

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»
В.о. завідувача кафедри автоматики та
телекомунікацій

_____ Валерій ПОЦЕПАСВ
(підпис) (ім'я та прізвище)

«__» _____ 2024 р.

Випускна кваліфікаційна робота

_____ бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Розробка телекомунікаційної інфраструктури для комплексної системи
охорони ШУ «Покровське»»

Виконав студент 4 курсу, групи ТКР-20
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

_____ Котова Сергія Вікторовича
(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 к.т.н., доц., доц. кафедри ЕТКІ _____ Олександр ШТЕПА
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Нормоконтроль:

Дар'я ЖУКОВСЬКА

19.06.2024 р.

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

Студент _____
(підпис)

Луцьк – 2024 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 інфраструктури для комплексної системи охорони ШУ «Покровське»»

Виконавець, студент

гр. ТКР – 20

Сергій КОТОВ

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Керівник

Гліб СТУПАК

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Консультанти:

Ганна ТЕЛИЧКО

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Дар'я ЖУКОВСЬКА

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Нормоконтроль

Дар'я ЖУКОВСЬКА

(підпис, дата, Ім'я ПРІЗВИЩЕ)

Луцьк – 2024 р.

**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
В.о. завідувача кафедри АТ

« » 2024 року

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

Котову Сергію Вікторовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розробка телекомунікаційної інфраструктури для комплексної системи охорони ШУ «Покровське»»

керівник проєкту (роботи) Ступак Гліб Володимирович

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від 25.04.2024 року № 164.

2. Строк подання студентом проєкту (роботи).

3. Вихідні дані до проєкту (роботи)

Технічна документація та матеріали з переддипломної практики

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Аналіз об'єкту проектування. 2. Аналіз загроз для даного підприємства та можливі рішення з комплексної безпеки. 3. Вибір обладнання для системи відеоспостереження, контролю доступу, охорони периметру та пожежної безпеки. 4. Розробка проекту розташування обладнання та його налаштування. 5. Моделювання мережі підприємства. 6. Алгоритми роботи системи охорони. 7. Тестування та аналіз роботи розробленої системи.

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

План шахти. План будівлі АПК. Характеристика приміщень АПК. План приміщень АПК. Планування розташування системи відеоспостереження. План розташування елементів СКУД. План розташування датчиків та ПКП. План охорони периметру. Імітаційні моделі.

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1,3	Ступак Г.В., ст. викл. каф.АТ		
2	Теличко Г.О., доц. каф. АТ		
4	Жуковська Д.О., асист. каф. АТ		
нормоконтроль	Жуковська Д.О., асист. каф. АТ	-	19.06.2024

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз завдання	27.04.2024	
2	Аналіз об'єкту проєктування	28.04-30.04.2024	
3	Побудова системи відеоспостереження	01.05-10.05.2024	
4	Побудова СКУД	11.05-15.05.2024	
5	Побудова системи охорони периметру та приміщень АПК	16.05-20.05.2024	
6	Побудова системи пожежної безпеки для приміщення АПК	21.05-25.05.2024	
7	Реалізація та налаштування моделі системи відеоспостереження	26.05-31.05.2024	
8	Розробка імітаційної моделі та налаштування основних параметрів	01.06-06.06.2024	
9	Реалізація системи захисту телекомунікаційної інфраструктури	07.06-12.06.2024	
10	Охорона праці та безпека під час надзвичайних ситуацій на підприємстві	13.06.2024	
11	Оформлення	14.06-20.06.2024	

Студент

(підпис)

Сергій КОТОВ

(прізвище та ініціали)

Керівник роботи

(підпис)

Гліб СТУПАК

(прізвище та ініціали)

ЛИСТ ЗАУВАЖЕНЬ

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

АНОТАЦІЯ

Котов Сергій Вікторович. Розробка телекомунікаційної інфраструктури для комплексної системи охорони ШУ «Покровське» / Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» зі спеціальності 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Луцьк, 2024.

Пояснювальна записка: 83 стор., 36 рис., 8 табл., 9, додатків, 28 посилань.

У випускній кваліфікаційній роботі проведено аналіз об'єкта проектування та визначено основні задачі та вимоги до комплексної системи охорони, використане аналітичне проектування та здійснено вибір відповідного обладнання та його кількість. В роботі також описано проектування системи відеоспостереження та моделювання з використанням сучасних програмних продуктів, представлено реалізацію системи захисту телекомунікаційної інфраструктури підприємства.

Завдяки детальному підходу до проектування та реалізації комплексної системи охорони, забезпечується високий рівень безпеки шахтоуправління «Покровське», що дозволяє ефективно захищати об'єкт, майно та співробітників підприємства від потенційних загроз.

Ключові слова: ОХОРОНА, ВІДЕОСПОСТЕРЕЖЕННЯ, ШУ «ПОКРОВСЬКЕ», СКУД, ДАТЧИК, МЕРЕЖА, VLAN, ІНФРАСТРУКТУРА, КАМЕРИ, БЕЗПЕКА.

Перелік публікацій:

1. Розробка системи контролю та управління доступом для об'єктів різного призначення // С.В. Котов, Д.О. Жуковська // «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 5-6 грудня 2023 р. / ДВНЗ «ДонНТУ»; відп. ред. Г.В. Ступак. – Луцьк: ДВНЗ «ДонНТУ», 2023. – с. 183 – 186.

ЗМІСТ

ВСТУП.....	9
1 АНАЛІЗ ОБ'ЄКТУ ПРОЄКТУВАННЯ.....	11
1.1 Загальна характеристика ШУ «Покровське».....	
1.2 Основні задачі та вимоги до комплексної системи охорони ШУ «Покровське».....	
1.3 Роль телекомунікаційної інфраструктури при побудові комплексної системи охорони ШУ «Покровське».....	
Висновки до розділу 1.....	
2 АНАЛІТИЧНЕ ПРОЄКТУВАННЯ/СКЛАДОВІ КОМПЛЕКСНОЇ СИСТЕМИ ОХОРОНИ.....	20
2.1 Побудова системи відеоспостереження.....	
2.2 Побудова СКУД.....	
2.3 Побудова системи охорони периметру та приміщень АПК.....	
2.4 Побудова системи пожежної безпеки для приміщення АПК.....	
Висновки до розділу 2.....	
3 ПЛАНУВАННЯ І ПРОЄКТУВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ.....	47
3.1 Огляд та порівняння популярних застосунків для моделювання систем відеоспостереження.....	
3.2 Реалізація та налаштування моделі системи відеоспостереження.....	
Висновки до розділу 3.....	
4 РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ.....	4
4.1 Розподіл адресного простору.....	
4.2 Розробка імітаційної моделі та налаштування основних параметрів..	
4.3 Реалізація системи захисту телекомунікаційної інфраструктури.....	
Висновки до розділу 4.....	

ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	68
ДОДАТОК А – Розділ охорони праці та пожежна безпека під час монтажних робіт на промислових підприємствах у галузі зв'язку.....	71
ДОДАТОК Б – План шахти.....	77
ДОДАТОК В – План будівлі АПК.....	78
ДОДАТОК Г – Характеристика приміщень АПК.....	79
ДОДАТОК Д – План приміщень АПК.....	81
ДОДАТОК Е – Планування розташування системи відеоспостереження....	82
ДОДАТОК Ж – План розташування елементів СКУД.....	84
ДОДАТОК К – План розташування датчиків та ПКП.....	85
ДОДАТОК Л – План охорони периметру.....	86

ВСТУП

У сучасному світі, де інформація є ключовим активом, безпека підприємства виходить за межі банального захисту майна. Комплексна система охорони (КСО) стає невід'ємною частиною стратегії розвитку бізнесу, забезпечуючи захист об'єкта, його майна та людей. Особливо це актуально для великих промислових підприємств, таких як шахтоуправління «Покровське», яке є найбільшим виробником коксівного вугілля в Україні.

Актуальність роботи. Зростання обсягів виробництва, збільшення кількості працівників та постійний розвиток технологій роблять забезпечення безпеки ключовою задачею для підприємств. В умовах сучасних загроз, таких як несанкціоноване проникнення, крадіжки, пожежі та інші надзвичайні ситуації, надійна система охорони стає необхідністю. Впровадження комплексної системи охорони дозволяє знизити ризики та забезпечити безперебійну роботу підприємства.

Метою даної роботи є захист об'єкта від несанкціонованого доступу, пожежі та крадіжки тощо, з використанням телекомунікаційних технологій.

Виходячи з поставленої мети, в роботі необхідно поставлені наступні **задачі:**

1. Проаналізувати об'єкт проектування та визначити основні вимоги до системи охорони.
2. Проаналізувати основний тип загроз для даного підприємства та можливі рішення з комплексної безпеки.
3. Вибрати сучасне обладнання для системи відеоспостереження, контролю доступу, охорони периметру та пожежної безпеки.
4. Розробити проєкт розташування обладнання та його налаштування.
5. Здійснити моделювання мережі підприємства з використанням відповідних програмних продуктів.
6. Розробити алгоритми роботи системи охорони для забезпечення

ефективної взаємодії всіх компонентів.

7. Провести тестування та аналіз роботи розробленої системи.

Об'єктом дослідження є підприємства шахтоуправління «Покровське», яке є найбільшим підприємством з видобутку коксівного вугілля в Україні.

Предметом дослідження є комплексна інфраструктура та технології захисту.

Для досягнення мети та вирішення поставлених завдань використовуються такі **методи**:

1. Аналіз літературних джерел та нормативних документів з питань безпеки підприємств.
2. Порівняльний аналіз сучасного обладнання для систем охорони.
3. Моделювання мережі та систем охорони з використанням програмних продуктів Cisco Packet Tracer та VideoCAD.
4. Метод проєктування для розробки розташування та налаштування обладнання.
5. Експериментальний метод для тестування та аналізу роботи розробленої системи.

Структура і обсяг роботи. Випускна кваліфікаційна робота складається з вступу, чотирьох розділів, висновків: 86 сторінок, списку використаних джерел: 28 посилань, 9 додатків. В роботі представлено 36 рис., 6 табл.

Завдяки детальному підходу до проєктування та реалізації комплексної системи охорони, забезпечується високий рівень безпеки шахтоуправління «Покровське», що дозволяє ефективно захищати об'єкт, майно та співробітників підприємства від потенційних загроз.

1 АНАЛІЗ ОБ'ЄКТУ ПРОЄКТУВАННЯ

1.1 Загальна характеристика ШУ «Покровське»

Шахтоуправління «Покровське» є найбільшим підприємством в Україні і одним з найбільших у Східній Європі з видобутку коксівного вугілля.

Підприємство було створене у 1990 році. Промислові запаси вугілля складають більше 200 млн тон, а термін розробки – більше 40 років. Сьогодні шахта – одна з найсучасніших та безпечніших у вітчизняній вугільній галузі.

На шахтоуправлінні «Покровське» працює унікальний комплекс обладнання для провітрювання, дегазації й утилізації шахтного газу. Відібраний метан використовується для вироблення власної електроенергії й тепла на КГЕС (когенераційна газопоршнева електростанція).

Підприємство активно інвестує в розвиток виробництва, а також постійно виділяє кошти на підтримку співробітників та розвиток соціальної сфери м. Покровська. Загальна сума соціальних інвестицій щороку складає десятки мільйонів гривень. За останніми даними 25.02.2021р. на шахті працює більш ніж 7000 працівників.

Територія шахти представляє собою комплекс будівель основними з яких є АПК (Адміністративно-побутовий комплекс). Довжина території шахти 6км, ширина – 2км [1]. План шахти наведено на в Додатку Б.

Для всіх будівель планування та принцип проєктування мережі для охоронних систем однакова. Тому я роздивлюся проєктування на прикладі будівлі АПК.

Адміністративно-побутовий комплекс (АПК) - це комплекс будівель та споруд, що призначений для забезпечення адміністративно-господарської діяльності підприємства, організації або установи.

Найчастіше головним призначенням адміністративно-побутового комплексу є створення та надійне забезпечення всіх необхідних умов

повноцінного життя величезного штату співробітників на території виробничого підприємства або поблизу. Це можуть бути промислові комбінати з видобутку або переробки природних ресурсів, будівництво та подальше обслуговування нафто і газопроводів, найбільші агрокомплекси і т.д. Приміщення АПК може бути як постійним, так і переміщуваним.

Офіс є сучасною 3-поверховою будівлею, побудованою з цегли та оздоблено метало – профільним каркасом у кольорах підприємства.

На ШУ «Покровське» приміщення АПК має такі розміри: 51 метр завдовжки та 18 метрів в ширину. Висота стелі становить 3 метри. Корпус складається з 3 поверхів, кожен поверх має однакове планування та розміри кабінетів.

На першому поверсі розміщені начальники діляниць та нарядні для підземних працівників. На другому поверсі – начальники цехів та старші механіки. На третьому поверсі – дирекція, фінансовий відділ, приймальня, ІТ відділ. План будівлі АПК приведено у Додатку В.

Поверх складається з 16 приміщень з урахуванням підсобних приміщень та туалетів. На рисунку 1 зображено план третього поверху, на плані є позначка кожного приміщення, а саме висота, площа та номер кабінету. Поверх розділено на два крила які сполучаються довгим коридором, з обох боків якого є сходи для сполучення між поверхами. У додатку Г, табл. 1.1 наведено назви приміщень та їх площа. У Додатку Д наведено план приміщень АПК.

Перший поверх налічує близько 45 працівників. Другий поверх – близько 30 працівників. Третій поверх – 25 працівників.

1.2 Основні задачі та вимоги до комплексної системи охорони ШУ «Покровське»

Безпека – запорука процвітання. У сучасному світі, де інформація є ключем до успіху, а конкуренція невблаганно зростає, безпека підприємства виходить

далеко за межі банального захисту майна. Вона стає невід'ємною частиною стратегії розвитку бізнесу.

Комплексна система охорони (КСО) – це сукупність організаційних, технічних та програмних заходів, спрямованих на забезпечення безпеки об'єкта, його майна та людей. КСО може бути застосована для охорони житлових, комерційних, промислових та інших об'єктів.

Основні задачі КСО:

1. Запобігання несанкціонованому проникненню: КСО повинна мати засоби для виявлення та затримання порушників, які намагаються проникнути на об'єкт.

2. Охорона майна: КСО повинна мати засоби для запобігання крадіжкам, псуванню або знищенню майна.

3. Контроль доступу: КСО повинна мати засоби для регулювання доступу до об'єкта, приміщень та зон.

