю кадру по вертикалі повинен займати спостерігаємий об'єкт. Для різних цілей необхідна різна величина об'єкту у кадрі. Але з появою мегапіксельної роздільної здатності це стало не дуже актуально, детальність зображення залежить не тільки від того з

яким наближенням спостерігаємо об'єкт, а більше від роздільної здатності матриці що використовується.

Навіть при широкому куту огляду та високій роздільній здатності матриці можливо цифровими засобами збільшити необхідний фрагмент та вирішити поставлену задачу.

2.6 Зона впевненого розпізнавання людини

Одного просторового розширення часто недостатньо щоб бути впевненим що людина буде опізнана, для цього необхідно ще ряд факторів.

Ідентифікація має імовірнісний характер, тобто в більшості випадків об'єкт може бути реально ідентифікований та виявлений лише з якоюсь імовірністю яка нажаль не дорівнює 100%. Таким чином можна казати лише о значній більшості ймовірності ідентифікації та виявлення в розрахованих зонах по відношенню до решти зон огляду камери.

Абсолютно точно цю ймовірність розрахувати практично неможливо із-за різноманітних вбиваючих на цей процес факторів.

Але вибираючи значення критеріїв для ідентифікації та виявлення можливо отримати зони різного розміру з більшою або меншою ймовірністю виявлення та ідентифікації.

Критерії ідентифікації людини.

Зони ідентифікації людини це частини зони огляду камери в якій виконуються всі критерії ідентифікації людини.

Є наступні критерії ідентифікації людини

- мінімальна висота ідентифікації.
- максимальна висота ідентифікації.
- мінімальний вертикальний розмір зображення лиця (кількість пікселів що приходить на лице).
- максимальний кут між напрямком на камеру і горизонталлю.

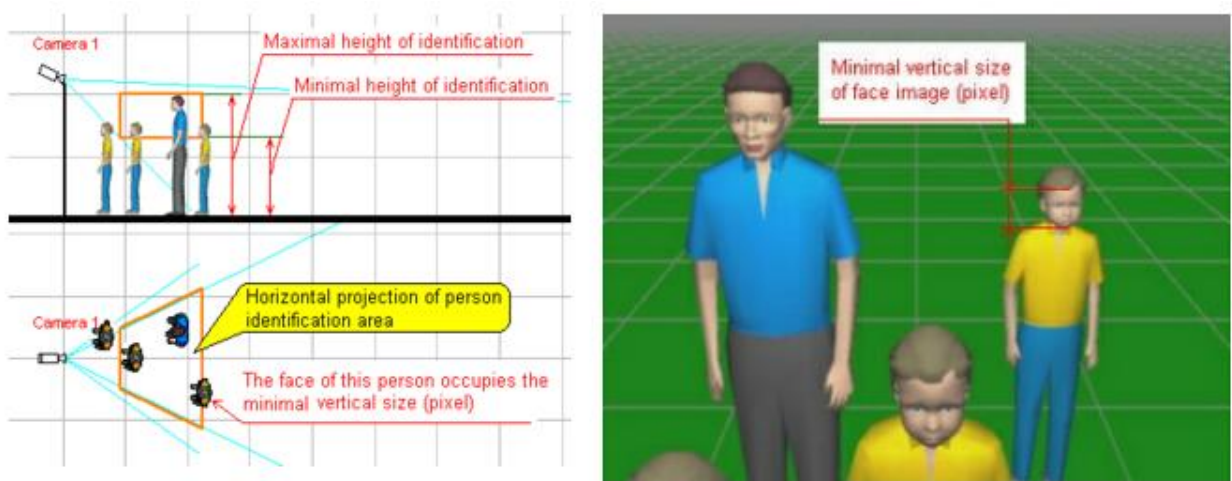


Рисунок 2.6 – Зона ідентифікації особи.

Всі критерії можна виміряти і тим самим можливо розрахувати горизонтальну проекцію огляду камери в якій з великою ймовірністю людина буде ідентифікована.

Для того щоб людина любого зросту була ідентифікована, необхідно щоб його лице потрапило в зону огляду. На даний факт впливає мінімальна та максимальна висота ідентифікації. В звичайних умовах вибираються наступні параметри, а саме 1.3 м для мінімальної та 2м для максимальної висоти ідентифікації.

Якщо лице людини потрапило до кадру необхідно мати достатню детальність зображення для подальшої ідентифікації.

Ідентифікація значно ускладнюється в тому випадку коли лице людини відображається на екрані під великим кутом, тим паче якщо люди з'являються у капелюхах, або дивляться під ноги.

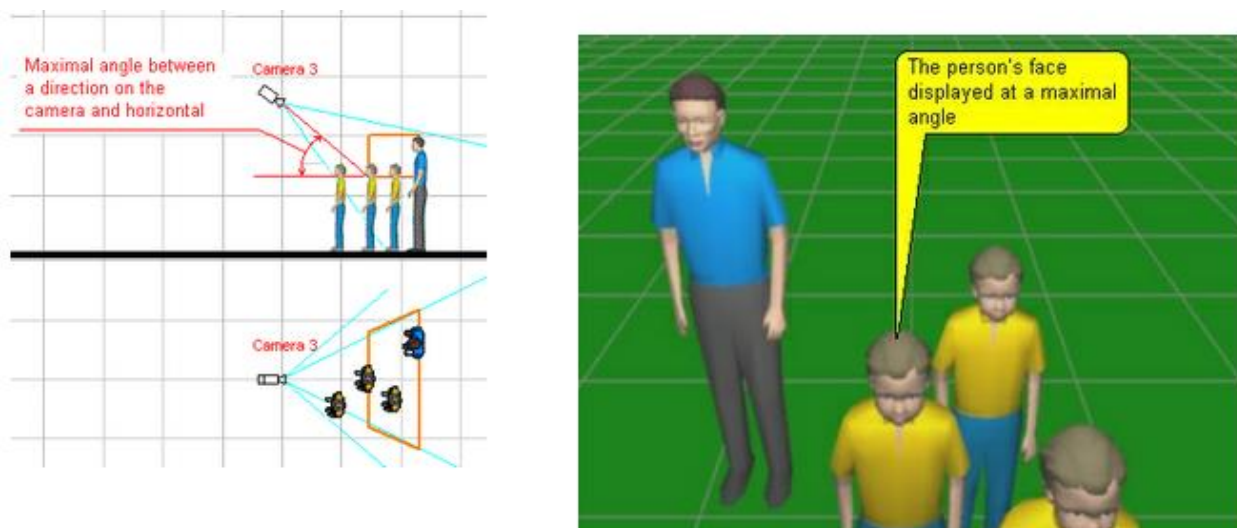


Рисунок 2.7 – Максимальний кут між напрямком на камеру та горизонтальну.

Наприклад для людей без капелюхів максимальний кут між горизонталлю та направленням на камеру складає 35° .

Зону ідентифікації особи необхідно забезпечити на двох напрямках, а саме на прохідних пунктах. За допомогою програмного забезпечення ProjectDesignTool вибираємо необхідні параметри камери та обираємо найбільш підходяще обладнання. На наступному малюнку приведені зони огляду для камер №1 та №2.