4. Візуальне та аудіо спостереження: КСО повинна мати засоби для спостереження за об'єктом та його периметром, а також для реєстрації подій [2].

Для ШУ Покровське необхідно спроектувати:

1. Охорону периметра, вона може включати в себе: Фізичні бар'єри(огорожі, паркани, колючий дріт); Технічні засоби (датчики руху, вібрації, магнітоконтантні датчики, тепловізори, системи відеоспостереження, шлагбауми); Службу охорони (фізична охорона, мобільні групи реагування);

2. Забезпечити охорону приміщень, а саме: Фізична охорона (охоронники, які знаходяться на об'єкті, здійснюють патрулювання та реагують на події); Технічна охорона (система датчиків, які реагують на рух, відкриття дверей, розбиття скла та інші події); Пультова охорона (система, яка передає сигнал про тривогу на пульт централізованого спостереження);

3. Пожежна безпека – на сьогоднішній день усі приміщення підприємства мають бути під охороною, основними технічними вимогами є: Приміщення має бути обладнане системами пожежної сигналізації та оповіщення(до пожежної сигналізації належать датчики різних типів та прибор керування); У

приміщеннях з підвищеною пожежною небезпекою мають бути встановлені автоматичні системи пожежогасіння.

У уваліфікаційній роботі ми розглядаємо проєкт як телекомунікаційну складову, тому із усіх складових охорони ми розглядаємо лише технічну частину. Коротко ознайомимося з кожною з них. Розповідати про систему буду у прив'язці до фірми Hikvision та Tiras.

Охоронна сигналізація – це система для виявлення та сповіщення про несанкціоноване проникнення в приміщення чи на територію, також за допомогою різних датчиків ця система може відповідати за витік води, газу таке інше. Охоронна сигналізація представляє собою панель керування на якій розташовані модуль зв'язку, блок живлення, виходи для підключення датчиків та релейні виходи, також сигналізація має бути обладнана резервним джерелом живлення. Кожний вихід на датчики називається шлейфом, який може об'єднувати в собі безліч датчиків. Шлейф – це замкнутий контур, що включає певну кількість датчиків, число яких визначається навантажувальною здатністю входу. За допомогою кнопок, розташованих на лицьовій панелі приладу, шлейф (зону) можна активувати, коли всі датчики знаходяться в черговому режимі, або скинути для проведення регламентних робіт. Кожен шлейф має кінцевий резистор EOL(End Of Line). Він дозволяє контрольній панелі визначати три стани зони – замкнуте через резистор, замкнуте без резистора, розімкнуте. Залежно від типу зони і типу датчиків кожен із цих станів може інтерпретуватися по-різному – норма, тривога, несправність. Що стосується ШУ Покровське, то тут будемо використовувати датчики руху, СМК датчики (датчик відкриття дверей) та сповіщувачі. Пожежна сигналізація – це комплекс технічних засобів, які відповідають за виявлення пожежі для подальшої передачі повідомлень на ЦПН(Центральний Пульт Нагляду), а також для активації систем пожежогасіння. Розглянемо основні компоненти пожежної системи:

1. Датчики пожежі: вони здатні виявляти що найменш 4 признаки пожежі, такі як дим, висока температура, відкрите полум'я, або високу концентрацію вуглекислого газу. Існує 5 основні типи датчиків на сьогоднішній день, та ще

випробовується шостий. Розглянемо кожний з них: Іонізаційні димові датчики – принцип їх роботи іонізація повітря в датчику, шляхом створення потоку заряджених частинок. Коли дим потрапляє в датчик, він перешкоджає руху іонів, що зменшує електричний струм і призводить до спрацьовування датчика; Оптико-електронні димові датчики – у їх основі полягає технологія інфрачервоного випромінювання для виявлення диму. Вони мають випромінювач, який випускає інфрачервоні промені, та приймач. Коли дим потрапляє у зону проходження променів, інфрачервоні промені розсіюються, що змінює кількість світла, що доходить до приймача, і активує датчик; Теплові датчики – реагують на різке зростання температури. Теплові датчики вимірюють абсолютну та відносну зміну температури в приміщенні і спрацьовують, коли температура досягає певного порогу; Ще існують світлові датчики – вони реагують на зміну освітленості приміщення, як правило їх ставлять у темних приміщеннях де немає змоги встановити попередні два датчики; Комбіновані датчики – поєднують властивості димових та теплових датчиків, забезпечуючи більшу надійність і зменшуючи ймовірність хибних спрацьовувань.

2. Приймально-контрольні прилади (ППК): приймають сигнали від датчиків і активують системи оповіщення та управління евакуацією.

3. Системи оповіщення: включають сирени, світлові індикатори та мовні сповіщувачі для інформування людей про необхідність евакуації.

4. Управління евакуацією: включає плани евакуації та маршрутизацію людей до безпечних зон.

5. Автоматичні установки пожежогасіння: можуть бути активовані системою для негайного реагування на пожежу.

На відміну від охоронної сигналізації, пожежна має набагато більше складнощів при проектуванні та виборі компонентів, бо є багато нюансів у виборі датчиків та є багато нормативних документів. Що стосується ШУ Покровське, вистачить оптико – електронних пожежних датчиків, вони чутливі та принцип їх роботи підходить до приміщень офісного типу.

Відеоспостереження є важливою частиною сучасних систем безпеки. Воно

дозволяє не тільки фіксувати події в реальному часі, але й зберігати записи для подальшого аналізу. Системи відеоспостереження можуть бути використані в різних сферах, від охорони приватної власності до забезпечення громадської безпеки [3].

Відеоспостереження зробило великий стрибок у розвитку, на сьогоднішній день актуальними є цифрові ір камери. Вони дозволяють ефективніше слідкувати за об'єктом. Цифрові ір камери мають більш швидкісну передачу кадрів, але це за умови якісного інтернет з'єднання. Цьому сприяють кодеки передачі даних, їх як правило два H.264 та H.265. Кодеки H.264 та H.265 є стандартами стиснення відео, які використовуються для зменшення розміру відеофайлів без значної втрати якості та зменшує навантаження на мережу. Основні відмінності між ними наведено у табл.11.

Таблиця 1.1 – Порівняння кодеків

H.264	H.265
Створений у 2003 році	Створений у 2013 році
Найпоширеніший кодек для відеострімінгу, завдяки своїй ефективності у стисненні відео зі збереженням низького бітрейту, також передача підвантажується зі збереженого на дисках файлу.	Забезпечує до 50% більше стиснення порівняно з H.264, що дозволяє передавати відео тієї ж якості, використовуючи менше пропускну здатності чи обсягу зберігання
Досі підтримується як новими пристроями так і старими	Ідеальний для форматів відео високої роздільної здатності, таких як 4K та 8K. Що не підтримується старими пристроями
Менш складний у стисненні та декодуванні, що робить його підходящим для менш потужних пристроїв	Вимагає більш потужного оброблення, що може бути проблемою для менш потужних пристроїв

Для ШУ Покровське, я виберу кодек H.264 бо навантаження на мережу буде невеликим надалі ми його розрахуємо [4].

Також цифрові ІР камери можуть виконувати її охоронні функції, такі як:

1. Розпізнавання обличчя – це технологія, яка дозволяє ідентифікувати або

верифікувати особу на основі її обличчя. Технологія порівнює зображення отримане з камери з зображенням яке зберігається у базі даних;

2. Охорона периметру – камера малює уявну лінію чи область, яку у разі перетину, спрацює тривога;

3. Також роботизовані камери вміють слідкувати за об'єктом, що рухається.

1.3 Роль телекомунікаційної інфраструктури при побудові комплексної системи охорони ШУ «Покровське»

На сьогоднішній день майже всі охоронні системи передають данні через мережу, тому телекомунікаційна інфраструктура відіграє вирішальну роль в охоронних системах. Для ШУ Покровське буде використовуватись локальна мережа для систем охорони це підвищує рівень захисту. Також локальна мережа забезпечить надійність роботи системи. Розглянемо основні аспекти, які відображають важливість телекомунікаційної складової:

1. Надійність – це здатність системи виконувати необхідні функції, забезпечуючи неперервний зв'язок та передачу даних у заданих обставинах. Поняття надійність включає в себе такі аспекти, як безвідмовність, довговічність, ремонтпридатність, збережуваність розглянемо їх:

- Безвідмовність – це здатність системи працювати без збоїв, та з навантаженнями протягом усього часу;
- Довговічність – це придатність системи до служби за заявленим строком;
- Ремонтпридатність – це стійкість системи до відновлення після відмови;
- Збережуваність – це властивість системи до збереження даних навіть за умови переміщення.

2. Швидкість передачі даних – цей параметр включає в себе високу

пропускну здатність та мінімальну затримку у передачі даних, що дозволяє швидко отримувати данні з датчиків, сенсорів чи камер. Основні поняття:

- Біт в секунду (bps) – це одиниця виміру швидкості передачі даних, яка використовується на фізичному рівні моделі OSI.
- Пропускна спроможність – це швидкість передачі даних без появи затримок або помилок, яка визначає працездатність системи або лінії зв'язку.

3. Масштабованість – це властивість мережі адаптуватися до зростаючого обсягу роботи або можливості легко розширюватися для задоволення збільшеного попиту. Інакше кажучи, система може при різних рівнях навантаження працювати ефективно без необхідності повного реконструювання мережі. Існують три основні складові масштабованості:

- Горизонтальна масштабованість – при додаванні додаткових вузлів (сервер, мережеві компоненти тощо), система буде збільшувати свою продуктивність;
- Вертикальна масштабованість – система також збільшить свою продуктивність, якщо вчасно оновлювати апаратне забезпечення існуючих вузлів;
- Еластичність – це здатність системи швидко збільшувати або зменшувати кількість існуючих систем.

4. Інтеграція – ця складова відповідає за інтеграцію різних систем безпеки, створюючи єдину координовану мережу.

5. Захист даних – забезпечити захист від несанкціонованого доступу та інших кіберзагроз, можливо шифруванням чи ще якимось методами.

Завдяки цим аспектам, телекомунікаційна інфраструктура є фундаментом для створення ефективної та надійної КСО, яка може адаптуватися до змінюваних умов та потреб об'єкту [5].

Висновок: Комплексні системи охорони є невід'ємною частиною сучасної інфраструктури безпеки. Вони дозволяють не тільки реагувати на поточні виклики, але й прогнозувати потенційні ризики, забезпечуючи високий рівень

захисту. Розвиток технологій, таких як штучний інтелект та машинне навчання, відкриває нові можливості для підвищення ефективності цих систем. Водночас, важливо звертати увагу на питання приватності та етики при використанні систем відеоспостереження та розпізнавання обличчя.

Висновки до розділу 1

Перший розділ роботи присвячений аналізу об'єкту проєктування, а саме шахтоуправління «Покровське» (ШУ Покровське

Поставлені основні задачі та вимоги до комплексної системи охорони ШУ Покровське: запобігання несанкціонованому проникненню, охорона майна, контроль доступу, візуальне та аудіо спостереження.

Для охорони периметра та приміщень використовуються різні технічні засоби, включаючи датчики руху, магнітоконтатні датчики, системи відеоспостереження та шлагбауми.

Пожежна безпека включає системи пожежної сигналізації та оповіщення, а також автоматичні системи пожежогасіння. Використовуються різні типи датчиків, включаючи іонізаційні, оптико-електронні, теплові та комбіновані датчики.

Відеоспостереження є важливою частиною системи безпеки, забезпечуючи фіксацію подій у реальному часі та збереження записів для подальшого аналізу. Використовуються цифрові ІР-камери з різними функціями, такими як розпізнавання обличчя, охорона периметру та слідкування за об'єктом.

Комплексні системи охорони є невід'ємною частиною сучасної інфраструктури безпеки. Вони дозволяють не лише реагувати на поточні загрози, але й прогнозувати потенційні ризики, забезпечуючи високий рівень захисту. Телекомунікаційна інфраструктура є основою для створення ефективної та надійної комплексної системи охорони, що може адаптуватися до змінюваних умов та потреб об'єкту.

2 АНАЛІТИЧНЕ ПРОЄКТУВАННЯ/СКЛАДОВІ КОМПЛЕКСНОЇ СИСТЕМИ ОХОРОНИ

2.1 Побудова системи відеоспостереження

Для побудови якісної системи відеоспостереження, необхідно обрати якісне обладнання, що забезпечить ефективний моніторинг та безпеку об'єкта.

Вибір обладнання відіграє важливу роль і він має декілька складових:

1. Вибір відеокамер: відеокамери розділяють на аналогові (CCTV) та цифрові (IP). Розглянемо різницю між ними у табл.2.1 [6]:

Таблиця 2.1 – Порівняння типів камер

Аналогові	Цифрові
Тип матриці що використовують частіше CCD або CMOS. Передача зображення виконується в три етапи: отримується аналогове зображення, для обробки перетворюється в цифрове, але для передачі воно знов перетворюється в аналогове.	З цифровими камерами набагато легше, зображення відразу передається в цифровому виді, що пришвидшує передачу зображення та не псує якість зображення.
Передача сигналу здійснюється через коаксіальний кабель, або зараз виробляють спеціальний кабель, та потребують окреме живлення.	Передача – здійснюється за допомогою виті пари, що пришвидшує швидкість передачі сигналу, та має можливість живлення за протоколом PoE (power over ethernet)
Замала чіткість картини	Передають відео високої роздільної здатності

Так як аналогові камери підходять більше для нагляду за будинком чи невеликим бізнесом, для ШУ Покровське краще обрати цифрові камери. Для приміщення АПК я обрав купольні камери, внутрішнього застосування від

компанії Hikvision. Вигляд камери наведено на рис.2.1.



Рисунок 2.1 – Купольна камера

Характеристики обладнання Hikvision DS-2CD2121G0-IS:

- Максимальна роздільна здатність відео: 2 МП (1920 × 1080) - 25 к\с;
- Кут огляду: 112°;
- Живлення: 12 VDC/PoE;
- Підсвітка: До 30 метрів;
- Кодеки: H.264; H.265+;
- Інтерфейс підключення: RJ45.

Камери такого типу чудово підійдуть для спостереження у коридорах та кабінетах [7].

Для охорони периметру АПК необхідно обрати камери вуличного типу. Вони можуть з більш меншим кутом але повинні мати гарну підсвітку, та відповідати стандартам вологозахисту не менш ніж IP67.



Рисунок 2.2 – Камера вуличного типу Hikvision DS-2CD2T86G2-4I

Характеристики обладнання наведеного на рис.2.2:

- Максимальна роздільна здатність відео: 8 МП (3840 × 2160) - 25 к\с;
- Кут огляду: 84°;
- Живлення: 12 VDC/PoE;
- Підсвітка: До 80 метрів;
- Кодеки: H.264; H.265+;
- Інтерфейс підключення: RJ45;
- Додаткові функції: AcuSense.

Функція AcuSense дозволяє: виявлення перетину лінії, вторгнення, входу в регіон, вихід із регіону виявлення, захоплення обличчя, виявлення зміни сцени, руху (класифікація цілей людей та транспортних засобів), сигналізація несанкціонованого доступу до відео [8].

Для спостереження за периметром я обрав роботизовані(PTZ) камери, бо у них є властивість патрулювання периметру.



Рисунок 2.3 – Камера PTZ Hikvision DS-2DF8C448I5XS-AELW(T5)

Характеристики обладнання наведеного на рис.2.3:

- Максимальна роздільна здатність відео: 4 МП (2560 × 1440) - 25 к\с;
- Кут огляду: 84°;
- Живлення: 24 VAC/PoE;
- Підсвітка: До 500 метрів;

- Кодеки: H.264; H.265+;
- Інтерфейс підключення: RJ45;
- Додаткові функції: AcuSense, Dark Fighter [7].

DarkFighter – це нова система підсвітки, вона дозволяє підсвічувати об'єкти на далекій відстані з використанням технології лазерної підсвітки.

2. Вибір реєстратора:

Оскільки ми обрали цифрові камери то в нас лишається вибір лише NVR реєстратори. Але і в них є вибір між мережевим та фізичним. Мережеві реєстратори дозволяють ставити їх віддалено від камер на відміну від фізичних, їх потрібно ставити не далеко від камер. Для забезпечення безпеки обладнання я обрав мережеві реєстратори.



Рисунок 2.4 – Реєстратор Hikvision DS-96064NI-I16

Характеристики обладнання наведеного на рис.2.4:

- IP канали: 64;
- Роздільна здатність відеовиходу: HDMI: 4096x2160;
- Живлення: АС 220В;
- Внутрішні HDD: 16 - SATA портів, до 10TB кожен диск;
- Кодеки: H.264; H.265+;
- Інтерфейс підключення: RJ45;
- Відео детекція: VCA пошук для виявлення осіб, аналізу поведінки, підрахунку людей і теплової карти [7-8].

Даний реєстратор підтримує 64 камери, та наслідуює усі їх можливості, включаючи функцію AcuSense.

3. Вибір комплектуючих для ЦПВН(Центральний Пульт Відео Нагляду).

Для того щоб дивитися велику кількість камер необхідні в екрани з гарною якістю та роздільною здатністю.



Рисунок 2.5 – Монітор для Smart Wall

Характеристики обладнання наведеного на рис.2.5:

- Діагональ: 55”;
- Частота оновлення: 120 Гц;
- Тип матриці: QNED;
- Кут огляду: 178°;
- Живлення: АС 220В.

Для того щоб реалізувати функцію ПЗ, Smart Wall, необхідно поставити декодер, який дозволить розподілити камери по моніторах.



Рисунок 2.6 – Декодер Hikvision DS-6916UDI(B)

Характеристики обладнання наведеного на рис.2.6:

- Канали декодування: 128 до 8мп;
- Кількість HDMI: 16;
- Інтерфейс відео входу: VGA [7-8].

Останній компонент – це комп’ютер, він потрібен для контролю та налаштування Smart Wall.



Рисунок 2.7 – Комп’ютер – робоча станція

Характеристики обладнання наведеного на рис.2.7:

- Процесор: 2 x Xeon E5 2680 v4;
- Кількість ядер: 28;
- Кількість потоків: 56;
- Відео карта: GeForce RTX 4060Ti;
- Об’єм відео пам’яті: 16 Гб;
- Об’єм оперативної: 128 Гб;
- Об’єм накопичувача: 1Тб.

Виходячи з вибраного обладнання складено план розташування, що розміщено у Додатку Е.

Також необхідно створити план відео нагляду за периметром, так як я обрав роботизовані камери, необхідно встановити їх на найвищій точці. Найвищою точкою є скіповий підйом висота складає 120 метрів.

Розташування камер на такій висоті дозволить переглядати весь периметр та залишає незначні «мертві» зони.

2.2 Побудова СКУД

Шахта налічує високу кількість працівників, тож виникає необхідність розмежування доступу співробітників. Наприклад працівник відділу бухгалтерії не повинні мати доступ до ІТ відділу. Цю проблему допоможе вирішити система керування доступом.

Основною системою контролю і управління доступом є контролер «DM – 20», слід встановлювати у захищених приміщеннях. Даний контролер приймає, оброблює та зберігає інформацію, яка надходить від зчитувача «XPass D2». Контролер «CoreStation CS-40» та «DM-20» виконують зв'язок із заводським програмно – технічним комплексом «Suprema» встановлених на АРМ операторів з програмним забезпеченням.

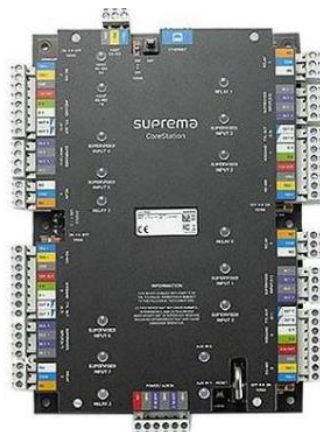


Рисунок 2.8 – Контролер «CoreStation CS-40»

Характеристики обладнання:

Suprema CoreStation – це інтелектуальний контролер, який забезпечує надійну та стабільну роботу для СКУД, за допомогою високої продуктивності. CoreStation пропонує усі функції BioStar 2, також є можливість підключення зчитувачів сторонніх виробників.

Ємність Enterprise – рівня:

- 1.4GHz Octa-core CPU;
- 8GB flash + 1GB RAM;

- Високошвидкісне зіставлення відбитків пальців, карток чи міток: до 400 000 порівнянь/секунду;
- Місткість користувачів: до 500 000 користувачів;
- Сховище журналу подій: до 5 000 000 подій;
- Централізоване безпечне сховище біометричних даних та даних груп доступу;
- Не має підключення по Ethernet до периферійних пристроїв;
- Безпечний зв'язок через TLS 1.2;
- Шифрування AES-256;
- Гнучкість системи та масштабованість;
- Сумісність із OSDP 2.0;
- Управління ліфтами з OM-120;
- Підтримує до 132 точок доступу з DM-20 та Secure I/O 2;
- 132 Wiegand-зчитувача / 64 RS-485-зчитувача;
- Підтримка сторонніх Wiegand-зчитувачів;
- RS-485, реле, входи, виходи, живлення, AUX [9].

Наступні комплектуючі це зчитувачі:



Рисунок 2.9 – Зчитувач «XPass D2»

Характеристики:

- ASK модуляція;

- Живлення: 12В;
- Клас захисту: IP67;
- Вбудований звуковий сигналізатор;
- Двоколірний світлодіодний індикатор;
- Оптичний тампер демонтажу;
- Вихід активований тампером;
- Вологозахищена залита компаундом конструкція для внутрішнього. та зовнішнього застосування;
- Корпус із міцного, стійкого до УФ променів пластику;
- Для спрощення установки постачається з монтажним шаблоном [10].

Він підійде для контролю відвідувань праці, та дозволить розмежувати відділи. Але для приміщень з більш високим рівнем доступу необхідно використовувати інші зчитувачі. Наприклад зчитувач відбитків пальців Hikvision DS-K1201AEF.



Рисунок 2.10 – Зчитувач відбитків пальців Hikvision DS-K1201AEF

Характеристики:

- Живлення: 12В;
- Клас захисту: IP67;
- Вбудований звуковий сигналізатор;
- Двоколірний світлодіодний індикатор;
- Оптичний тампер демонтажу;
- Вихід активований тампером;
- Вологозахищена залита компаундом конструкція для внутрішнього.

та зовнішнього застосування;

- Корпус із міцного, стійкого до УФ променів пластику;
- Для спрощення установки постачається з монтажним шаблоном [11].

В якості турнікетів обрати Centurion Tiso.



Рисунок 2.11 – Турнікет Centurion Tiso

Характеристики:

- Напруга живлення турнікету – $12 \pm 1,2$ В;
- Максимально споживаний струм – 0,5 А;
- Пропускна спроможність у режимі вільного проходу – 60 чол./хв.;
- Пропускна здатність в режимі одноразового проходу – 30 чол./хв [12].

На основі описаних комплектуючих елементів розроблено принципову схему розташування обладнання, що наведена у Додатку Ж.

2.3 Побудова системи охорони периметру та приміщень АПК

Розпочнемо з розробки охорони приміщень АПК. Найбільш уражене місце це перший поверх, тому на цьому поверсі потрібно ставити датчики руху у кожний кабінет, та виникає необхідність у застосуванні СМК датчиків.

Основною панеллю ПКП буде Hikvision DS – PHA64 – М.



Рисунок 2.12 – ПКП Hikvision DS – PHA64 – М

Характеристики приладу:

- Кількість зон: 64;
- Тип зв'язку: GPRS, 3G, 4G, Ethernet;
- Кількість користувачів: 45;
- Інтерфейс підключення датчиків: RS485;
- АВР живлення: Акумулятор 12В (вистачає на 16 годин) [7-8].

Датчики руху я обрав DS-PDC15-EG2 PIR Detector.



Рисунок 2.13 – Датчики руху DS-PDC15-EG2 PIR Detector

Принцип його дії заснован на перетині двох пасивних інфрачервоних датчиків.

Характеристики датчика:

На рис.2.14 бачимо, що оптимальна висота встановлення датчику 3 метри, а дальність дії 15 метрів. Кут огляду 6.3° . Датчик можливо розбити на 8 зон детекції [7-8].

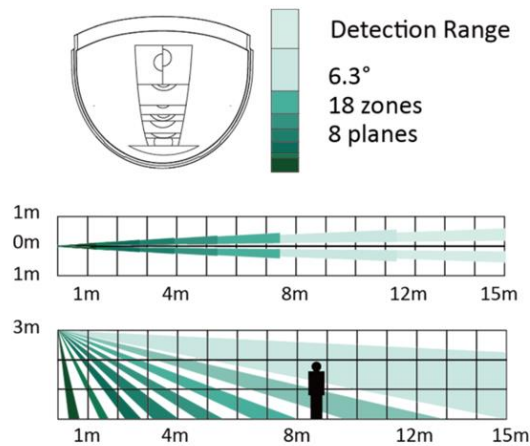


Рисунок 2.14 – Діаграма направленості датчику

Для захисту дверей використаю датчик відкриття Ajax DoorProtect Fibra. Його принцип заснован на дії електромагнітного поля, коли магніт потрапляє на відповідну частину контакти замикаються, при розмиканні контактів спрацює сигналізація [13].



Рисунок 2.15 – Датчик відкриття Ajax DoorProtect Fibra

Для захисту вікон від розбиття використаємо датчик розбиття Ajax GlassProtect Fibra, принцип дії заснован на уловлюванні звуку через мікрофон, він реагує на різкі звуки [14].



Рисунок 2.16 – Датчик розбиття Ajax GlassProtect Fibra

На інших поверхах достатньо встановити тільки датчики відкривання дверей та руху. Згідно цього розробимо план розташування датчиків та ПКП, що міститься у Додатку К.

З охороною АПК розібрались, далі охорона периметра. З цим буде трішки важче, бо територія шахти дуже велика. Щоб забезпечити надійну охорону периметру, я використаю два типи систем, а саме: Вібраційно-оптична система охорони периметру та радар Hikvision DS-PR1120.



Рисунок 2.17 – Радар Hikvision DS-PR1120

Характеристики:

- Покриття: 120м;
- Живлення: PoE або 12В;
- Ступінь захисту: IP67, IK09;
- Кут огляду: 180 °[7-8].

Вібраційно-оптична система охорони периметру, є більш сучасною та надійною. Але ця система не є автономною вона потребує ще додаткову систему. Так як в нас вона вже є, це Hikvision DS – PHA64 – М то ми використаємо її. Розглянемо основні компоненти. Перший і основний компонент це оптоволоконний дріт, наступним є оптичний спліттер [7].



Рисунок 2.18 – Оптичний спліттер

Оптичний спліттер представляє собою пасивний пристрій, який розподіляє світловий потік, що передається в одному волокні, на два або більше волокон. У нашій системі воно буде використовуватись для створення зон охорони.

Також цій системі необхідний контрольний прилад TVF-VOC-Z8 8-и зонний.



Рисунок 2.19 – Вібраційно-оптичний охоронний прилад TVF-VOC-Z8 8-и зонний

Характеристики приладу:

- Максимальна довжина кабелю охоронної зони: 1000м;
- Діапазон частот вібрації: 500 Гц~100 кГц;
- Максимальна вихідна оптична потужність: 10 дБ;
- Довжина хвилі: 1510~1590 нм;

- Кількість волокон для роботи системи-16;
- Інтерфейси: Ethernet 100Mb, FC-APC, RS485 [15].

Виходячи із компонентів створимо план розташування компонентів. Розроблений план міститься у Додатку Л.

2.4 Побудова системи пожежної безпеки для приміщення АПК

Як я вже казав раніше, проектування систем оповіщення та пожежогасіння складний процес, від нього залежить ефективність захисту об'єкту від пожежі, та у разі надзвичайної ситуації, евакуація людей.

Для того щоб вірно спроектувати пожежну сигналізацію, необхідно ознайомитися з Державним стандартами України, та основними положеннями проектування пожежної сигналізації. Для свого проєкту я обрав датчик димовий точковий оптичний, типу СПД-3.2 , попередньо ознайомившись з ДСТУ [16].



Рисунок 2.20 – СПД – 3.2

Для розрахунку кількості датчиків, необхідно провести наведені розрахунки у нормативних документах ДСТУ, кількість датчиків на пряму залежить від розміру приміщення та здатністю датчика яку площу він може контролювати [17-19].

Для початку слід вибрати схему розташування датчиків бо від цього залежать подальші розрахунки. Існує два типи розміщення – квадратне та трикутне.