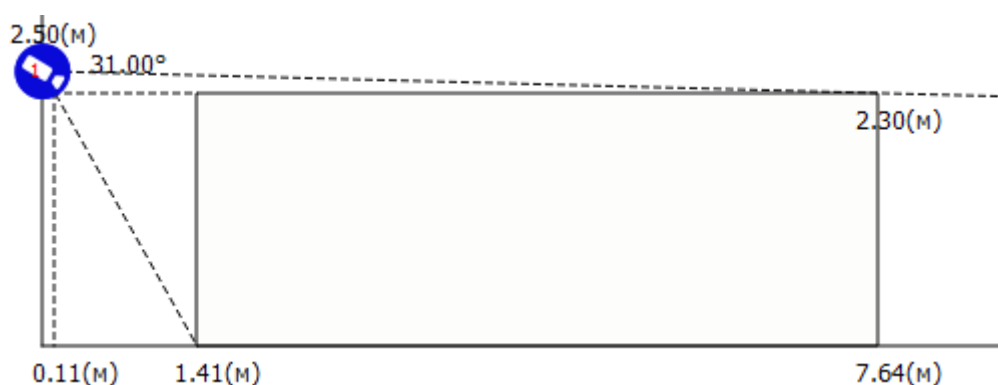


Рисунок 2.8 – Зона огляду камери №1

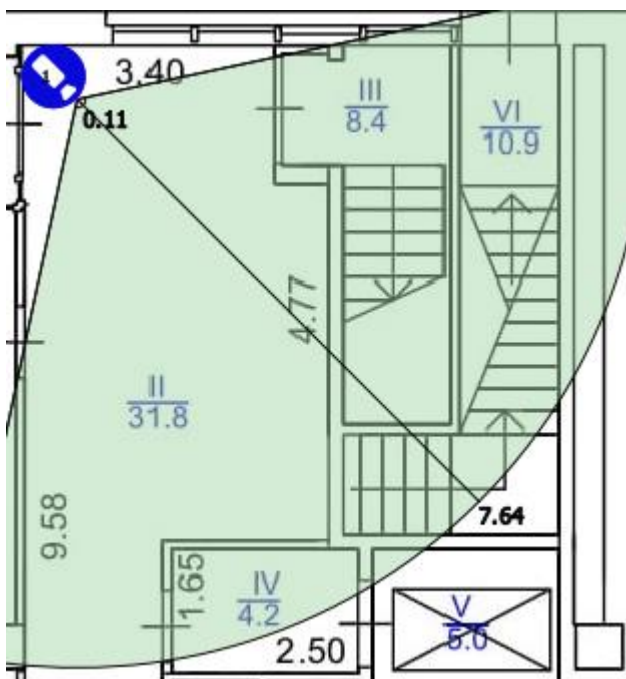


Рисунок 2.9 – Вид зверху на камеру №1

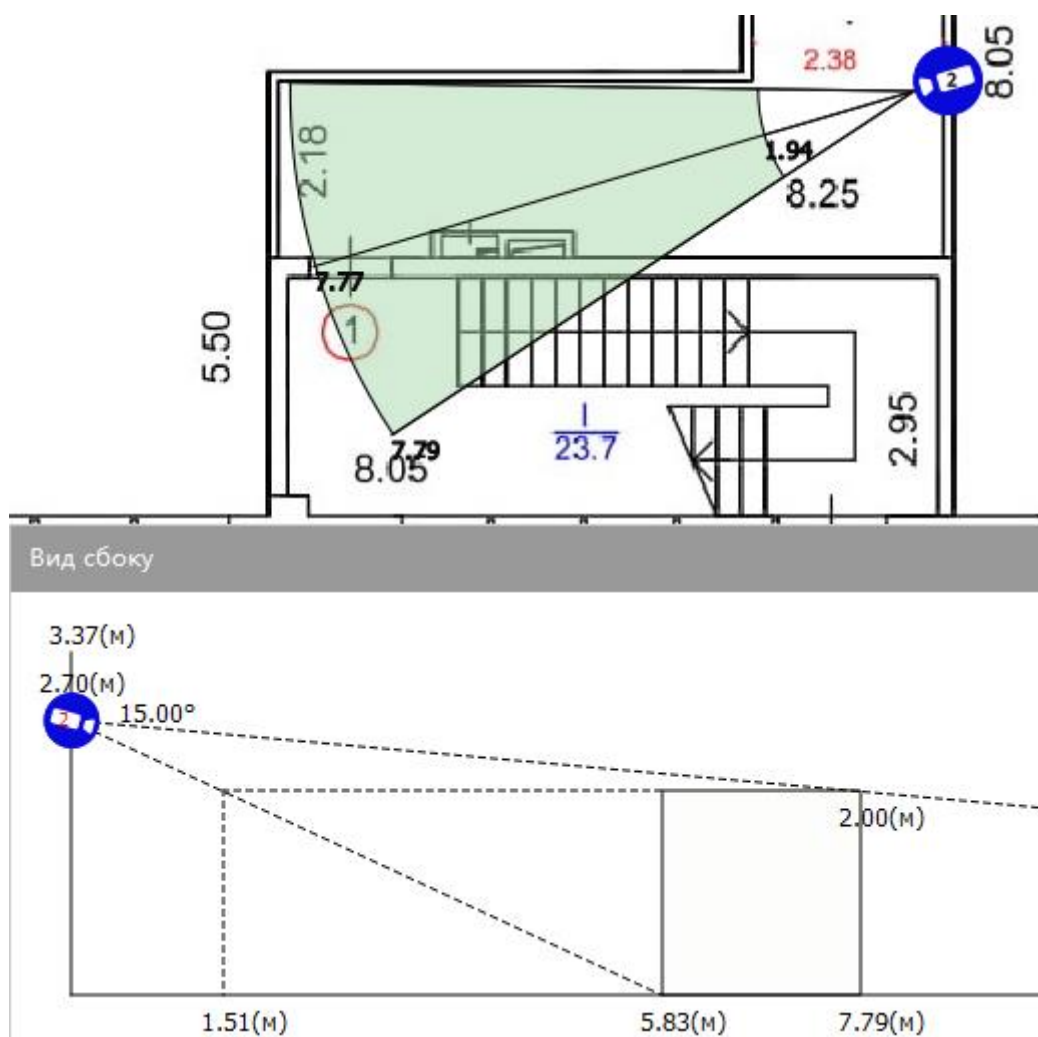


Рисунок 2.10 – Зона огляду та вид зверху камери №2.

Завдяки програмному забезпеченню були визначенні наступні параметри:

- висота установки камери
- висота верхньої границі зони огляду.
- відстань до верхньої границі зони огляду

Як було описано вище ці параметри необхідні щоб на наступному етапі проектування методом простих обчислень отримати фокусну відстань та розширення матриці камери відеоспостереження. Використовуючи програму CCTV Design lens calculator визначаємо параметри об'єктиву та відео сенсору що підійдуть для даної зони огляду .

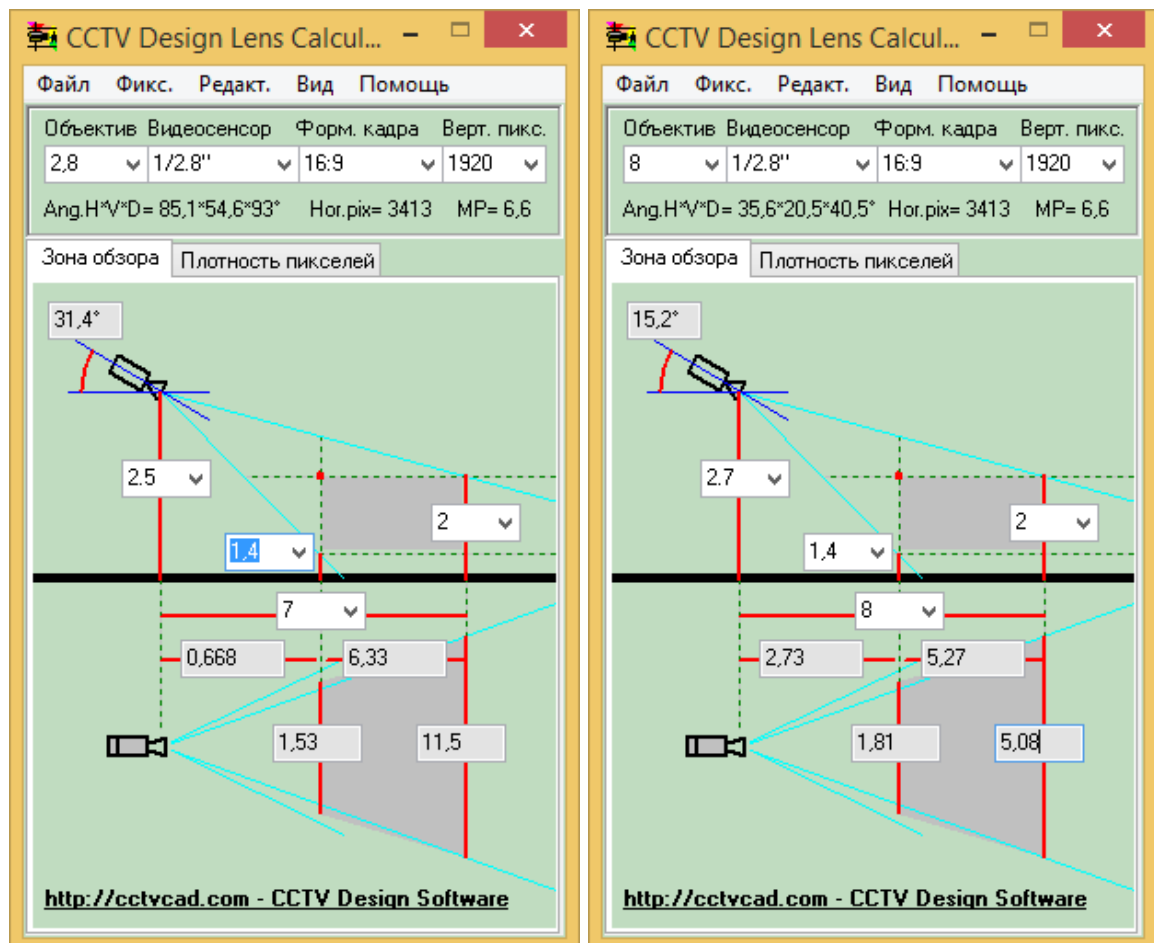


Рисунок 2.11 – Параметри зони огляду камер №1 та №2

Для камер №1 та №2 дуже важливо провести ці розрахунки так як на дане обладнання лягає функція ідентифікації людини. Камера №1 та №2 розташовані перед входом у офіс біля поста охорони. Вони спостерігають за

головними проходами і призначаються для ідентифікації осіб, що входять у двері. Також камери повинні мати функції інтелектуального розпізнавання що підвищує охороні та аналітичні можливості системи.