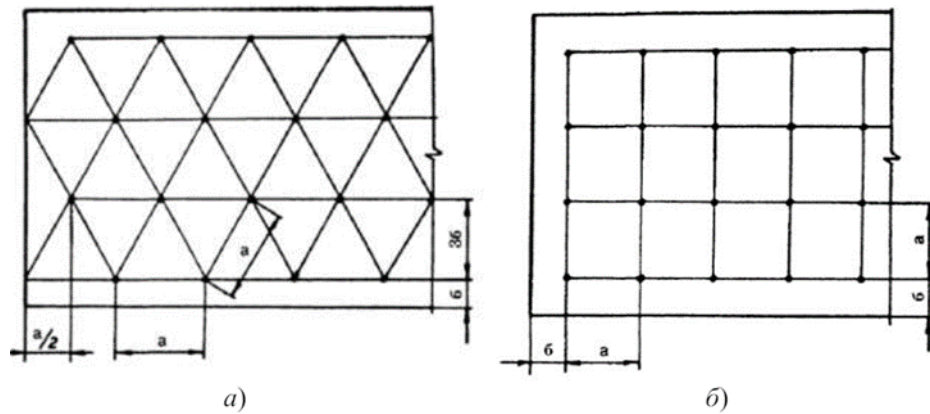


Рисунок 2.21 – Схеми трикутної (а) і квадратної (б) інсталяції сповіщувачів
а) – відстань між сповіщувачами; б) – відстань від стіни до сповіщувача

Для свого проєкту я обрав схему інсталяції – квадрат. Для заданої схеми рекомендована відстань між сповіщувачами (а) та висотою стелі до 8 метрів включно, складає 10, метрів. Відстань від стіни до сповіщувача (б) – складає 5,3 метри. Розрахуємо кількість датчиків для одного поверху АПК, так як структура приміщень однакова, тож і розташування і кількість датчиків буде однакова на всіх поверхах.

Виходячи із значення паспортної площі $S_{\text{конт}}$ для сповіщувача ця площа є коло для квадратної схеми, визначити розрахунковим шляхом максимальну допустиму відстань між сповіщувачами.

$$a_{\text{к роз}} = \sqrt{\frac{2S_{\text{конт}}}{\pi}} \quad (2.1)$$

де $a_{\text{к роз}}$ – максимальна відстань між СП для квадратної схеми;

$S_{\text{конт}}$ – паспортна зона чутливості датчика.

Спираючись на формулу (2.1), розрахуємо значення для нашого СП:

$$a_{\text{к роз}} = \sqrt{\frac{2S_{\text{конт}}}{\pi}} = \sqrt{\frac{2 \cdot 20}{3,14}} = 3,6 \text{ метра}$$

Наступним потрібно знайти максимальну відстань від СП до стіни:

$$b_{\kappa_{роз}} = \frac{a_{\kappa_{роз}}}{2} \quad (2.2)$$

де $b_{\kappa_{роз}}$ – максимальна відстань від СП до стіни для квадратної схеми;

$a_{\kappa_{роз}}$ – максимальна відстань між СП для квадратної схеми.

Спираючись на формулу (2.2), розрахуємо значення для нашого СП:

$$b_{\kappa_{роз}} = \frac{a_{\kappa_{роз}}}{2} = \frac{3,6}{2} = 1,8 \text{ метра.}$$

Виходячи з цих даних можна розрахувати кількість датчиків для кожного кабінету, але в тих яких розміщення СП регламентовано нормами ДСТУ. Користуючись даними з додатку Б розрахуємо:

– Для кабінету 303:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_{\kappa}} = A - 2b_{\kappa_{роз}} \quad (2.3)$$

де A – довжина кімнати;

$b_{\kappa_{роз}}$ – максимальна відстань від СП до стіни для квадратної схеми.

$$L_{B_{\kappa}} = B - 2b_{\kappa_{роз}} \quad (2.4)$$

де B – ширина кімнати;

$b_{\kappa_{роз}}$ – максимальна відстань від СП до стіни для квадратної схеми.

Користуючись цими формулами маємо:

$$L_{A_{\kappa}} = A - 2b_{\kappa_{роз}} = 38,43 - 2 \cdot 1,8 = 34,83 \text{ метри ;}$$

$$L_{B_{\kappa}} = B - 2b_{\kappa_{роз}} = 1,6 - 2 \cdot 1,8 = 0,2 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} \quad (2.5)$$

де L_{A_k} – відстань між крайніми сповіщувачами;

$a_{k_{роз}}$ – максимальна відстань між СП для квадратної схеми.

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} \quad (2.6)$$

де L_{B_k} – відстань між крайніми сповіщувачами;

$a_{k_{роз}}$ – максимальна відстань між СП для квадратної схеми.

Користуючись цими формулами маємо:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{34,83}{3,6} = 9,7 \approx 10 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{0,2}{3,6} = 0,05 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{cn_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) \quad (2.7)$$

де N_{B_k} та N_{A_k} – кількість проміжків між датчиками.

Звідси:

$$N_{cn_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (10 + 1) \cdot (0 + 1) = 11 \text{ шт.}$$

Аналогічно до інших кабінетів необхідно провести розрахунки.

– Для кабінету 304:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{k_{роз}} = 7,45 - 2 \cdot 1,8 = 3,85 \text{ метри};$$

$$L_{B_k} = B - 2b_{k_{роз}} = 4,23 - 2 \cdot 1,8 = 0,63 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{3,8}{3,6} = 1,1 \approx 1 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{0,63}{3,6} = 0,2 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{сн_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (1 + 1) \cdot (0 + 1) = 2 \text{ шт.}$$

– Для кабінету 305:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{k_{роз}} = 6,32 - 2 \cdot 1,8 = 2,72 \text{ метри ;}$$

$$L_{B_k} = B - 2b_{k_{роз}} = 2,66 - 2 \cdot 1,8 = 0,9 \text{ метри .}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{2,72}{3,6} = 0,76 \approx 1 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{0,9}{3,6} = 0,25 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{сн_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (1 + 1) \cdot (0 + 1) = 2 \text{ шт.}$$

– Для кабінету 306:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{k_{роз}} = 10 - 2 \cdot 1,8 = 6,4 \text{ метри ;}$$

$$L_{B_k} = B - 2b_{k_{роз}} = 6 - 2 \cdot 1,8 = 2,4 \text{ метри .}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{6,4}{3,6} = 1,76 \approx 2 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{2,4}{3,6} = 0,6 \approx 1 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{\text{сн}_\kappa} = (N_{A_\kappa} + 1) \cdot (N_{B_\kappa} + 1) = (2 + 1) \cdot (1 + 1) = 6 \text{ шт.}$$

Для спрощення розрахунку я додав сюди ще кабінет 307, у якому буде 1 датчик.

– Для кабінету 308:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_\kappa} = A - 2b_{\kappa_{\text{роз}}} = 6 - 2 \cdot 1,8 = 2,4 \text{ метри};$$

$$L_{B_\kappa} = B - 2b_{\kappa_{\text{роз}}} = 3,7 - 2 \cdot 1,8 = 0,1 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_\kappa} = \frac{L_{A_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{2,4}{3,6} = 0,6 \approx 1 \text{ пром.}$$

$$N_{B_\kappa} = \frac{L_{B_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{0,1}{3,6} = 0,02 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{\text{сн}_\kappa} = (N_{A_\kappa} + 1) \cdot (N_{B_\kappa} + 1) = (1 + 1) \cdot (0 + 1) = 2 \text{ шт.}$$

Для кабінету 309 буде така ж кількість датчиків, бо розміри приміщення приблизно однакові

– Для кабінету 310:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_\kappa} = A - 2b_{\kappa_{\text{роз}}} = 5,7 - 2 \cdot 1,8 = 2,1 \text{ метри};$$

$$L_{B_\kappa} = B - 2b_{\kappa_{\text{роз}}} = 3 - 2 \cdot 1,8 = 0,06 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_\kappa} = \frac{L_{A_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{2,1}{3,6} = 0,6 \approx 1 \text{ пром.}$$

$$N_{B_\kappa} = \frac{L_{B_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{0,06}{3,6} = 0,02 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{\text{сн}_\kappa} = (N_{A_\kappa} + 1) \cdot (N_{B_\kappa} + 1) = (1 + 1) \cdot (0 + 1) = 2 \text{ шт.}$$

– Для кабінету 311:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{\kappa_{роз}} = 5,7 - 2 \cdot 1,8 = 2,1 \text{ метри};$$

$$L_{B_k} = B - 2b_{\kappa_{роз}} = 7 - 2 \cdot 1,8 = 3,4 \text{ метри}.$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{\kappa_{роз}}} = \frac{2,1}{3,6} = 0,6 \approx 1 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{\kappa_{роз}}} = \frac{3,4}{3,6} = 0,9 \approx 1 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{cn_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (1 + 1) \cdot (1 + 1) = 4 \text{ шт.}$$

– Для кабінету 312:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{\kappa_{роз}} = 5,7 - 2 \cdot 1,8 = 2,1 \text{ метри};$$

$$L_{B_k} = B - 2b_{\kappa_{роз}} = 3,47 - 2 \cdot 1,8 = 0,1 \text{ метри}.$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{\kappa_{роз}}} = \frac{2,1}{3,6} = 0,6 \approx 1 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{\kappa_{роз}}} = \frac{0,1}{3,6} = 0,03 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{cn_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (1 + 1) \cdot (0 + 1) = 2 \text{ шт.}$$

– Для кабінету 313:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{\kappa_{роз}} = 6 - 2 \cdot 1,8 = 2,4 \text{ метри};$$

$$L_{B_k} = B - 2b_{\kappa_{роз}} = 6,5 - 2 \cdot 1,8 = 2,9 \text{ метри}.$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{2,4}{3,6} = 0,7 \approx 1 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{2,9}{3,6} = 0,8 \approx 1 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{сн_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (1 + 1) \cdot (1 + 1) = 4 \text{ шт.}$$

– Для кабінету 314:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{k_{роз}} = 8,6 - 2 \cdot 1,8 = 5 \text{ метри};$$

$$L_{B_k} = B - 2b_{k_{роз}} = 3,9 - 2 \cdot 1,8 = 0,3 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{5}{3,6} = 1,4 \approx 2 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{0,3}{3,6} = 0,1 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{сн_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (2 + 1) \cdot (0 + 1) = 3 \text{ шт.}$$

– Для кабінету 315:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{k_{роз}} = 3,7 - 2 \cdot 1,8 = 0,1 \text{ метри};$$

$$L_{B_k} = B - 2b_{k_{роз}} = 2,5 - 2 \cdot 1,8 = 0,01 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{0,1}{3,6} = 0,03 \approx 0 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{0,01}{3,6} = 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{\text{сн}_\kappa} = (N_{A_\kappa} + 1) \cdot (N_{B_\kappa} + 1) = (0 + 1) \cdot (0 + 1) = 1 \text{ шт.}$$

– Для кабінету 317:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_\kappa} = A - 2b_{\kappa_{\text{роз}}} = 4,6 - 2 \cdot 1,8 = 1 \text{ метри};$$

$$L_{B_\kappa} = B - 2b_{\kappa_{\text{роз}}} = 3,7 - 2 \cdot 1,8 = 0,1 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_\kappa} = \frac{L_{A_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{1}{3,6} = 0,3 \approx 1 \text{ пром.}$$

$$N_{B_\kappa} = \frac{L_{B_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{0,1}{3,6} = 0,03 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{\text{сн}_\kappa} = (N_{A_\kappa} + 1) \cdot (N_{B_\kappa} + 1) = (1 + 1) \cdot (0 + 1) = 2 \text{ шт.}$$

– Для кабінету 318:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_\kappa} = A - 2b_{\kappa_{\text{роз}}} = 8,96 - 2 \cdot 1,8 = 5,4 \text{ метри};$$

$$L_{B_\kappa} = B - 2b_{\kappa_{\text{роз}}} = 7,45 - 2 \cdot 1,8 = 3,9 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_\kappa} = \frac{L_{A_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{5,4}{3,6} = 1,5 \approx 2 \text{ пром.}$$

$$N_{B_\kappa} = \frac{L_{B_\kappa}}{a_{\kappa_{\text{роз}}}} = \frac{3,9}{3,6} = 1,08 \approx 1 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{\text{сн}_\kappa} = (N_{A_\kappa} + 1) \cdot (N_{B_\kappa} + 1) = (2 + 1) \cdot (1 + 1) = 6 \text{ шт.}$$

– Для кабінету 321:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_\kappa} = A - 2b_{\kappa_{\text{роз}}} = 2,28 - 2 \cdot 1,8 = 0,1 \text{ метри};$$

$$L_{B_\kappa} = B - 2b_{\kappa_{\text{роз}}} = 2,1 - 2 \cdot 1,8 = 0,1 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{0,1}{3,6} = 0,03 \approx 0 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{0,1}{3,6} = 0,03 \approx 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{сн_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (0 + 1) \cdot (0 + 1) = 1 \text{ шт.}$$

Проаналізувавши розміри, можна зробити висновок, що у кабінетах №322, 325, 328, 329 – буде однакова кількість датчиків, а саме 1 штука.

– Для кабінету 330:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{k_{роз}} = 6,6 - 2 \cdot 1,8 = 3 \text{ метри};$$

$$L_{B_k} = B - 2b_{k_{роз}} = 6 - 2 \cdot 1,8 = 2,4 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{3}{3,6} = 0,8 \approx 1 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{k_{роз}}} = \frac{2,4}{3,6} = 0,7 \approx 1 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{сн_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (1 + 1) \cdot (1 + 1) = 4 \text{ шт.}$$

– Для кабінету 331:

Визначимо відстань між крайніми сповіщувачами:

$$L_{A_k} = A - 2b_{k_{роз}} = 4,2 - 2 \cdot 1,8 = 0,6 \text{ метри};$$

$$L_{B_k} = B - 2b_{k_{роз}} = 3,6 - 2 \cdot 1,8 = 0 \text{ метри.}$$

Визначимо кількість проміжків між датчиками:

$$N_{A_k} = \frac{L_{A_k}}{a_{k_{роз}}} = \frac{0,6}{3,6} = 0,2 \approx 1 \text{ пром.}$$

$$N_{B_k} = \frac{L_{B_k}}{a_{K_{роз}}} = \frac{0}{3,6} = 0 \text{ пром.}$$

Розрахуємо кількість датчиків:

$$N_{сп_k} = (N_{A_k} + 1) \cdot (N_{B_k} + 1) = (1 + 1) \cdot (0 + 1) = 2 \text{ шт.}$$

Для кабінету 332 кількість датчиків буде така сам, бо площа приміщення однакова. Зробимо результуючу таблицю кількості СП.

Таблиця 2.3 – Кількість СП

№ Кабінету	Кількість СП	№ Кабінету	Кількість СП
303	11	317	2
304	2	318	6
305	2	321	1
306	5	322	1
307	1	325	1
308	2	328	1
309	2	329	1
310	2	330	4
311	4	331	2
312	2	332	2
313	4		
314	3		
315	1		

Згідно ДСТУ кожний вихід має бути укомплектований аварійним автономним світильником «ВИХІД» як на рис.2.22.



Рисунок 2.22 – Аварійний світильник

Також біля кожного виходу має стояти ручний пожежний сповіщувач як

на рис.2.23(а), також оскільки в нас використовується система СКУД повинні стояти пристрої для розблокування дверей як на рис.2.23(б).



Рисунок 2.23– Ручний сповіщувач (а) та пристрій для розблокування дверей (б)

Головним ППКП буде Tiras -16.128 П, це основний пристрій який підтримує підключення до себе інших ППКП [20].

Висновки до розділу 2

Для забезпечення якісного відеоспостереження на об'єкті АПК вирішено використовувати цифрові камери, які забезпечують кращу якість зображення і функціональність у порівнянні з аналоговими.

Для приміщень обрані купольні камери Hikvision DS-2CD2121G0-IS з роздільною здатністю 2 МП і кутом огляду 112°.

Для охорони периметру використані вуличні камери Hikvision DS-2CD2T86G2-4I з роздільною здатністю 8 МП і функцією AcuSense.

Роботизовані PTZ камери Hikvision DS-2DF8C448I5XS-AELW(T5) з функціями AcuSense та DarkFighter розташовані на найвищій точці для патрулювання периметру.

Для побудови системи контролю доступу (СКУД) обрано контролер Suprema CoreStation CS-40, який підтримує до 500 000 користувачів та забезпечує високошвидкісне зіставлення відбитків пальців, карток чи міток.

Для ідентифікації співробітників застосовуються зчитувачі XPass D2 та зчитувачі відбитків пальців Hikvision DS-K1201AEF.

Вхідні та вихідні точки контролюються турнікетами Centurion Tiso, які забезпечують швидку та ефективну пропускну здатність.

Для охорони приміщень обрано датчики руху DS-PDC15-EG2 PIR Detector та датчики відкриття дверей Ajax DoorProtect Fibra.

Для захисту вікон від розбиття застосовуються датчики Ajax GlassProtect Fibra.

Охорона периметру забезпечується радаром Hikvision DS-PRI120 та вібраційно-оптичною системою охорони периметру з оптичним спліттером та контролером TVF-VOC-Z8 8-и зонний.

Для побудови системи пожежної безпеки застосовано димові точкові оптичні датчики СПД-3.2, які розташовані за квадратною схемою з оптимальною відстанню між датчиками.

Для кожного виходу передбачено встановлення аварійного автономного світильника "ВИХІД" та ручного пожежного сповіщувача, а також пристроїв для розблокування дверей.

Головним пристроєм пожежної сигналізації є Tiras-16.128 П, який підтримує підключення інших ППКП.

Таким чином, запропоновані системи відеоспостереження, контролю доступу, охорони периметру та приміщень, а також пожежної безпеки забезпечують комплексний захист об'єкта АПК та гарантують високий рівень безпеки та ефективного контролю.

3 ПЛАНУВАННЯ І ПРОЄКТУВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

3.1 Огляд та порівняння популярних застосунків для моделювання систем відеоспостереження

При проєктуванні системи відеоспостереження важливо визначити кількість та тип відеокамер, їх розміщення, зони огляду, фокусну відстань об'єктивів і кількість пікселів на метр. Широкий кут огляду зменшує роздільну здатність, тому необхідно знайти баланс між розпізнаванням об'єктів, розміром зони огляду та кількістю камер. Сучасні калькулятори не враховують ефективність мегапіксельних камер і не показують кінцеве зображення, яке бачитиме оператор. Крім підбору камер та об'єктивів, важливо розрахувати обсяг відеоархіву та навантаження на мережу при використанні IP-камер.

1. CCTVCAD Software (VideoCAD).

CCTVCAD Software, заснована у 2003 році, пропонує VideoCAD та інші інструменти для автоматизації проєктування систем відеоспостереження.

Основні можливості VideoCAD:

- розрахунки: визначення геометричних параметрів зон огляду, глибини різкості, довжин і параметрів кабелів, освітленості;
- 2D проєкції: відображення результатів розрахунків на планах, моделювання зон огляду та розподілу просторової роздільної здатності;
- 3D моделювання: візуалізація меж зон огляду камер, впливу дисторсії об'єктива та покриття зон контролю;
- моделювання зображень: врахування параметрів камери, освітлення, умов середовища, фокусної відстані об'єктивів;
- інтерфейс оператора: моделювання розмірів та роздільної здатності моніторів, створення анімованих моделей;

- імпорт даних: підтримка імпорту планувань та моделей з різних форматів;
- експорт даних: можливість експорту креслень у різні графічні формати [21].

2. IP Video System Design Tool (JVSG).

JVSG пропонує IP Video System Design Tool для проєктування систем відеоспостереження. Основні можливості:

- розрахунки: кути огляду, фокусні відстані, розміри жорстких дисків, мережевий трафік, горизонтальні проєкції зон;
- 2D проєкції: побудова зон контролю з урахуванням затінення;
- 3D моделювання: відображення зон ідентифікації, розпізнавання та детекції;
- моделювання зображень: відображення від 2 до 16 камер;
- імпорт даних: підтримка форматів PDF, JPEG, BMP, PNG, AutoCAD DWG, DXF;
- експорт даних: експорт креслень у PDF [22].

3. Pelco 3D Camera Tool.

Інструмент від Pelco дозволяє моделювати зони огляду та зображення від камер Pelco. Функціональність обмежена порівняно з іншими продуктами [23].

4. Axis Camera Extension для SketchUp.

SketchUp – 3D редактор, що підтримує плагін Axis Camera Extension для моделювання зон огляду та зображень від камер AXIS Communications.

5. Axis Camera Families для Autodesk Revit.

Плагін для Autodesk Revit дозволяє моделювати зони огляду та зображення від камер AXIS Communications. Підтримує версії Revit [24].

Після аналізу сучасних програмних продуктів для проєктування систем відеоспостереження було обрано VideoCAD для моделювання системи відеоспостереження.

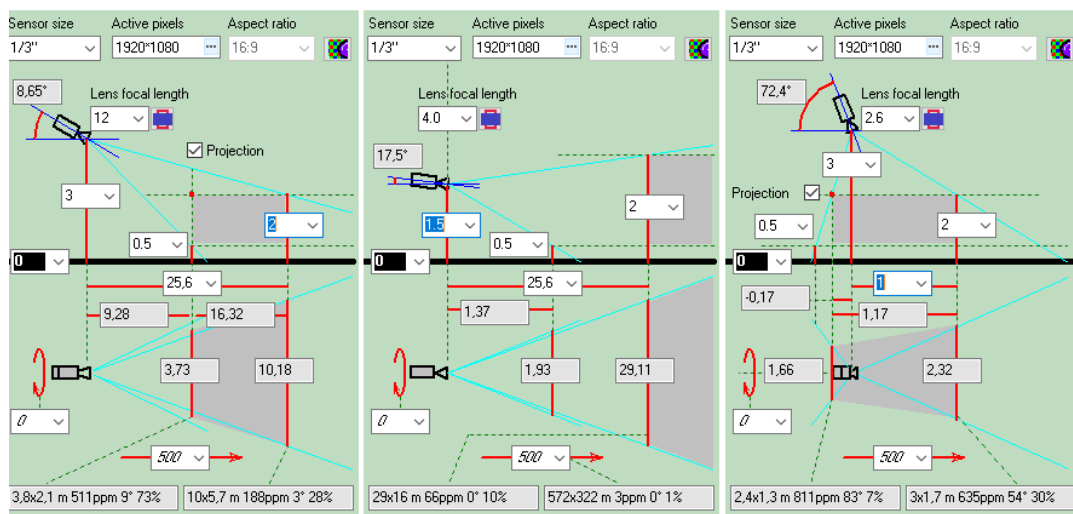
3.2 Реалізація та налаштування моделі системи відеоспостереження

При побудові моделі системи відеоспостереження важливо визначити геометричні параметри області огляду камери в горизонтальній та вертикальній площинах. У полі "Геометрія камери" відображаються проєкції області огляду, а текстові поля показують розташування камери та розрахункові параметри. Ці параметри можна змінювати, і всі інші значення автоматично перераховуються.

Для налаштування параметрів обираються камери на макеті, а їхні значення вказуються в текстових полях. Лінійні параметри вводяться в метрах або футах, а кутові – в градусах. Параметри геометрії камери не враховують спотворення об'єктива та обертання камери, якщо кут повороту менший за 45 градусів.

Приклади розрахунків:

Геометричні параметри зони огляду наведено на рис. 3.1.



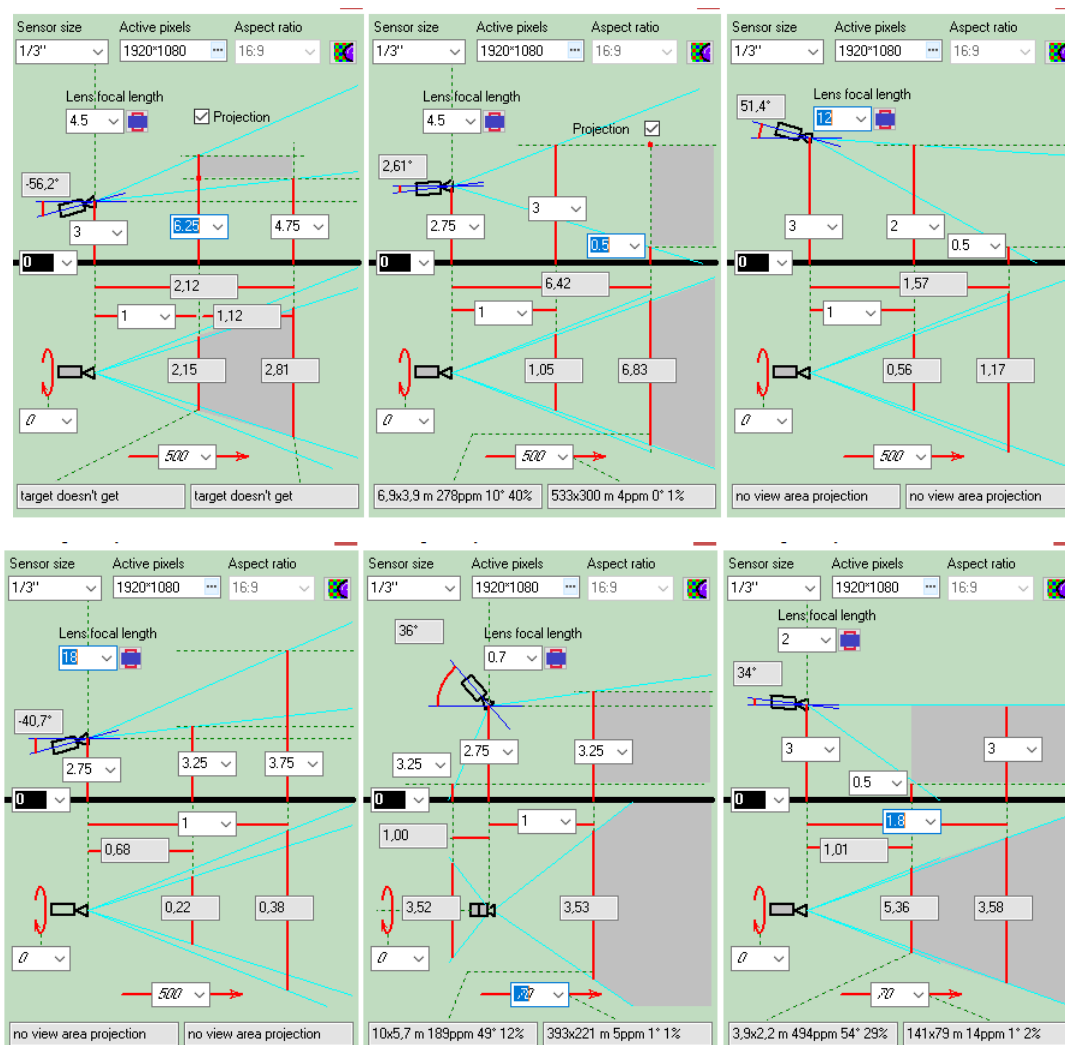


Рисунок 3.1 – Розрахунок та візуалізація зони огляду камери

Розрахунок відсотків від розміру дисплея, кількості пікселів та міліметрів.