Камери №3,№4,№5,№6 розташовані в робочій зоні та зоні відпочинку і виконують функції моніторингу процесів або локацій. А саме дотримання трудової дисципліни, стандартів обслуговування клієнтів або слідкують за правилами приймання товару. Також можливо використовувати це як маркетинговий інструмент підвищення довіри споживача через трансляцію на різноманітні веб ресурси. Ці камера розташовані таким чином щоб з мінімальною кількістю камер забезпечити функцію огляду по всій робочій зоні.

Камера №7 розташована в складському приміщенні та оглядає невелику кімнату, фіксуючи кожного хто заходить туди.

2.7 Локальна мережа

ІР відео нагляд будується на основі технології Ethernet і враховує обмеження та особливості мережевих протоколів та стандартів, таких як RTSP, РоЕ і так далі.

Класична структура локальної мережі стандарту Ethernet це зірка, але часто не вистачає стандартного сегменту в 100 метрів, бо для мереж відеонагляду це частіше за все недостатньо. Тому виникає спокуса використовувати каскадне підключення комутаторів, але це неправильний підхід до вирішення задачі. Існують дуже серйозні мінуси каскадного підключення такі як затримка в передачі інформації, додатковий транзитний трафік для проміжних комутаторів та низька надійність такого рішення.

Переважною є схема по топології зірка, при чому якщо довжини Ethernet кабелю недостатньо то необхідно переходити на оптоволоконні лінії.

Для переметральних та магістральних систем відеонагляду має більшу перевагу кільцева архітектура. Кільце призначено для підвищення надійності

та живучості системи, використовуються стандарти Industrial Ethernet, що виконують швидку перебудову маршруту передачі пакетів трафіка при обриві мережі по резервному маршруту, перебудова маршруту займає приблизно 20мс, що для відеонагляду зовсім не критично.

Оптимальна структура локальної мережі для систем відеонагляду представлена на рисунку 1.9.

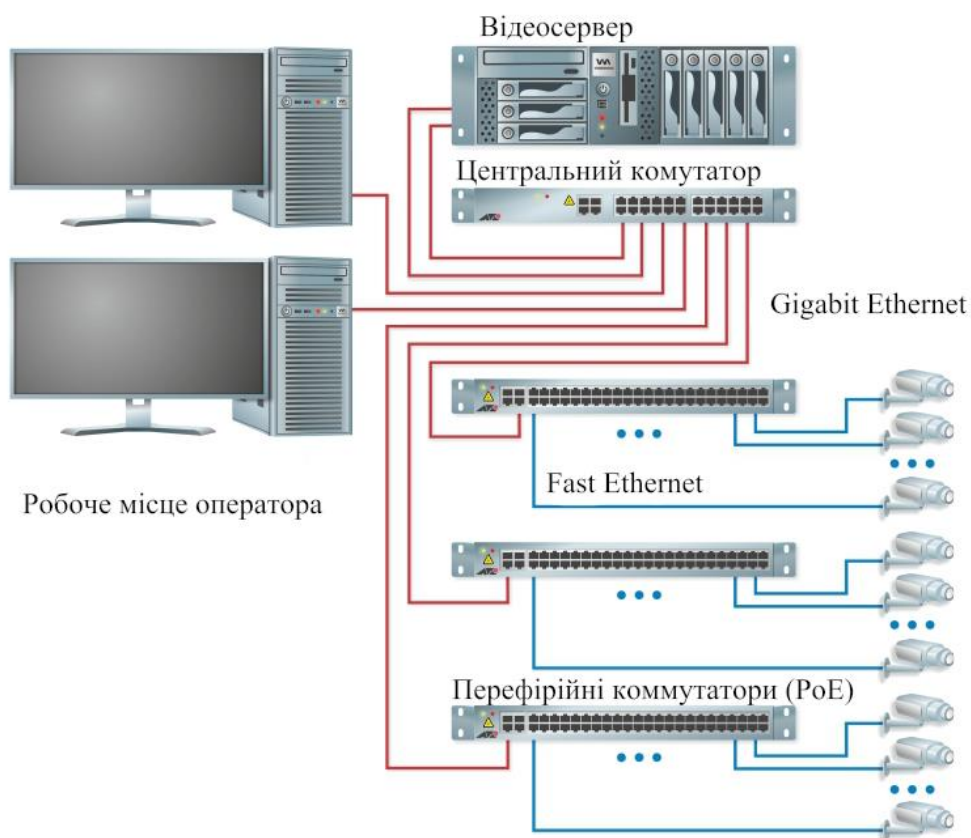


Рисунок 2.7 – Оптимальна структура локальної мережі для систем відеонагляду

Вона припускає що периферійні комутатори приймають потік від камер та живлять їх за допомогою технології POE, та передають дані на центральний комутатор, так зване ядро. До нього підключаються відеосервери та робочі місця операторів.

2.8 Розрахунок трафіку

Розрахунок трафіка необхідний для визначення вимог до комутаторів для виявлення потреби в агрегації каналів і визначення кількості відеосерверів. Розрахунок відбувається від IP камер як основного джерела генерації трафіка. Інформацію про те який потік генерує камера можна взяти у виробника даних камер, ці дані будуть в певній мірі точними, при цьому необхідно враховувати який буде використовувати відео-кодек, як правило використовують кодеки з між кадровим стисненням, коли передається не кожен кадр з камери, а лише опорні кадри, а між ними лише змінення картинки у порівнянні з попереднім кадром. Це дозволяє сильно зменшувати бітрейт але при цьому є цілий ряд побічних ефектів які будуть заважати при розрахунках.

По перше бітрейт при між кадровому стисненні дуже сильно залежить від того яка сцена буде зніматися камерою, наскільки вона буде насичена дрібними деталями, як часто попадають до кадру рухомі об'єкти. Різниця у потоках з камери де нічого не відбувається і потоком з камери де йде інтенсивний рух натовпу може бути в декілька разів.

При розрахунках необхідно хоча б приблизно враховувати яка буде інтенсивність руху в кадрі для того щоб в одному разі не перебільшити запас системи, а з другого боку щоб система працювала в нормальному режимі. Для цього необхідно використовувати рекомендації виробників або калькулятори які виробники обладнання розміщують на своїх веб ресурсах.

Програмне забезпечення що буде керувати системою відеонагляду при підключені до камери може змінювати деякі параметри передачі відео потоку тим самим змінюючи бітрейт з камери, наприклад програма може змінити значення опорного кадру щоб більш якісно детектувати рух, із-за цього потік буде збільшено.

До розрахунку необхідно приймати всі потоки що передає камера. Сучасні IP камери передають як мінімум два потоки, на запис та на відтворення. Потоки можуть бути різної якості, як правило на запис йде у

повному розширенні, другий потік на відтворення йде у меншій якості, та з меншою кількістю кадрів на секунду. Як правило відображення відбувається на одному моніторі декількох камер тому немає сенсу відображати в повній якості, розширення самого екрану не дасть це зробити. В окремих випадках з камери може надходити третій потік наприклад для відеоаналітики. Всі потоки необхідно скласти і отримаємо трафік що йде з одної IP камери. Як не дивно у нічний час бітрейт камери збільшується, так як камера посилено передає шум матриці із-за недостатчі освітлення.

В класичному варіанті трафік йде через комутатори на сервери системи відеоспостереження, а від серверів на робочі місця операторів. Але існують варіанти коли потік на відображення передається напряму з камер до робочого місця оператора, це дозволяє розвантажити мережеві інтерфейси сервера. Кожне підключення віддаленого робочого місця оператора до камери запитує свій незалежний потік від камери, тому якщо є декілька операторів то трафік мережі збільшиться у декілька разів також ресурси камери можуть закінчитися, при певній кількості запитів камера починає знижувати кількість кадрів в секунду яку видає в потоках.



Рисунок 2.8 – Варіанти передачі потоку на відображення

Який з цих способів краще відповісти однозначно складно, потрібно в кожному окремому випадку шукати баланс. З одної сторони є затрати на

створення локально-обчислювальну мережу, на інтерфейси та комутатори, а з іншої сторони є затрати на сервер та робоче місце оператора.

2.9 Вибір мережевих інтерфейсів

З типом мережевих інтерфейсів все досить просто. Перерахуємо різновиди Ethernet, які найпоширеніші в IP-відеоспостереженні:

100BASE-TX (100 Мбіт/с, Fast Ethernet). Використовує як середовище передачі мідну кручену пару категорії 5. Використовуються дві пари (чотири провідника). Відстань до 100 м. Режим повного дуплексу.

1000BASE-T (1 Гбіт/с, Gigabit Ethernet). Використовує мідну кручену пару категорії не нижче 5е. Задіює прийому і передачі всі 4 пари (вісім провідників). Відстань 100 м. Режим повного дуплексу.

10GBASE-T (10 Гбіт/с, 10G Ethernet). Мідна кручена пара категорії 6 для передачі на відстані до 55 м, і 6а - на відстані до 100 м. Режим повного дуплексу.

Номінальні значення швидкостей 10, 100 Мбіт/с та 1Гбіт/с не слід плутати з пропускною здатністю. Для потоків h264-h265 виробники рекомендують використовувати 50-70% пропускної спроможності кабелю, це пов'язано з тим що при передачі інформації в каналі також існує службовий трафік, та для того щоб система справлялася з піковим навантаженням (вмикання та вимикання серверів), або задля можливості розширення та модернізації системи.

2.10 Вибір комутаторів

Після розрахунку пропускної спроможності сегментів ЛОМ та вибору типів мережевих інтерфейсів можна переходити до вибору комутаторів

Визначимо вимоги до комутатора, виходячи зі специфіки роботи в системах ІР-відеоспостереження:

Пропускна спроможність. Комутатор повинен прийняти задані потоки та передати одержувачам. Існує такий параметр, як внутрішня пропускна здатність комутатора. Він вимірюється у десятках та сотнях Гбіт/с. Цей параметр рідко зустрічається у коротких специфікаціях. Пов'язано це з тим, що всі сучасні комутатори забезпечують повну пропускну здатність по всіх портах одночасно. Немає проблем із пропускнуою спроможністю!

Бюджет PoE. В описі на комутатор необхідно звернути увагу не лише на специфікацію портів PoE (можливість видачі камери необхідної потужності), але й загальний бюджет PoE. Бюджет PoE – максимальна сумарна потужність, яку комутатор забезпечує по всіх портах PoE. Найчастіше вона менше, ніж сума номінальних значень потужностей всіх інтерфейсів з PoE цього комутатора;

Рівень комутатора. Базові рекомендації – для периферійних комутаторів закритої системи відеоспостереження можна використовувати некеровані комутатори. Як центральний комутатор (ядра мережі) рекомендується використовувати керований комутатор 2-го або 3-го рівня. Керовані комутатори 2-го рівня також знадобляться для побудови кільця.

Підтримка мережевих протоколів та технологій. У відеоспостереженні можуть бути потрібні: агрегація каналів IEEE 802.3ad - об'єднання кількох інтерфейсів в один віртуальний канал передачі інформації, QoS, VLAN і шифрування - можуть знадобитися, якщо система відеоспостереження інтегрована в загальну локальну мережу замовника.

Рекомендується забезпечити запас за кількістю портів та бюджету PoE у розмірі 20-30%. Запас дозволить забезпечити розширення та модернізацію системи відеоспостереження.

Докладніше про перераховані технології та мережеві стандарти.

PoE – Технологія Power over Ethernet (PoE) – забезпечує живлення пристроїв, підключених до мережі Ethernet, за допомогою кабелю, що використовується для передачі даних. Технологія Power over Ethernet стала де-

факто стандартом для подачі живлення IP-камерам.

IEEE 802.3ad Link aggregation for parallel links - агрегування каналів. Використовується підвищення пропускну здатність каналу. Фактично це об'єднання кількох портів в один високошвидкісний порт із сумарною швидкістю об'єднаних портів. Максимальна швидкість віртуального каналу визначена стандартом IEEE 802.3ad та становить 8 Гбіт/сек.

IEEE 802.1q або віртуальні мережі (VLAN) - протокол дозволяє всередині однієї фізичної мережі побудувати кілька окремих логічних мереж (віртуальних мереж). Наприклад, якщо на об'єкті IP-камери працюють в існуючій офісній мережі замовника, то за допомогою VLAN можна виділити окрему мережу для відеоспостереження.

IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) – протокол дозволяє керувати логічними кільцями всередині ЛОМ, приводячи її до деревоподібної структури. Основне завдання протоколу RSTP - підвищення відмовостійкості всієї ЛОМ та запобігання за кільцюванню трафіку.

IEEE 802.1p priority queues (QoS) – можливість надання різним класам трафіку різних пріоритетів в обслуговуванні за допомогою різноманітних технологій. Одна з найпоширеніших технологій, реалізована в комутаторах 2-го рівня і вище - це DSCP (Differentiated Service Codepoint - поле коду диференціювання трафіку), за допомогою якої комутатори здатні визначати тип даних у пакеті даних і таким чином розподіляти пакети типу потоку інформації, що має різний пріоритет для пересилки. QoS користується попитом у ситуації, коли необхідно забезпечити гарантовану смугу пропускання для робочого трафіку та трафіку від IP-камер при роботі в існуючій мережі замовника. Або виділення пріоритету сервісному трафіку у мережі IP-камер - управління PTZ, команди управління, події від камер тощо.

DHCP (Dynamic Host Configuration Protocol – протокол динамічного налаштування вузла) – мережевий протокол, що дозволяє пристроям у ЛОМ автоматично отримувати IP-адресу для роботи в мережі TCP/IP. Не використовується для IP-відеоспостереження через вимоги фіксованих IP-адрес

в камерах та серверах у більшості програмного забезпечення відеоспостереження.

PORT FORWARDING - це технологія, яка дозволяє звертатися з Інтернету до сервера або IP камери у внутрішній мережі за маршрутизатором. Доступ здійснюється за допомогою перенаправлення трафіку певних портів із зовнішньої адреси маршрутизатора на адресу вибраного сервера або IP-камери у локальній мережі.

VPN (Virtual Private Network – віртуальна приватна мережа) - ця технологія дозволяє забезпечити одне або кілька мережевих з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). Часто використовується для об'єднання віддалених об'єктів розподіленої архітектури в одну приватну мережу.

Якщо у вас замкнута система відеоспостереження та виділена мережа, то достатньо некерованих комутаторів. У цьому випадку їхнє завдання – запитати камери та передати трафік на станційне обладнання.

Якщо ж ви знаєте, що системі доведеться працювати в локальній мережі замовника або віддавати трафік на бік, а тим більше якщо у вас велика розподілена система, то рекомендуємо застосовувати керовані комутатори 2-го рівня, а для ядра мережі - комутатор 3-го рівня.

2.11 Розрахунок об'єму архіву запису

Спрощено можна рахувати трафік за формулою: сумарний потік з камери Мбіт/с / 8 біт * 60 секунд * 60 хвилин * кількість годин запису на добу * необхідна глибина архіву = архів на 1 камеру. Множимо на число точно таких же камер за такими параметрами і отримаємо спільний архів на даний тип камери. Таким чином потрібно розрахувати всі типи камер що є в наявності, скласти всі данні та отримати об'єм архіву для всієї відеосистеми. Таким чином розраховується чистий об'єм архіву, без врахунку службової інформації, запису

звуча.

Також необхідно враховувати резервування архіву. Ресурс жорстких дисків, які у системах відеоспостереження, навіть спеціалізованого типу, наприклад серверних, за умов постійної інтенсивної роботи під час запису відеоархіву досить інтенсивно витрачається, і завдяки цьому жорсткі диски досить швидко виходять з ладу. Один із способів, що дозволяють продовжити термін служби дискової підсистеми та захистити дані від втрати у разі виходу та строю жорстких дисків, можна використовувати RAID-масиви.

Таблиця 2.1 – Основні види RAID та їх особливості.

Рівень raid	Кількість дисків	Швидкість запису	Ефективна ємність	Захист від поломки hdd	Примітка
RAID0	Без обмежень	висока	$N \cdot S$	ні	При виході з експлуатації HDD відбувається втрата всіх даних.
RAID1	2	Низька	S	1 HDD	Найчастіше застосовується для захисту диска з ОС
RAID5	от 3	Середня	$(N-1) \cdot S$	1 HDD	При виході з ладу HDD переходить у критичний режим роботи зі зниженням швидкості запису та різким збільшенням ймовірності поломки інших дисків
RAID6	от 4	середня	$(N-2) \cdot S$	2 HDD	Витримує вихід з ладу до 2-х HDD у масиві

Де N – кількість дисків, S – об'єм одного диска.

2.12 Відео-сервер та відеореєстратор

Розглянемо переваги та недоліки відео серверів та відео реєстраторів.

Відео-сервер - це спеціалізований виріб, що складається з серверної платформи та спеціального програмного забезпечення. Завдання серверної платформи - забезпечити роботу ПЗ відеоспостереження з урахуванням специфіки конкретного і вирішуваних завдань.

Розглянемо завдання, які можна вирішити лише з використанням відео сервера.

Відео аналітика вирішує прикладні завдання, пов'язані з розпізнаванням автомобільних номерів, осіб, тривожних ситуацій. Це може бути виявлення зловмисників у натовпі, відкривання шлагбауму за розпізнаним номером або відео верифікація на прохідній. До цього варто додати безліч завдань, пов'язаних з трекінгом об'єктів, таких як видача тривоги при знаходженні об'єкта в зоні довшою заданого часу, рух у забороненому напрямку, підрахунок відвідувачів тощо;

Інтеграція з ОПС та СКУД, створення складних комплексів, що забезпечують взаємодію та об'єднують кілька окремих систем у єдине ціле, можливе лише на основі інтеграційної програмно-апаратної платформи. Завдяки інтеграції вирішується безліч і більш простих завдань, таких як запис фрагментів відео по сигналах з ОПС зі СКУД (запис інцидентів, запис факту проходження через ТД), управління поворотною камерою спрацьовування датчика проникнення на периметрі, управління розкладками на моніторах оператора та виведення камери місця пригоди по тривозі з ОПС або СКУД.