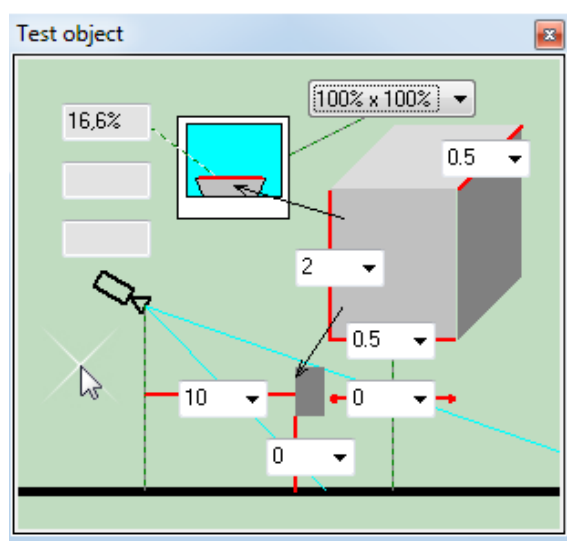


Рисунок 3.2 – Розмір зображення на дисплеї:

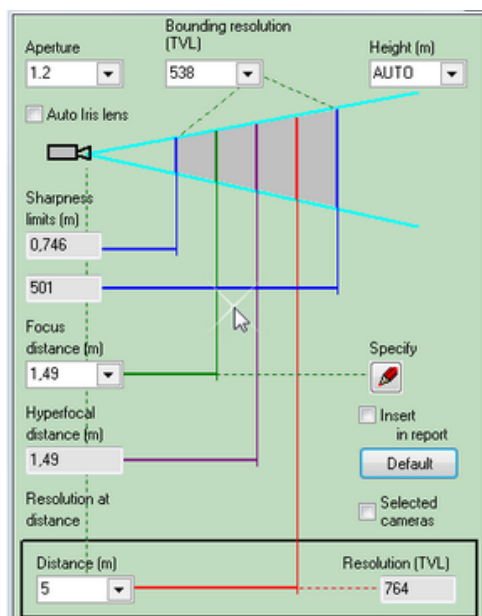


Рисунок 3.3 – Глибина різкості

Cable brand	Twisted pair	Conductor cross-section area (mm ²)	0.75
Total length of all segments in layouts (m)	0	Conductor diameter (mm)	0.98
Reserve for cable laying (%)	10	AWG	
Reserve for camera connection (m)	2	Cable resistance (Ohm) (both directions)	0.209
Reserve for source connection (m)	2	Voltage at cable start (V)	12
Cable length including reserves (m)	4	Consumption current (A)	0.417
Cable coil size (m)	250	Quantity of cameras	1
Cable coil number	1	Voltage at cable end (V)	11.9
Cable surplus (m)	246		

OK Cancel Help

Рисунок 3.4 – Довжина та електричні параметри кабелів:

LAMP Lamp type Incandescent (Tc=2850K) Light efficiency (lm/watt) 12 Spectral efficiency of radiation IT CCD ExView Black/white Black/white Color 1.08 1.1 1 Day/night Day/night 1.1 1.12 ☐ Edit		LUMINAIRE Lamp quantity 1 Efficiency factor 0.5 ☐ Omnidirectional light source ☒ Projector Angle of radiation 120 Concentration 0.5 Axial light intensity (cd) 212 Light intensity (cd)
Lamp power (watt) 100 Light flux emitted by lamp (lm) 1000	Illumination at distance Distance (m) 10 Illumination (lux) 2.12	

OK Help

Рисунок 3.5 – Освітленість

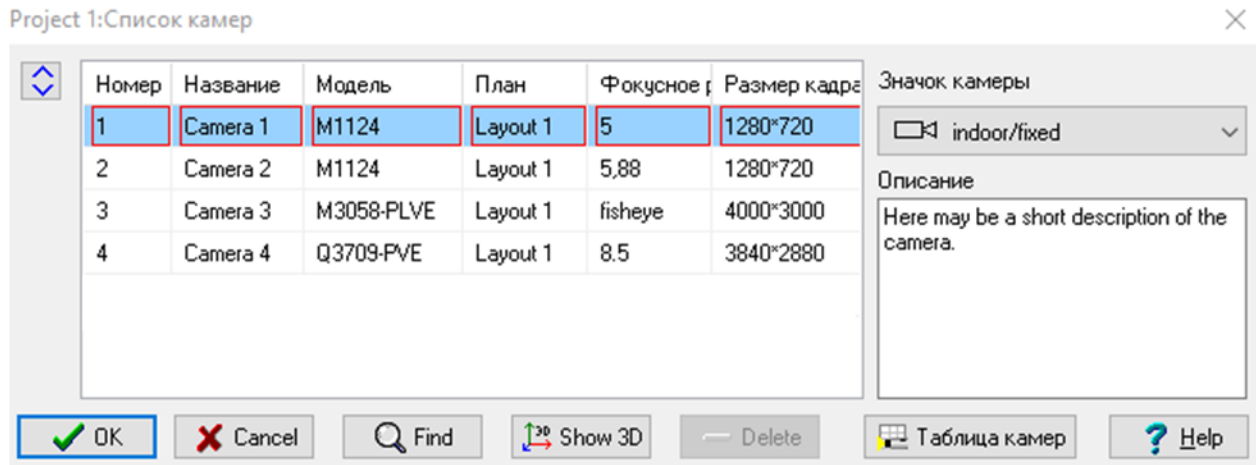


Рисунок 3.6 – Внесення змін до проєкту та додавання камер

Використання 2D/3D-конструкцій.

За допомогою програмного забезпечення можна створити модель системи відеоспостереження, враховуючи плани приміщень та необхідне обладнання. Інтерфейс дозволяє використовувати різні пристрої та інструменти для точного розміщення камер, з можливістю створення до 10 макетів у кожному проєкті та необмеженої кількості шарів.

Висновки до розділу 3

Для проєктування систем відеоспостереження важливо визначити не тільки кількість і тип камер, а також їх розміщення, зони огляду, фокусну відстань та кількість пікселів на метр, а також розрахувати обсяг відеоархіву і навантаження на мережу.

В даному розділі проведено огляд програмних продуктів, таких як: VideoCAD, IP Video System Design Tool (JVSG), Pelco 3D Camera Tool, Axis Camera Extension для SketchUp, Axis Camera Families для Autodesk Revit.

На основі розглянутих властивостей та обраного обладнання в попередніх розділах було обрано саме VideoCAD для створення моделі системи відеоспостереження, що найкраще відображає результати проєктування та

дозволяє перевірити їх адекватність.

Також, у розділі було визначено геометричні параметри зон огляду камер, розміри зображення на дисплеї, глибину різкості, довжини кабелів та освітленість.

4 РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ

4.1 Розподіл адресного простору

У попередніх розділах випускної кваліфікаційної роботи успішного спроектовано всі необхідні компоненти телекомунікаційної мережі та обрано все необхідне обладнання. Отже, наступним кроком є моделювання мережі підприємства за допомогою віртуальних додатків.

Серед численних програм для створення мереж, лідирують Packet Tracer від Cisco та OpNet. Packet Tracer частково безкоштовний, але охоплює переважно обладнання Cisco, тоді як OpNet дозволяє моделювати пристрої інших компаній. Для проектування мережі обрано Cisco Packet Tracer через його простоту у використанні. При реалізації телекомунікаційної інфраструктури комплексної системи охорони ШУ Покровське в модельному середовищі Cisco Packet Tracer будуть застосовані лише фрагменти мережі через обмеженість обладнання та складність реалізації повної схеми разом з усіма налаштуваннями, але це дасть можливість перевірити працездатність та функціональність запропонованих рішень [25].

Для правильної структуризації мережі існує кілька простих методик, які передбачають використання окремого адресного діапазону для кожної групи мережі. Ізоляція мереж досягається за допомогою VLAN, брандмауера та матриці привілеїв для обмеження списків ACL. Це реалізується через маршрутизатори та комутатори. Найдоступніший і найменш витратний метод — використання VLAN [26].

Для побудови мережі використовуються групи віртуальних локальних підмереж, а обладнання розподіляється за типами, обмежуючи доступ лише до певних сервісів (див. табл. 4.1). У кожній VLAN використовується унікальний адресний простір, а маршрутизатор забезпечує обмеження доступу. Служба

DHCP реалізована через спеціальний сервер. Інформація про поділ адресного простору наведена в таблиці 4.2.

Таблиця 4.1 – Матриця привілеїв для обмеження списків ACL

VLAN	Name	Інтернет	файловий сервер	сервер спостереження
101	detect	-	-	+
102	client	+	+	-
103	camera	-	-	+

Таблиця 4.2 – Мережні адреси до відповідних VLAN

VLAN	Name	Мережа	Маска
101	Detect	192.168.0.128	25
102	Client	192.168.0.256	24
103	Camera	192.168.0.32	27

4.2 Розробка імітаційної моделі та налаштування основних параметрів

Для моделювання мережі буде використано емулятор Cisco Packet Tracer. Вибір технологій здійснюється з урахуванням відстані лінії зв'язку. Модель мережі у Packet Tracer містить такі елементи:

1. Мережа IP-камер.
2. Мережа персональних комп'ютерів.
3. Мережа Інтернет.

Компоненти мережі:

1. Головний комутатор, з'єднаний з Інтернетом через оптичне волокно та технологію GigabitEthernet, підключений до комутаторів АПК, серверів підприємства та комутатора.
2. Комутатори, підключені до маршрутизаторів мережі через виту пару типу TX-Base100.
3. Вісім персональних комп'ютерів операторської мережі,

розподілених за віртуальними інтерфейсами (7 до комутатора 2-го рівня, 1 до комутатора 3-го рівня).

4. Чотири IP-камери для відеоспостереження.

Обладнання мережі Інтернет:

1. Маршрутизатор для виходу в мережу Інтернет.
2. Сервер зовнішнього типу для відкритих ресурсів мережі Інтернет.
3. Персональний комп'ютер для зовнішнього користувача мережі Інтернет.

Інтернет.

Результат побудови фрагменту проєктованої мережі представлено на рисунку 4.1.

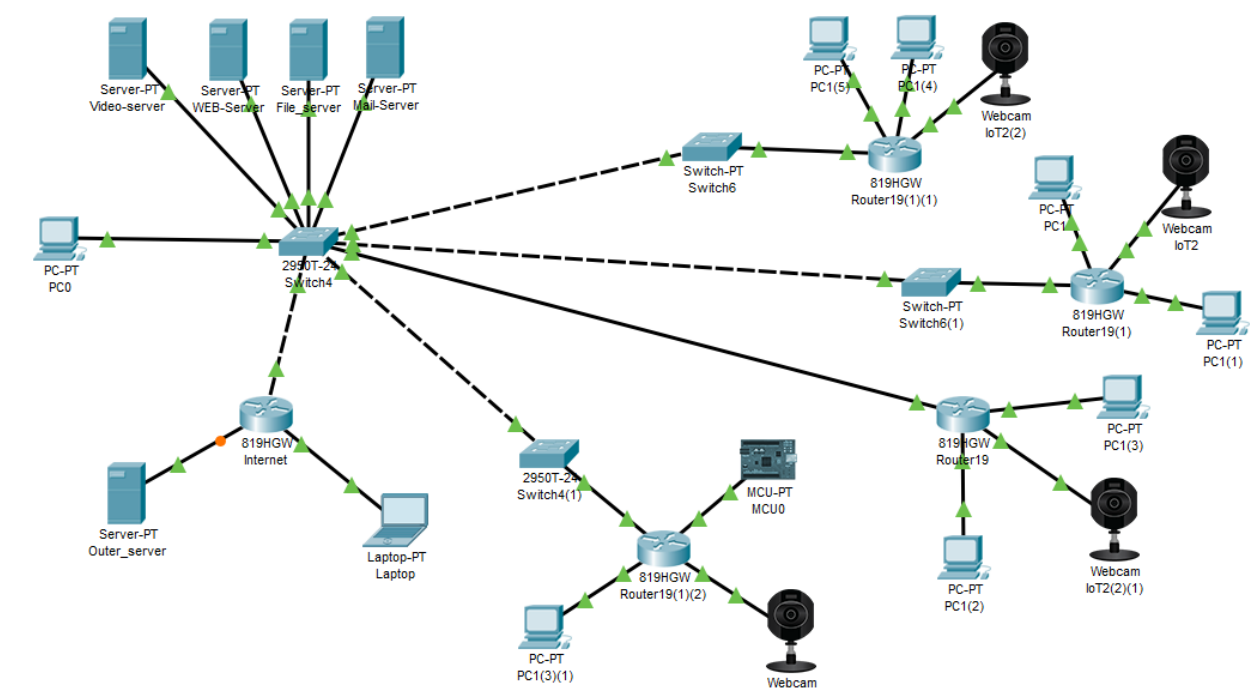


Рисунок 4.1 – Фрагмент проєктованої мережі

В проєктованій мережі всі конфігураційні налаштування мають в деякому виді ідентичні команди, тому розглянуто приклад налаштувань для одного типу конфігурації. Наприклад, налаштування VLAN 101:


```

Switch>en
Switch#conf
Switch#configure t
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 101
Switch(config-vlan)#ex
Switch(config)#int fa1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 101
Switch(config-if)#ex

```

DHCP:

```

Switch(config)#ip routing
Switch(config)#ip dh
Switch(config)#ip dhcp pool vl01
Switch(dhcp-config)#network 192.168.0.128 255.255.255.128
Switch(dhcp-config)#de
Switch(dhcp-config)#default-router 192.168.0.129
Switch(dhcp-config)#ex
Switch(config)#ip dhcp excluded-address 192.168.0.129 192.168.0.130 // 1 додаткову адресу
залишимо для налаштування access листів.

```

Таблиця прав доступу має вигляд (див. табл. 4.3).

Таблиця 4.3 – Відповідні права доступу до серверів і виходу в мережу інтернет

Обладнання	WEB сервер	Файловий сервер	Поштовий сервер	Сервер відеоспостереження	Інтернет
Відеокамери	-	-	-	+	
Датчики	-	+	-	-	-
Робочий персонал	+	+	+	-	+
Охорона	+	+	+	+	-
Адміністратор	+	+	+	+	-

Приклад конфігурації маршрутизатора внутрішніх служб:

```

Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#acc 122 permit ip 192.168.0.128 0.0.0.127 host 10.0.7.83
Router(config)#acc 122 deny ip 192.168.0.128 0.0.0.127 host 10.0.7.84
Router(config)#acc 122 deny ip 192.168.0.128 0.0.0.127 host 10.0.7.82
Router(config)#acc 122 deny ip 192.168.0.128 0.0.0.127 host 10.0.7.85
Router(config)#acc 122 deny ip 192.168.0.128 0.0.0.127 host 210.210.2
Router(config)#acc 122 permit ip any any
Router(config)#int gig0/0
Router(config-if)#ip access-group 122 in
Router(config-if)#ex

```

Приклад конфігурації виходу в мережу Інтернет наступний:

```

Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip nat inside
Router(config-if)#int gig0/0
Router(config-if)#ip nat outside
Router(config-if)#ex
Router(config)#ip access-list standard NatIntOne
Router(config-std-nacl)#permit 10.0.0.0 0.0.7.255
Router(config-std-nacl)#ex
Router(config)#ip nat pool Pool 210 210.210.2.2 210.210.2.50 netmask 255.255.2255.0
Router(config)# ip nat inside source list NatIntTwo interface gig0/0 overload
Router(config)#ex

```

4.3 Реалізація системи захисту телекомунікаційної інфраструктури

Враховуючи заплановане обладнання, необхідно створити схему моделі для встановлених датчиків. Ця модель не обов'язково повинна охоплювати кожен окремий датчик через їх велику кількість, але вона повинна чітко

продемонструвати принцип їх роботи та підключення до локальної мережі. Модель повинна відображати основні компоненти системи, зокрема, як датчики взаємодіють з іншими елементами мережі та передають дані. Це дозволить зрозуміти загальну структуру і функціональність системи, що відображено на рисунку 4.2 [27-28].