Інтелектуальний пошук в архіві це цілий клас завдань, які можна сформулювати як "оптимізація часу пошуку в архіві". Пошук може здійснюватися за прикметами, за метаданими (напрямок, швидкість, час знаходження, область, що цікавить, та ін.). З'явилися комплекси, що дозволяють шукати за номерами автомобілів, за завантаженою фотографією особи. Все це в рази і навіть у десятки разів скорочує час пошуку потрібної

інформації в архіві.

Відеореєстратори частіше за все мають доволі урізаний функціонал в порівнянні з відео-сервером. Заради справедливості варто сказати, що деякі великі виробники систем відеоспостереження пропонують складні апаратні рішення з багатим функціоналом, які на базі багатофункціональних DVR та NVR та спеціального програмного комплексу вирішують деякі з перелічених завдань. Але вартість таких рішень наближається до вартості відео-серверів та програмного забезпечення відеоспостереження. Ситуації, коли завдання може бути вирішено з використанням відеореєстратора (NVR, DVR), можна сформулювати в одному реченні. Коли вам необхідно оснастити невеликий об'єкт, де потрібно дивитися і писати, де немає сильної ІТ-служби, де не планується в найближчій або навіть віддаленій перспективі жодного розвитку. Застосування програмного забезпечення відеоспостереження та серверів буде в цьому випадку невиправданим і дорогим.

2.13 Програмне забезпечення для систем відеоспостереження

На даний момент на ринку є велика кількість різного ПЗ відеоспостереження. Відомого, іменитого, платного та безкоштовного (у комплекті з камерами відеоспостереження), з інтелектуальними функціями та без, з можливістю інтеграції з іншими системами підприємства та досить просте. Вибирати потрібно, звичайно ж, з потреб клієнта, поставлених завдань та специфіки об'єкта.

Список критеріїв для порівняння ПЗ відеоспостереження:

- Інтерфейс користувача, зручність адміністрування та швидкість запуску системи в роботу інсталятором
- Спосіб запису архіву у призмі надійності
- Вартість. Вартість порівнюємо за ліцензіями та в рамках сервера;
- WEB клієнти, мобільні програми

- Технічна підтримка
- Особливості ліцензування ПЗ. Ліцензування дод. функцій камери, оновлення та підтримка
- Розширюваність та нарощування. Докуп доп. ПЗ або заміна платформи.

З заліком вартості чи ні

- Спосіб інтеграції. В т.ч. зручність придбання. Складність налаштування
- Резервування серверів
- Програмування. Скрипти. Макроси. Автоматизація
- Популярність бренду та успішні аналогічні кейси

Система відеонагляду в офісі на Парк авеню належить до невеликої системи з простими вимогами:

- 20 IP-камер (архів 14 днів, типові параметри)
- Завдання: дивитися камери та записувати архів
- доступ переважно по WEB

Взагалі, для цієї мети чудово підходить звичайний відеореєстратор, і досить часто використання тут PC-based відео-сервера не обґрунтовано. Однак, якщо замовник ставить умову використовувати тільки сервер з програмним забезпеченням і нічого іншого, припустимо така у нього корпоративна політика, то для вирішення цього завдання вам підійде будь-яке програмне забезпечення.

Висновки до розділу 2

В даному розділі були розглянуті теоретичні дані про основні моменти проектування відеоспостереження. Розглянуті ключові етапи проектування системи відеоспостереження, проаналізована офісна будівля, виявлені зони де необхідно розташувати камери відеоспостереження. Розглянуті стандарти відеоспостереження та їх технічні особливості.

3 АПАРАТНИЙ СИНТЕЗ

3.1 Вибір відеокамер

Використовуючи інформацію приведену в минулому розділі визначимо найбільш підходящі розрахунковим параметрам щоб забезпечити експлуатаційні вимоги до системи відеоспостереження.

Таблиця 3.1 – Характеристики камер що використовуються в офісі

	DH-IPC-HDBW7442HP-Z	IPC-HFW7442HP-Z4	IPC-HDBW5241E-ZE	IPC-HFW5241EP-Z12E
Мережний інтерфейс	10/100BASE-TX	10/100BASE-TX	10/100BASE-TX	10/100BASE-TX
Матриця	1/1.8" CMOS	1/1.8" CMOS	1/2.8" CMOS	1/2.8" CMOS
Об'єктив	2.7-12mm	8-32 mm	2.7-13.5mm	8-32 mm
Нічний режим	+	+	+	+
Вбудована пам'ять	2GB	2GB	512mb	512mb
Формат відео	H.264+/H.265+	H.264+/H.265+	H.264+/H.265+	H.264+/H.265+
PoE	+	+	+	+

Після визначення зон огляду камер №1 та №2, підбираємо камери що задовольняють даним параметрам. Я вибрав камери Dahua DH-IPC-HDBW7442HP-Z та IPC-HFW7442HP-Z4. Це якісні камери які мають відео аналітичні функції та добре виконують функцію ідентифікації персоналу.

Для робочої зони та складу підходить камера IPC-HDBW5241E-ZE. Камера може бути універсальним рішенням практично в будь-якій ситуації, де необхідно організувати внутрішнє відеоспостереження за різних умов освітленості. Ідеально підходить для торгових площ та офісів. Я вибрав камеру IPC-HDBW5241E-ZE тому що вона відповідає розрахунковим параметрам. Ця

3.2 Розрахунок дискового простору для зберігання відеозаписів та вибір відеореєстратора

Завдяки програмному забезпеченню ProjectDesignTool одразу відома пропускна здатність відео потоку та необхідний об'єм архіву для зберігання даних протягом 30 діб. Камери що використовуються в даній мережі при використанні відео кодеку h264 передає повні кадри (JPEG), між ними передаються тільки кодовані зміни зображення щодо опорного кадру. У цьому полягає суть між кадрового стиску. Повні кадри отримали назву І-кадри. Далі йдуть Р і В-кадри. Р-кадри містять інформацію про зміни щодо І-кадра. В-кадри пов'язані як з І-кадрами, і з Р-кадрами. Все це націлене на більш ефективне стиснення та низький потік з високою якістю, але за це доводиться розплачуватися високими витратами на обчислювальні потужності та оперативну пам'ять сервера під час декодування. Завдяки цій технології отримуємо потік 28.41 Мбіт/с, що доволі небагато.

Щоб зберігати ці дані на жорстких дисках впродовж 30 діб необхідно 9000 Гб, а отже необхідно використовувати жорсткий диск ємністю 10 терабайт.

No.	Model	Area	Quantity	Compression	Frame Rate(FPS)	Resolution	Frame Rate(FPS)	Audio	Bit Rate(Kbps)	Recording Days
1	DH-IPC-HDBW7442HP-Z	1	1	H.264 ▼	-	4MP ▼	25 ▼	☒	4156	30
2	DH-IPC-HFW7442HP-Z4	1	1	H.264 ▼	-	4MP ▼	25 ▼	☒	4156	30
3	DH-IPC-HFW5241EP-ZE	1	1	H.264 ▼	-	1080P ▼	25 ▼	☒	4156	30
4	DH-IPC-HDBW5241EP-ZE	▼	4	H.264 ▼	-	1080P ▼	25 ▼	☒	4156	30
Capacity Requirement: 8989.15 GB Used Bandwidth: 28.41 Mbps										

Рисунок 3.2 – Розрахунок дискового простору

Знаючи кількість камер їх характеристики, та необхідний об'єм архіву можна визначити який відеореєстратор чи відео-сервер використовувати. Так як в системі доволі мала кількість камер та немає великої потреби у відеоаналітиці достатньо використовувати відеореєстратор.

Для даної системи ідеально підійде IP відеореєстратор 16-ти каналний 4K та H.265 c PoE DHI-NVR5816-16P-4KS2E. Він має можливість підключати 16 камер, тобто має непоганий запас якщо виникне потреба в збільшенні або модернізації системи. Вхідний потік на запис: до 320Мбит/с, має порти PoE та підтримує систему RAID 0/1/5/10. При організації IP-системи відеоспостереження бажано, щоб реєстратор і камери спостереження були одного виробника, це значно полегшує налаштування камер з відеореєстратором.

Комутатор доступу призначений для підключення персональних комп'ютерів, точок бездротового доступу, камер спостереження та IP-телефонів. До комутаторів доступу в ТЗ сформовані наступні вимоги:

- кількість портів – 24/48x100 BaseTX, 2x1000 BaseLX;
- підтримка VLAN;
- підтримка STP;
- технологія PoE;

Поставленим вимогам відповідає комутатор DGS-3120 з підтримкою PoE відповідає вимогам більшості сучасних IP-камер. Має функції які виходять за рамки базових (розширений режим, режим пріоритету, режим ізоляції), дозволяючи створити гнучку та надійну мережу для зростаючого бізнесу.

Для побудови локальної мережі та живлення камер по PoE знадобиться кабель витієї пари не нижче 3 категорії та роз'єм RJ-45. Я використовуватиму кабель категорії 5е для з'єднання вузлів мережі. Цей тип складається з 4-х кручених пар і підходить для 10BASE-T, 100BASE-TX (Fast Ethernet), та 1000BASE-T (Gigabit Ethernet).

Тут потрібно зазначити, що правильне з'єднання камери з комутатором здійснюється через фіксований сегмент між розеткою і патч-панеллю,

виконаний одно дротяним кабелем (solid). З'єднання камери з розеткою та комутатора з відповідним портом патч-панелі здійснюється патч-кордом у вигляді гнучкого багатодротового (patch) кабелю з роз'ємами RJ45, виготовленим та протестованим у заводських умовах. Це єдиний варіант з'єднання, передбачений стандартом.

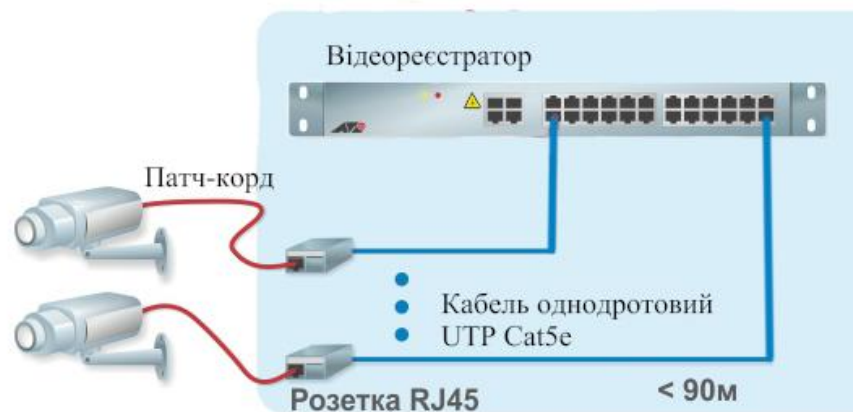


Рисунок 3.2.1 – Схема підключення відеокamer до відео реєстратора

У проектованій локальній мережі (рис.2.2.2) всі 7 внутрішніх камер підключаються до відеореєстратора по кабелю UTP 5e. Відеореєстратор забезпечує камери електроживленням та здійснює запис відеопотоків, їх архівацію та передачу записаних даних. Сигнал із відеореєстратора надходить на робочий монітор співробітника служби безпеки. Відеореєстратор підключено до інтернет-сервера. Це дозволяє керівництву вести спостереження за об'єктом віддалено.

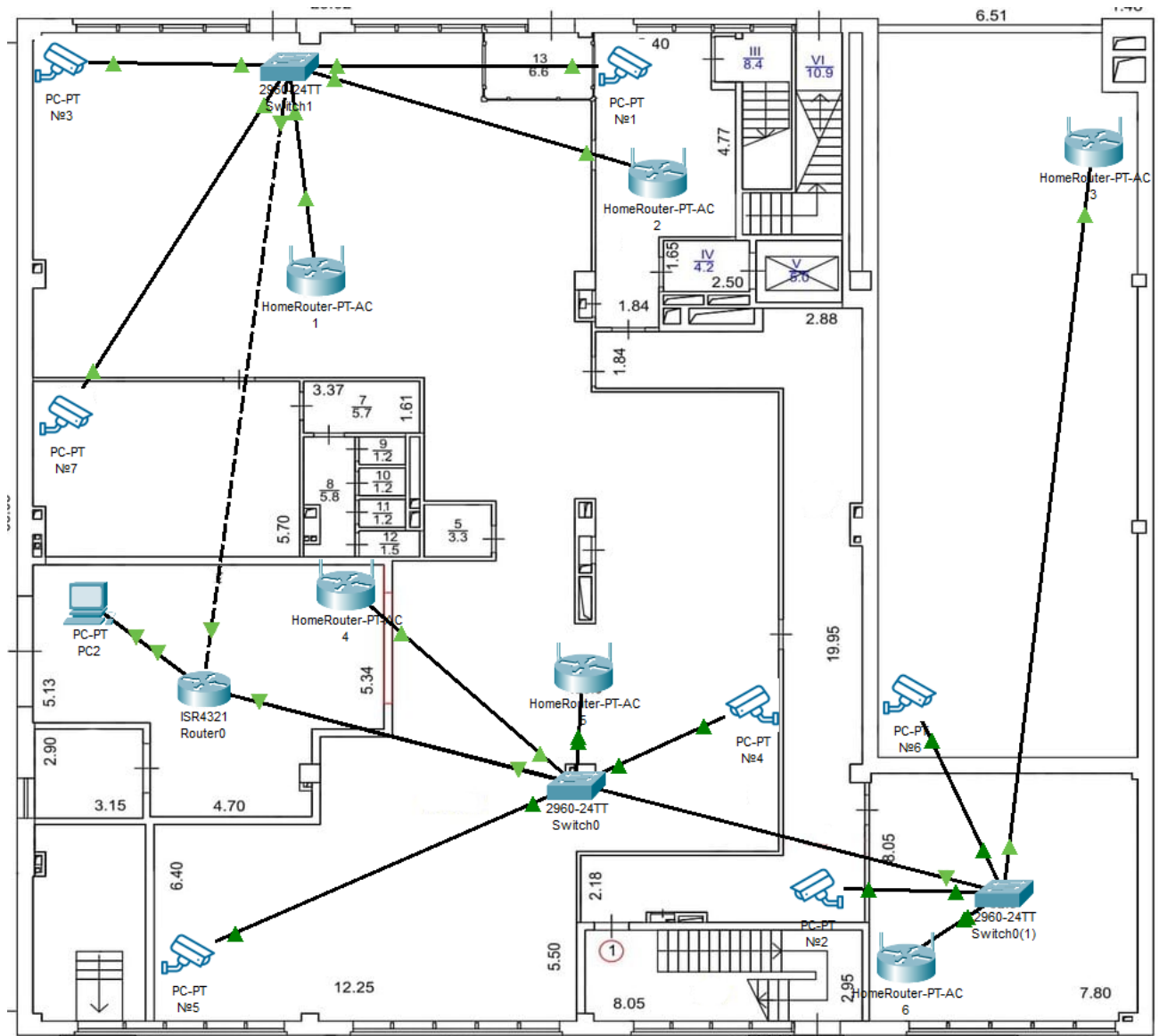


Рисунок 3.2.2 – Схема локальної мережі для IP-відеокамер

На рисунку 3.2.2 представлена схема локальної мережі для IP відеокамер. В даному випадку розглянутий випадок коли до існуючої локальної мережі додають систему відеонагляду. Головним фактором на який варто звернути уваги це пропускна здатність мережі. В класичному варіанті трафік йде через комутатори на сервери системи відеоспостереження, а від серверів на робочі місця операторів, при цьому для систем відеоспостереження рекомендується залишати про запас близько 40-30% пропускної здатності мережі. Для вже існуючих систем це доволі багато тому необхідно чітко розуміти для чого саме

система відеонагляду, щоб зберегти баланс між виконанням необхідних функцій та розумним навантаженням на вже існуючу мережу.

Висновки до розділу 3

В даному розділі за допомогою програмного забезпечення ProjectDesignTool була змодельована система відеонагляду і визначене обладнання для коректної роботи цієї системи.

ВИСНОВКИ

У рамках даної випускної роботи було спроектовано систему відеоспостереження для офісної будівлі.

Для реалізації поставленої мети необхідно було вирішити:

- проаналізувати різні технології відеоспостереження та виявити їх переваги та недоліки;
- здійснити обґрунтований вибір технології відеоспостереження, на якій будуватиметься майбутня система;
- спроектувати систему відеоспостереження;
- Провести розрахунок основних характеристик обладнання та здійснити обґрунтований вибір.

Отримана система відеоспостереження здебільшого контролює поведінку людей усередині будівлі. Фізичний захист посилено, камери діють як стримуючий фактор, спрямований проти зловмисників, які вирішили зазіхнути на майно компанії та життя та здоров'я її співробітників. Якщо навіть несанкціонований доступ до будь-якого приміщення, камери зможуть зафіксувати це та охорона встигне зреагувати, а відео архів терміном зберігання даних до 30 діб допоможе у пошуку порушника, якщо якимось чином не вдалося уникнути порушень на об'єкті.

Також система допомагає розслідувати різноманітні інциденти: збір доказової бази о протиправних діях зловмисників, клієнтів або персоналу для передачі правоохоронним органам і використання у судовому розгляді. Створювати чорні списки клієнтів. Аналізувати дії персоналу після інциденту (навчання персоналу при аналізі інциденту). Підготовка відео-кейсів для корпоративних тренінгів, корегування дій персоналу, для навчання нових співробітників чи зміна регламенту обслуговування клієнтів.