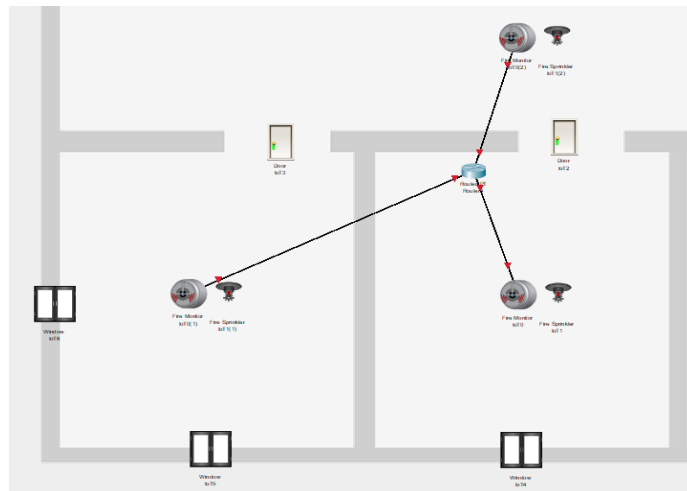


Рисунок 4.2 – Розміщення датчиків пожежної безпеки

Основний комплект обладнання для забезпечення пожежної безпеки включає кілька ключових компонентів:

Датчик вогню: Цей датчик є основним засобом виявлення пожежі або диму в кімнаті. Як тільки він фіксує підвищення температури або наявність диму, датчик миттєво активується.

Розприскувач: Після активації датчика вогню, він відправляє сигнал до розприскувача, який починає розпорошувати воду або іншу пожежогасильну речовину для зупинення розповсюдження вогню.

При виявленні вогню або диму, датчик вогню відправляє сигнал до розприскувача, який автоматично вмикається. Одночасно активується сирена, яка повідомляє про виникнення пожежі. Вимкнути сирену можна лише за допомогою керуючого комп'ютера, що забезпечує централізоване управління системою.

Першим кроком є налаштування протоколу DHCP на сервері. DHCP

(Dynamic Host Configuration Protocol) є мережевим протоколом, що дозволяє пристроям автоматично отримувати IP-адресу та інші необхідні параметри для роботи в мережі TCP/IP. Цей протокол працює за моделлю "клієнт-сервер", де сервер DHCP надає конфігураційні дані клієнтам [28].

Процедура налаштування протоколу DHCP включає:

1. Запуск сервера DHCP: Сервер DHCP налаштовується на автоматичне призначення IP-адрес кожному пристрою в мережі.
2. Аутентифікація пристроїв: Кожен пристрій системи підключається до DHCP і проходить процедуру аутентифікації, отримуючи унікальну IP-адресу та інші мережеві параметри.
3. Підключення до комутаторів: Усі пристрої в кожній кімнаті підключаються до окремого комутатора. На комутаторах здійснюються відповідні налаштування для забезпечення коректної роботи мережі.
4. З'єднання комутаторів: Комутатори різних кімнат з'єднуються між собою та з сервером для забезпечення централізованого контролю та управління.

Ця схема підключення дозволяє ефективно керувати системою пожежної безпеки, забезпечуючи надійне виявлення та реагування на пожежі. Алгоритм налаштування протоколу DHCP та детальна схема роботи системи наведені на рисунку 4.3.

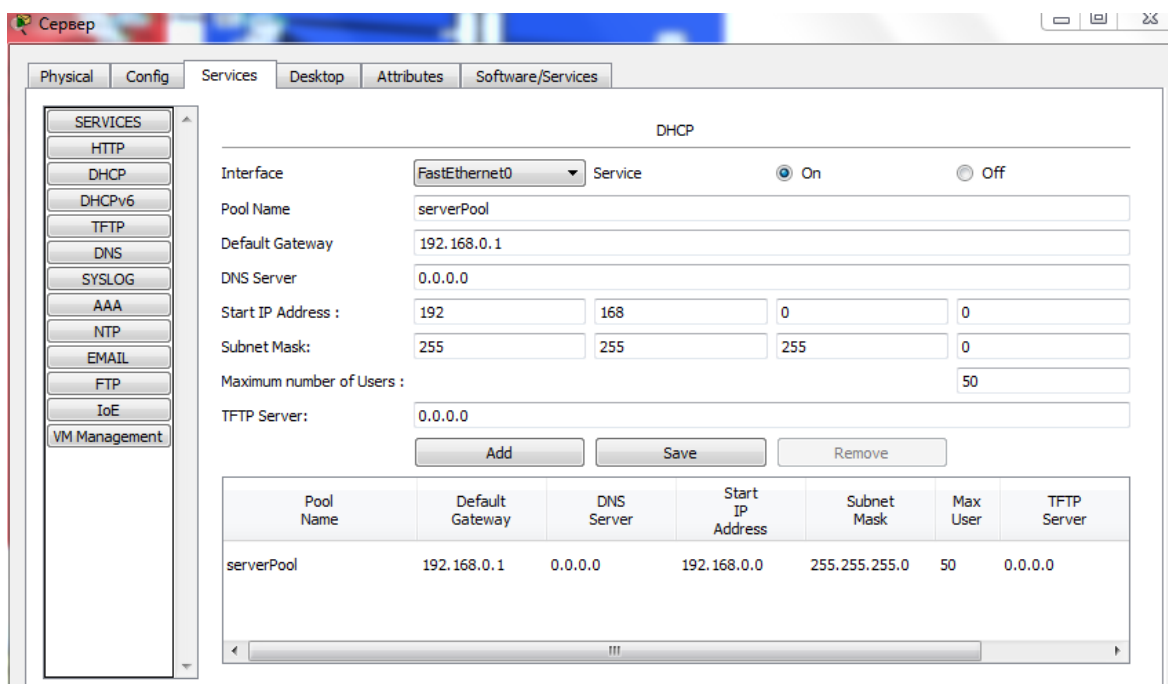


Рисунок 4.3 – Алгоритм налаштування протоколу DHCP

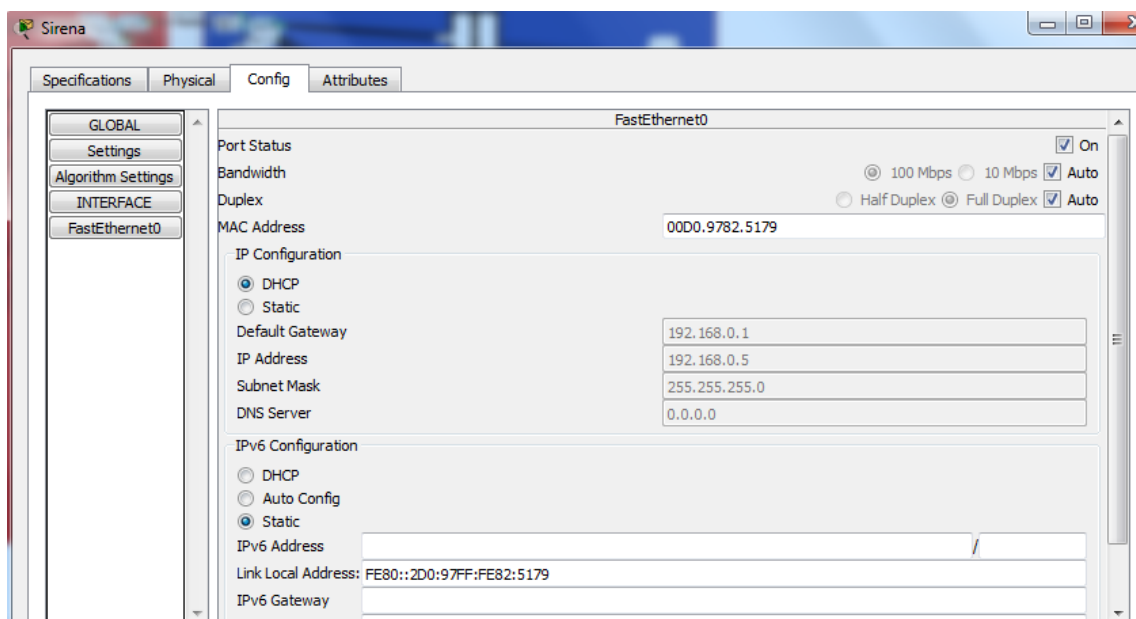


Рисунок 4.4 – Алгоритм підключення кінцевих пристроїв

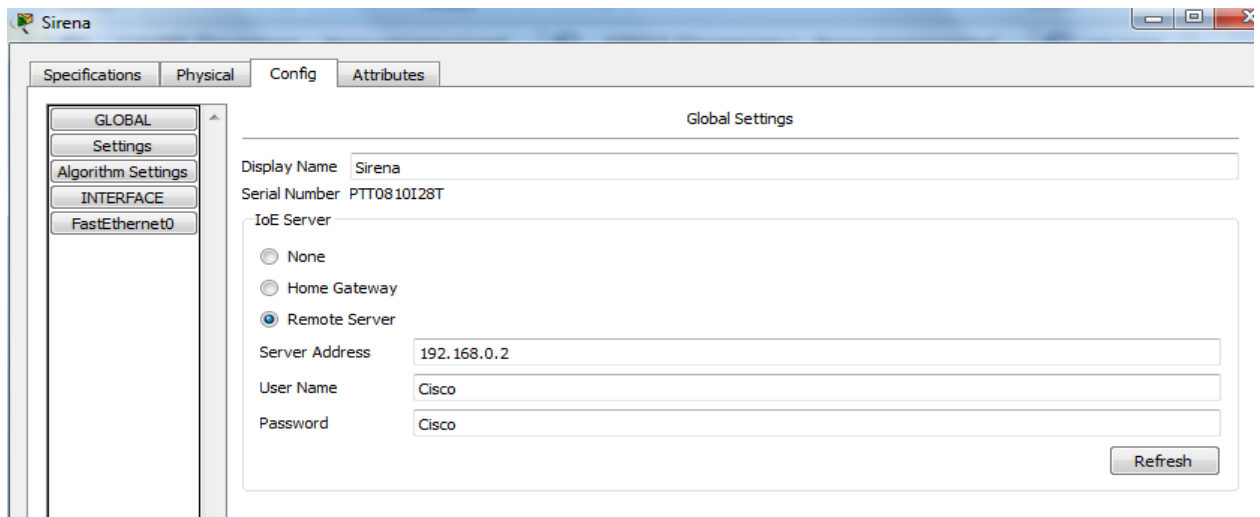


Рисунок 4.5 – Конфігурація алгоритму аутентифікації

Для забезпечення правильної роботи системи пожежної безпеки необхідно налаштувати алгоритми функціонування кожного пристрою на сервері. Це включає налаштування параметрів для датчиків вогню, розприскувачів та сирен, щоб вони ефективно працювали у разі виникнення пожежі.

На рисунку 4.6 наведені налаштування алгоритму дій системи пожежної безпеки при виявленні займання. Ці налаштування включають:

1. Активацію датчиків вогню: Датчики повинні негайно реагувати на наявність диму або підвищення температури.
2. Включення розприскувачів: Після отримання сигналу від датчиків вогню, розприскувачі повинні автоматично розпилювати воду або іншу пожежогасильну речовину для зупинення поширення вогню.
3. Запуск сирен: Одночасно з включенням розприскувачів повинні активуватися сирени, які сигналізуватимуть про небезпеку.
4. Налаштування пристроїв у кожній кімнаті є однаковими, що забезпечує уніфіковану та ефективну роботу системи в усьому будинку. Це дозволяє легко підтримувати систему та здійснювати моніторинг її стану.

Окрім цього, сервер має бути налаштований на автоматичне призначення IP-адрес кожному пристрою через протокол DHCP, що забезпечує надійне підключення та аутентифікацію всіх компонентів системи. Кожен пристрій підключається до окремого комутатора, який потім з'єднується з іншими

комутаторами та сервером, формуючи єдину мережу для централізованого управління та контролю.

Edit Rule [X]

Name

Enabled ☒

If:

Match All + Condition + Group

DatchukVogn`u Fire Detected is true -

Then set:

Poliv Status to true -

Sirena On to true -

+ Action

OK Cancel

Рисунок 4.6 – Конфігурація алгоритму роботи системи пожежної безпеки

Таким чином, налаштування алгоритмів роботи на сервері та однаковість конфігурацій для всіх пристроїв гарантують надійне функціонування системи пожежної безпеки в усіх приміщеннях. Алгоритм налаштування та принцип роботи системи детально показані на рисунку 4.6.

Для коректної роботи системи охоронної сигналізації на сервері треба здійснити відповідні налаштування алгоритму роботи кожного пристрою [27-28].

На рисунку 4.7 приведені налаштування алгоритму роботи сирени у випадку зламу. Налаштування для сирени кожної кімнати є ідентичними.

Edit Rule

Name:

Enabled: ☒

If:

Match:

DatchukRuhu	On	is	true	-
Door	Lock	is	Lock	-
Window	On	is	false	-

Then set:

Sirena	On	to	true	+ Action
Lampa	Status	to	On	-
Camera	On	to	true	-

Рисунок 4.7 – Конфігурація алгоритму роботи сирени

Висновки до розділу 4

У даному розділі роботи було детально розглянуто процес реалізації системи захисту телекомунікаційної інфраструктури підприємства. Основні висновки можна підсумувати наступним чином:

Успішно спроектовано всі необхідні компоненти телекомунікаційної мережі та обрано відповідне обладнання.

Для моделювання мережі підприємства використано Cisco Packet Tracer, який надає прості у використанні інструменти для проєктування та тестування мережеских рішень.

Застосовано методологію розподілу мережі на віртуальні локальні підмережі (VLAN) для забезпечення ізоляції та підвищення безпеки. Це рішення дозволяє обмежити доступ до ресурсів мережі за допомогою брандмауера та списків контролю доступу (ACL).

У кожній VLAN використано унікальний адресний простір, що забезпечує ефективне управління та безпеку мережі. DHCP-сервер надає автоматичне призначення IP-адрес і мережеских параметрів.

Модель мережі у Cisco Packet Tracer включає мережі IP-камер, персональних комп'ютерів та Інтернету.

Налаштовано протокол DHCP на сервері для автоматичного призначення IP-адрес і аутентифікації пристроїв. Кожен пристрій підключений до окремого комутатора, що забезпечує надійне функціонування мережі.

Продемонстровано приклади налаштувань VLAN, включаючи таблицю прав доступу до серверів і Інтернету.

Для забезпечення пожежної безпеки розроблено модель, яка включає датчики вогню, розприскувачі та сирени. При виявленні пожежі датчики автоматично активують розприскувачі та сирени, які сигналізують про небезпеку.