У результаті ми отримали гнучку та функціональну систему відеоспостереження, що дозволяє охороняти та контролювати об'єкт.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Нил Коэн., Джей Гэтузо., Кен МакЛеннан-Браун., Рекомендации британского МВД по выбору систем видеонаблюдения для защиты ваших объектов-2009
2. The principles of CCTV design in VideoCAD – URL: https://www.cctvcad.com/Files/the_principles_of_cctv_design_in_videocad_part1.pdf
3. Организация рабочего места оператора видеонаблюдения – URL: <https://www.videomax.ru/support/articles/organizatsiya-rabochego-mesta-operatora-videonablyudeniya/>
4. СКС для IP-видеонаблюдения – URL: <https://www.videomax.ru/support/articles/sks-dlya-ip-videonablyudeniya/>
5. ЛВС для IP-видеонаблюдения – URL: <https://www.videomax.ru/support/articles/lvs-dlya-ip-videonablyudeniya/>
6. Какие задачи может решить видеонаблюдение? – URL: <https://eozarov.ru/what-tasks-can-cctv-solve/>
7. Как выбрать матрицу камеры? – URL: <https://eozarov.ru/how-do-i-choose-a-matrix-for-the-camera/>
8. Как выбрать объектив камеры? – URL: <https://eozarov.ru/how-to-choose-a-cctv-lens/>
9. Видеосервер или видеорегистратор – URL: <https://www.videomax.ru/support/articles/videoserver-ili-videoregistrator/>
10. Опорный кадр в H.264. Маленький параметр с большими последствиями – URL: <https://www.videomax.ru/support/articles/opornyy-kadr-v-h-264-malenkiy-parametr-s-bolshimi-posledstviyami/>
11. Инструкция по охране труда при использовании систем видеонаблюдения – URL: <https://arkons.biz/instruktsiya-po-ohrane-truda-pri-ispolzovanii-sistem-videonablyudeniya>.

12. Кодек Н.265 - майбутнє IP відеоспостереження – URL:
https://secur.ua/ua/news/ua_kodek-h-265-majbutne-ip-videosposterezhennja.html

13. Проектування мережної складової системи відеонагляду заводу з
виробництва металевої продукції – URL:
https://revolution.allbest.ru/radio/00684446_0.html

ДОДАТОК А

Охорона праці, безпека в надзвичайних ситуаціях

А.1 Аналіз умов праці

Відділ оператора відеоспостереження розташований у будівлі. До основних видів діяльності належать:

- Не відволікаючись, спостерігати за виділеними для спостереження приміщеннями та об'єктами.
- Вести добовий журнал обліку роботи системи відеоспостереження.
- Негайно повідомляти керівника установи, заступників керівника, про всі помічені підозрілі події, дії.
- Знати місця встановлення відеокамер в об'єктах спостереження відповідно до схем та таблиць.
- Стежити за технічним станом та безперебійною роботою системи відеоспостереження. У разі виявлення збою у роботі негайно повідомляти керівника навчального закладу.
- Знати інструкції, положення, розпорядження, що регламентують організацію відеоспостереження на об'єкті.

Діяльність працівників напряду пов'язана з роботою на комп'ютерному обладнанні (ноутбук або стаціонарний комп'ютер) та користуванням мобільними телефонами. До основних шкідливих та небезпечних факторів виробничого середовища, пов'язаних з роботою на персональному комп'ютері, НПАОП 0.00–1.28-10 «правила охорони праці при експлуатації ОМ» належать: напруга зорових органів та пов'язане з нею перевтомлення; значне навантаження на кисті рук та пальці; тривале знаходження в сидячій позі, що викликає застійні явища в організмі; випромінювання різного виду (рентгенівське, електромагнітне, інфрачервоне, статистичні поля); механічні шуми, пов'язані з роботою кулера, дискового приводу, оргтехніки; іонізація

повітря; виділення в повітря робочого приміщення різних хімічних речовин.

Мобільний телефон є також джерелом електромагнітного випромінювання, на яке організм певним чином реагує. Наукові дослідження підтверджують негативний вплив таких пристроїв на мозок. Але вплив мобільного апарату на організм користувача і досі не є достатньо вивченим.

До психологічно шкідливих факторів, які впливають на людину при роботі з комп'ютером можна віднести розумову напругу та нервово-емоційне перевантаження, які виникають внаслідок підвищеної концентрації уваги.

А.2 Проектування робочого місця оператора

Для покращення робочих умов оператора необхідно розуміти специфіку роботи та особливості людського організму. У людини є фокус уваги, і, відповідно, він не зможе одночасно уважно спостерігати за декількома моніторами. Імовірність візуального виявлення тривожної ситуації дорівнює добутку ймовірностей подій, що його складають. Для одного екрана ймовірність дорівнює 0,4 (40%), а чотирьох вже менше 3%. Отже, виводячи оператору більше одного монітора, слід пам'ятати, що для нього один буде головним, а решта - другорядними. Крім того, існує обмеження щодо утримання підвищеної уваги – не більше 10 хв.

Таблиця А.1 – Кути огляду людського ока:

Кут зору	По горизонталі, градуси	По вертикалі, градуси
Просторовий кут ясного зору людини	12	9
Кут периферійного зору	60	60
Кут огляду з поворотом очей без повороту голови	120	90 (40 вверх, 50 вниз)

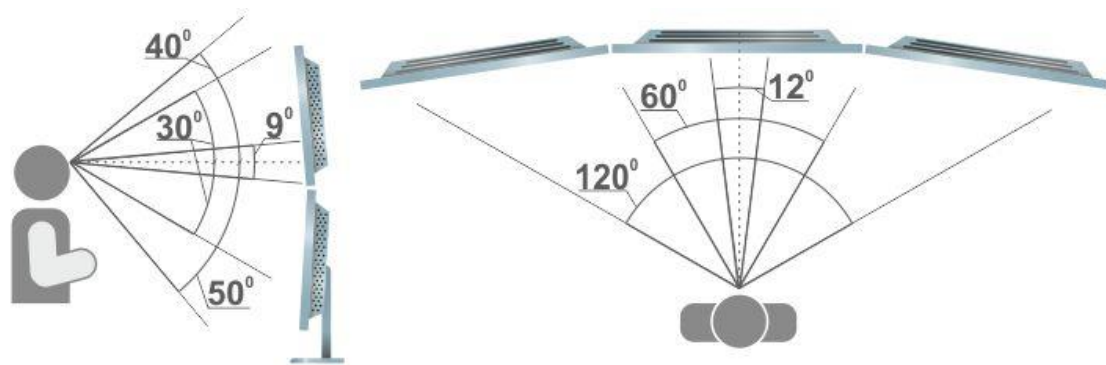


Рисунок А.2 – Кути огляду людського ока

А.3 Схема розташування моніторів та налаштування робочого місця

Спираючись на кути огляду, про які говорили вище, ми можемо сформувати типове компонування розташування екранів. У центрі розміщуються екрани з найважливішими камерами, що потребують постійної уваги: «черговий» та «оперативний». Поверх чергових моніторів правильно розташувати «тривожні» монітори, для виведення інформації про спрацювання сигналізації, тривожні ситуації, повідомлення про неполадки і т.д. У сфері периферійного зору маємо монітори з іншими камерами, які вимагають періодичної уваги оператора, звані «довідкові» монітори.

Працівник повинен знати, що раціональна робоча поза сприяє зменшенню втоми, тому необхідно забезпечити наступні вимоги.

Монітор повинен бути відрегульований відповідно до робочої пози працівника. Конструкція робочого випорожнення (крісла) повинна забезпечувати підтримку робочої пози працівника, дозволяти змінювати позу з метою зниження статичної напруги м'язів шийно-плечової області та спини для попередження розвитку втоми. Екран відеомонітора повинен знаходитись від очей працівника на оптимальній відстані 600-700 мм, але не ближче 500 мм.

Робочий стілець (крісло) повинен бути підйомно-поворотним і регульованим по висоті та кутам нахилу сидіння та спинки, а також відстані спинки від переднього краю сидіння; при цьому регулювання кожного

параметра має бути незалежним, легко здійснюваним і мати надійну фіксацію.

Конструкція робочого стільця (крісла) повинна забезпечувати:

- ширину та глибину поверхні сидіння не менше 400 мм;
- Поверхня сидіння з закругленим переднім краєм;
- Регулювання висоти поверхні сидіння в межах 400-550 мм і кутам нахилу вперед до 15° і назад до 5° ;
- висоту опорної поверхні спинки $300 + 20$ мм, ширину - не менше 380 мм і радіус кривизни горизонтальної площини - 400 мм;
- Кут нахилу спинки у вертикальній площині в межах $0 + 30^\circ$;
- Регулювання відстані спинки від переднього краю сидіння в межах 260-400 мм;
- стаціонарні або знімні підлокітники довжиною не менше 250 мм і шириною - 50-70 мм;
- регулювання підлокітників за висотою над сидінням у межах $230 + 30$ мм та внутрішньої відстані між підлокітниками в межах 350-500 мм.

Робоче місце працівника слід обладнати підставкою для ніг, що має ширину не менше ніж 300 мм, глибину не менше ніж 400 мм, регулювання по висоті в межах до 150 мм та по куту нахилу опорної поверхні підставки до 20° .

Висота робочої поверхні столу має становити 725 мм. Робочий стіл повинен мати простір для ніг заввишки не менше 600 мм, шириною - не менше 500 мм, глибиною на рівні колін - не менше 450 мм і на рівні витягнутих ніг - не менше 650 мм.

З метою зниження зорової та кістково-м'язової втоми працівникові слід дотримуватися встановленого режиму праці та відпочинку.

А.4. Автоматизація праці оператора

Автоматизувати працю оператора допоможе відеоаналітика та компонування камер.

Найпростіший спосіб полегшити життя оператору – це назвати камери за місцем встановлення, а не за номером. Далі можна групувати камери за типом. Наприклад, усі коридори, усі входи, усі вуличні камери. Крім того, добре мати готові розкладки сусідніх камер, які можна виводити на кілька моніторів за певною подією. При виявленні об'єкта в межах огляду однієї з камер відображаються зображення сусідніх камер. Адже зловмисник міг уже зникнути з поля зору цієї камери, і нам треба одразу бачити, в якій із сусідніх камер він з'явиться. Сучасні програмні комплекси дозволяють змінювати такі розкладки.

Більшість рутинних задач, що формуються, здатна виконувати відеоаналітика, коли математика за заданими правилами виявляє тривожні ситуації і сповіщає про це оператора. Звичайно, завжди є певна ймовірність виявлення і, можливо, буде багато помилкових спрацьовувань, але це незрівнянно зручніше, ніж постійно дивитися в монітори кільком операторам. В ідеалі оператор лише реагує на тривоги та приймає рішення.

Для великих та розподілених об'єктів не варто нехтувати і сервісними детекторами. Це дозволить швидко реагувати на випадки умисного порушення охоронної системи. Зараз практично будь-яке пз має у своєму арсеналі цей функціонал, при цьому безкоштовно.

- Детектор закриття об'єктива
- Детектор засвічення
- Детектор зсуву камери
- Детектор зміни фону
- Детектор розфокусування

Використовуючи цей додатковий функціонал, ми допомагаємо оператору зосередитися на найважливіших завданнях.

А.5 Заходи щодо поліпшення умов праці

Для зменшення шкідливого впливу негативних факторів виробничого середовища будуть вжити заходи щодо поліпшення умов праці. Розміщення робочих місць з ПК у підвальних приміщеннях та на цокольних поверхах заборонено. Кімната, у якій розташоване робоче місце з ПК має природне освітлення, яке здійснюється через світлові прорізи, орієнтовані переважно на північний схід. Віконні прорізи такого приміщення обладнані регульованими пристроями (жалюзі, завіски, зовнішні козирки). Також приміщення обладнане системою опалення, кондиціонування повітря, або припливно-витяжною вентиляцією для забезпечення оптимальних показників мікроклімату. Загальний контур заземлення будівлі виведений через розетку на кожне робоче місце з ПК. Забороняється для оздоблення інтер'єру приміщень з ПК застосовувати полімерні матеріали (деревинно-стружкові плити, шпалери, що миються, рулонні синтетичні матеріали, шаруватий паперовий пластик тощо), що виділяють у повітря шкідливі хімічні речовини. У приміщеннях, де розташовано монітори, потрібно виконувати заходи щодо боротьби зі статичним полем.

Площа на одне робоче місце з ПК становить не менше ніж 6,0 м², а об'єм не менше ніж 20,0 м³. Відстань від робочого місця з ПК до стіни з вікном становить не менше ніж 1,5 м; від інших стін – на відстані 1 м, а відстань між столами – 1,5 м.

Для зменшення негативного впливу мобільного апарату необхідно: скоротити до мінімуму час розмови по телефону; обирати мобільний телефон з мінімальним значенням SAR (specific absorbtion rate) – одиниця виміру питомої величини поглинання випромінювання організмом людини. Максимальне значення SAR у Європі складає 2 Вт/кг.

А.6 Пожежна безпека

Найважливішою умовою роботи будь-якого підприємства є дотримання правил пожежної охорони. У приміщенні відділу основні міри для забезпечення пожежної безпеки визначає інструкція про заходи пожежної безпеки для службових приміщень. Вона є обов'язковою для виконання всіма співробітниками. В інструкції про засоби пожежної безпеки для службових приміщень забороняється:

- улаштовувати тимчасові електромережі, застосовувати саморобні плавкі вставки в запобіжниках, прокладати електричні проводи безпосередньо по пальній основі, експлуатувати світильники зі знятими ковпаками (розсіювачами), використовувати саморобні подовжувачі, що не відповідають вимогам правил пристрою електроустановок;

- пристосовувати вимикачі, штепсельні розетки для підвішування одягу й інших предметів, обгортати електролампи і світильники, заклеювати ділянки електромережі пальною тканиною, папером;

- використовувати побутові електрокип'ятильники, чайники без непальних підставок, залишати без нагляду включеними в електромережу кондиціонери, комп'ютери, рахункові і друкарські машинки і т.п.;

- палити (крім спеціально відведених для цього адміністрацією місць, позначених написом «місце для паління» і забезпечених урною чи Попільницею з непального матеріалу), проводити зварювальні й інші вогневі роботи без оформлення відповідного дозволу, застосовувати легкозаймисті рідини.

Первинні засоби пожежогасіння (зокрема вогнегасники) призначені для гасіння пожеж у початковій стадії їхнього розвитку силами персоналу об'єкта до прибуття штатних підрозділів пожежної охорони. Визначення видів та кількості вогнегасників слід проводити з врахуванням фізико-хімічних та пожежонебезпечних властивостей горючих речовин, площ і категорії виробничих приміщень за вибухопожежною небезпекою, а також класу

можливої пожежі.

В даному випадку виробниче приміщення, де розташовані комп'ютери займає площу 50 м². Категорія приміщення за вибухопожежною та пожежною небезпекою – в, оскільки в ньому знаходяться тверді горючі матеріали (папір, меблі, тощо). Клас можливої пожежі – а. Згідно даних це приміщення, з огляду на мінімальне псування комп'ютерної техніки під час гасіння пожежі бажано оснастити двома вуглекислотними вогнегасниками типу вв – 5.

А.7 Безпека при надзвичайних ситуаціях

Об'єктом розгляду на предмет визначення надзвичайних небезпек та їх наслідків є електрообладнання. Однією із вірогідних загроз може бути раптове виникнення пожежу внаслідок короткого замикання в електромережах або розрядів статистичної електрики, що може привести до пошкодження і руйнування будівлі, устаткування, комунікацій, виділення токсичних продуктів горіння.

Тому розроблено оперативний план гасіння пожежі, який визначає порядок дії персоналу при пожежі, порядок її гасіння в електроустановках, Взаємодію з власним складом пожежних підрозділів, а також застосування схем и засобів пожежогасіння з урахуванням заходів безпеки.

Корпус обладнаний мережею протипожежного водозабезпечення, установками виявлення та гасіння пожеж відповідно вимогам нормативно-технічних документів. Кожний працівник повинен чітко знати та виконувати вимоги ППБ та протиаварійний режим на об'єкті, уміти користуватися наявними вогнегасниками, іншими первинними засобами пожежогасіння і знати місце їхнього перебування.

Меблі й устаткування розташовані таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи і виходи необхідно постійно держатися

вільними. Засоби протипожежного захисту в приміщеннях тримаються у справному стані.

При виникненні пожежі у початковій стадії його розвитку випромінюється тепло, накопичуються токсичні продукти згоряння, імовірні руйнування будівельних споруд. Тому слід як можна швидше провести евакуацію людей із палаючої будівлі. Показником ефективності евакуації є час, протягом якого працівники можуть при необхідності залишити окремі приміщення і будівлю в цілому. Безпека евакуації досягається тоді, коли час евакуації не перевищує час настання критичної фази розвитку пожежі, тобто часу від початку пожежі до досягнення граничних для людини впливів факторів пожежі (критичних температур, ступені задимлення, зниження концентрації кисню и т.п.). Число евакуаційних виходів у будівлі - два. Вони розташовувані розосереджено.

Двері на шляхах евакуації відкриваються у напрямку виходу із будівлі (приміщення). У кожному приміщенні на видному місці є вивішений план евакуації при пожежі. При пожежі обов'язково необхідно враховувати небезпечні чинники і механізм їх дії на людину. При виникненні пожежі, після виклику пожежної охорони, необхідно попередити про це усіх, хто знаходиться поруч, після чого евакуюватися самому і по можливості Допомогти евакуюватися іншим. Користуватися ліфтом категорично забороняється, за винятком ліфтів, які спеціально призначені для транспортування пожежної охорони. Шахта ліфта є шляхом для поширення диму і отруйних продуктів горіння, до того ж при пожежі ліфт часто відключають і можна опинитися в пастці при пожежі.

Якщо людина знаходиться в приміщенні де немає пожежі, но відрізана вогнем, димом, високою температурою від головних шляхів евакуації, то в першу чергу необхідно заважити доступу диму и продуктів горіння в це приміщення. Для чого необхідно негайно закрити усі щілини у дверях та під ними змоченими водою ганчірками, рушниками, робочими халатами та інш.

Рухатись у задимленій зоні поповзом або максимально пригнувшись,

необхідно тому що більшість нагрітих газоподібних отруйних речовин та дим збираються у верхній зоні приміщення, окрім цього, в приміщенні при горінні температура на рівні очей людини у 6 разів вище за температуру на рівні полу, до того ж внизу завжди зберігається більша концентрація кисню. Коли ви опинились біля вікна трохи відкрийте його та дихайте через щілину, очікуючи прибуття пожежників. При їх прибутті негайно звернути на себе увагу. Ніколи не можна стрибати через вікно без відомої на це необхідності (кожний другий стрибок з 4-г поверху при пожежі смертельний).