Налаштовано протокол DHCP для підключення та аутентифікації всіх компонентів системи пожежної безпеки.

Всі пристрої підключені до окремих комутаторів, які забезпечують централізоване управління та моніторинг стану системи.

Розроблено та налаштовано алгоритм роботи сирен у випадку зламу. Налаштування для кожної кімнати є однаковими, що забезпечує уніфіковану роботу системи в усіх приміщеннях.

Загалом, реалізація системи захисту телекомунікаційної інфраструктури підприємства включає комплексні налаштування мережевих і безпекових компонентів, що забезпечує ефективну та безперебійну роботу всієї системи.

ВИСНОВКИ

У ході написання випускної кваліфікаційної роботи були успішно спроектовані та реалізовані всі необхідні компоненти телекомунікаційної інфраструктури для забезпечення комплексної системи охорони на підприємстві шахтоуправління «Покровське».

В першому розділі розглянуто аналіз об'єкту, яким виступає Шахтоуправління «Покровське» - найбільше підприємством з видобутку коксівного вугілля в Україні, з високим рівнем технологічного оснащення та безпеки.

Визначено основні задачі та вимоги до комплексної системи охорони, включаючи запобігання несанкціонованому проникненню, охорону майна, контроль доступу, візуальне та аудіоспостереження, а також пожежну безпеку.

Здійснено аналіз і вибір сучасного обладнання для забезпечення безпеки та контролю, зокрема цифрові IP-камери, системи відеоспостереження, датчики руху та пожежної сигналізації.

У другому розділі роботи проведене аналітичне проектування, обрано та розміщено відповідне обладнання для системи відеоспостереження, контролю доступу, охорони периметру та приміщень, а також пожежної безпеки. Використано купольні та вуличні камери Hikvision для забезпечення якісного відеоспостереження. Для побудови системи контролю доступу застосовано контролер Suprema CoreStation CS-40, зчитувачі XPass D2 та зчитувачі відбитків пальців Hikvision. Забезпечено охорону периметру за допомогою радару Hikvision та вібраційно-оптичної системи. Розроблено план розташування обладнання, що забезпечує ефективний захист об'єкта та високу функціональність системи.

У третьому розділі здійснено проектування системи відеоспостереження, проведено огляд програмних продуктів для моделювання систем відеоспостереження, включаючи VideoCAD, IP Video System Design Tool (JVSG),

та інші. Обрано VideoCAD як основний інструмент для створення моделі системи відеоспостереження, що дозволяє точно відображати результати проектування та перевіряти їх адекватність. Визначено геометричні параметри зон огляду камер, розміри зображення на дисплеї, глибину різкості, довжини кабелів та освітленість.

В четвертому розділі роботи показана реалізація системи захисту телекомунікаційної інфраструктури з використанням Cisco Packet Tracer для моделювання мережі підприємства, з огляду на простоту використання та можливість тестування мережевих рішень. Застосовано методологію розподілу мережі на VLAN для забезпечення ізоляції та підвищення безпеки, а також використано унікальний адресний простір для кожної VLAN. Налаштовано протокол DHCP для автоматичного призначення IP-адрес і аутентифікації пристроїв, що забезпечує централізоване управління та моніторинг системи.

Розроблено та налаштовано модель системи пожежної безпеки, включаючи датчики вогню, розприскувачі та сирени, що забезпечують ефективне реагування на пожежі.

Результати роботи показують, що проектування та реалізація комплексної системи охорони для ШУ «Покровське» забезпечують високий рівень безпеки та ефективний контроль за об'єктом. Використання сучасного обладнання та програмних продуктів дозволяє створити надійну телекомунікаційну інфраструктуру, що може адаптуватися до змінюваних умов та потреб об'єкта. Це забезпечує не лише реагування на поточні загрози, але й прогнозування потенційних ризиків, гарантуючи високий рівень захисту та безпеки підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шахтоуправління «Покровське» [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A8%D0%B0%D1%85%D1%82%D0%BE%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%C2%AB%D0%9F%D0%BE%D0%BA%D1%80%D0%BE%D0%B2%D1%81%D1%8C%D0%BA%D0%B5%C2%BB. – Назва з екрану.
2. Інформаційна безпека підприємства [Електронний ресурс]. – Режим доступу: <https://iitd.com.ua/news/shho-take-informacijna-bezpeka-pidpriiemstva-ta-jaki-osnovni-zasadi-zahistu-danih-isnujut/>. – Назва з екрану.
3. UNICOM. Рішення [Електронний ресурс]. – Режим доступу: https://el-sys.com.ua/solution_5 – Назва з екрану.
4. H.265 vs H.264 [Електронний ресурс]. – Режим доступу: <https://vkursi.in.ua/h-265-vs-h-264-porivniannia-formativ-video-shcho-take-hevc-ta-avc/> – Назва з екрану.
5. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.
6. Види камер для відеоспостереження: форм-фактор та технології передачі сигналу [Електронний ресурс]. – Режим доступу: <https://control.ua/ua/blog/vidy-kamer-dlya-videonablyudeniya-form-faktor-i-tehnologii-peredachi-signala.html> – Назва з екрану.
7. Hikvision Digital Technology Co., Ltd. Hikvision Product Specifications [Електронний ресурс]. – Режим доступу: <https://www.hikvision.com>. – Назва з екрану.
8. Hikvision Digital Technology Co., Ltd. Hikvision AcuSense Technology Overview [Електронний ресурс]. – Режим доступу: <https://www.hikvision.com>. – Назва з екрану.
9. Suprema Inc. CoreStation CS-40 Product Manual [Електронний ресурс]. – Режим доступу: <https://www.supremainc.com>. – Назва з екрану.

10. Вуличний зчитувач XPass D2 [Електронний ресурс]. – Режим доступу: <https://supremainc.com.ua/suprema-xpass-d2-rfid-zchytuvach-nfc-i-ble/>. – Назва з екрану.
11. DS-K1201AEF Зчитувач відбитків пальців [Електронний ресурс]. – Режим доступу: https://hik.ua/index.php?route=product/product&product_id=2517 – Назва з екрану.
12. Турнікет TISO CENTURION-M [Електронний ресурс]. – Режим доступу: <https://securitylab.com.ua/tiso-centurion-shlifovannaya-nerzhaveyka/>. – Назва з екрану.
13. Ukrainian State Construction Standards. DBN V.2.5-56:2014. Fire Safety Systems [Електронний ресурс]. – Режим доступу: <https://www.minregion.gov.ua>. – Назва з екрану.
14. DoorProtect Fibra [Електронний ресурс]. – Режим доступу: <https://ajax.systems.ua/products/doorprotect-fibra/>. – Назва з екрану.
15. TVF-VOC-Z8 8-и зонний вібраційно-оптичний охоронний прилад [Електронний ресурс]. – Режим доступу: <https://shop-security.com.ua/tvf-voc-z8-8-i-zonnij-vibratsijno-optichnij-ohoronnij-prilad/> – Назва з екрану.
16. Датчик пожежний димовий Артон СПД-3.2 (НЗ) [Електронний ресурс]. – Режим доступу: <https://ohrana.ua/uk/datchiki/spd-3-2.html>. – Назва з екрану.
17. International Organization for Standardization. ISO/IEC 27001:2013 Information Security Management [Електронний ресурс]. – Режим доступу: <https://www.iso.org>. – Назва з екрану.
18. National Institute of Standards and Technology (NIST). NIST Cybersecurity Framework [Електронний ресурс]. – Режим доступу: <https://www.nist.gov>. – Назва з екрану.
19. SANS Institute. SANS Security Policy Templates [Електронний ресурс]. – Режим доступу: <https://www.sans.org>. – Назва з екрану.
20. Tiras-16.128 P. Fire Alarm Control Panel User Manual [Електронний ресурс]. – Режим доступу: <https://www.tiras.com.ua>. – Назва з екрану.

21. VideoCAD. VideoCAD Professional User Guide [Электронный ресурс]. – Режим доступа: <https://www.cctvcad.com>. – Назва з екрану.
22. JVSG. IP Video System Design Tool User Guide [Электронный ресурс]. – Режим доступа: <https://www.jvsg.com>. – Назва з екрану.
23. VELKOM. VELKOM Security Solutions Overview [Электронный ресурс]. – Режим доступа: <https://www.velkom.com>. – Назва з екрану.
24. Axis Communications AB. Axis Camera Families for Autodesk Revit User Guide [Электронный ресурс]. – Режим доступа: <https://www.axis.com>. – Назва з екрану.
25. Packet Tracer. Network Simulation Tool Documentation [Электронный ресурс]. – Режим доступа: <https://www.packettracer.com>. – Назва з екрану.
26. IEEE Standards Association. IEEE 802.1Q-2018 - Standard for Local and Metropolitan Area Networks [Электронный ресурс]. – Режим доступа: <https://standards.ieee.org>. – Назва з екрану.
27. Cisco Systems, Inc. DHCP Configuration Guide [Электронный ресурс]. – Режим доступа: <https://www.cisco.com>. – Назва з екрану.
28. Cisco Systems, Inc. Cisco Packet Tracer User Guide [Электронный ресурс]. – Режим доступа: <https://www.cisco.com>. – Назва з екрану.

ДОДАТОК А – Розділ охорони праці та пожежна безпека під час
монтажних робіт на промислових підприємствах у галузі зв'язку

Розроблений на підставі Законів України «Про охорону праці», «Про пожежну безпеку» та «Про охорону навколишнього середовища, державних будівельних норм України ДБН А.3.2-2-2009 «Охорона праці і промислова безпека в будівництві», комплекс заходів забезпечує в даному проєкті безпеку будівельно-монтажних робіт і подальшу експлуатацію обладнання комплексної системи.

До початку виробництва будівельних або монтажних робіт робочі майданчики повинні бути забезпечені питною водою, аптечками, засобами для надання першої медичної допомоги, телефонним зв'язком.

На робочих площах повинні бути організовані пожежні пости з протипожежними засобами.

Робочі майданчики повинні бути оснащені сучасною контрольно-вимірною апаратурою.

До робіт з монтажу обладнання та кабельних ліній зв'язку допускаються особи, які досягли 18-річного віку, пройшли медичний огляд, навчені безпечним методам роботи і мають посвідчення про перевірку знань з охорони праці та електробезпеки.

Зазначені особи повинні пройти вступний інструктаж на робочому місці. У бригаді монтажників обов'язково повинне бути присутнім особа, що спостерігає за безпекою виконання робіт. такою особою бажано призначати старшого по бригаді.

До робіт не допускаються працівники, що знаходяться в стані алкогольного або наркотичного сп'яніння.

Виробництво робіт по монтажу обладнання і кабельних ліній зв'язку виробляти в суворій відповідності з нормативними документами:

- НПАОП 0.00-1.15-07 Правила охорони праці під час Виконання робіт на висоті;

- НПАОП 40.1-1.01-97 (ДНАОП 1.1.10-1.01-97) Правила безпечної ЕКСПЛУАТАЦІЇ електроустановок;
- НПАОП 0.00-1.04-07 Правила Вибори та застосування засобів індивідуального захисту органів дихання;
- НПАОП 40.1-1.32-01 (ДНАОП 0.00-1.32-01) Правила будови електроустановок. Електрообладнання спеціальних установок;
- НПАОП 40.1-1.21-98 (ДНАОП 0.00-1.21-98) Правила безпечної експлуатації електроустановок споживачів;
- ДБН В.1.1-7 Пожежна безпека об'єктів будівництва;
- ГОСТ 12.1.030-81 Електробезпека. Захисне заземлення. Занулення.

Основні рішення з промислової безпеки;

- "ССБП. Охорона праці и промислова безпека в будівництві. Основні положення "з урахуванням місцевих умов. Крім того, при розробці розділу використані нормативні документи:
- ГОСТ 12.1.002-84 «Електричні поля промислової частоти допустимі рівні напруженості і вимоги до проведення контролю на робочих місцях»;
- ГОСТ 12.1.005-88 «Загальні санітарно-гігієнічні вимоги до повітря робочої зони»;
- ДСТУ Б А.3.2-13: 2011 Системи стандартів безпеки праці. Будівництво. Електробезпечність. Загальні вимоги (ГОСТ 12.1.013-78, MOD);
- ГОСТ 12.1.030-81 ССБТ. «Електробезпека. Захисне заземлення. Занулення»;
- ГОСТ 12.2.003-91 ССБТ. «Обладнання промислове. Загальні вимоги безпеки»;
- ГОСТ 12.2.007.0-75 * ССБТ. «Вироби електротехнічні. Загальні вимоги безпеки»;
- ДСТУ ІЕС 60745-1: 2010 Інструмент ручний електромеханічний.

Безпека. Частина 1. Загальні вимоги;

- ГОСТ 12.3.032-84 * ССБТ «Роботи електромонтажні. Загальні вимоги безпеки»;
- ГОСТ 12.4.051-87 (СТ РЕВ 5803- 86) ССБТ. «Засоби індивідуального захисту органів слуху»;
- ГОСТ 464-79 «Заземлення для стаціонарних установок проводового зв'язку, радіорелейних станцій, радіотрансляційних вузлів проводового мовлення і антен систем колективного прийому телебачення. Норми опору»;
- ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку»;
- НПАОП 0.00-1.71-13 «Правила охорони праці під час роботи з інструментом та пристроями»;
- НПАОП 40.1-1.21-98 (ДНАОП 0.00-1.21-98) «Правила безпечної експлуатації електроустановок споживачів»;
- НПАОП 64.2-1.07-96 (ДНАОП 5.2.30-1.07-96) «Правила безпеки при роботах на кабельних лініях зв'язку і проводового мовлення»;
- НПАОП 63.12-1.03-96. (ДНАОП 7.1.00-1.03-96) «Правила охорони праці при експлуатації баз, складів і сховищ, виконанні вантажо-розвантажувальних робіт на об'єктах оптової торгівлі».

Існуючі системи опалення та вентиляція повинні відповідати:

ДБН В.2.5-67 «Опалення, вентиляція та кондиціонування» Опалення, вентиляція і кондиціонування ГОСТ 12.1.005-88 «Загальні санітарно-гігієнічні вимоги до повітря робочої зони».

Блискавкозахист будівлі повинна відповідати ДСТУ Б В.2.5-38: 2008 «Інженерне обладнання будинків і споруд. Улаштування блискавкозахисту будівель і споруд »(IE C 62305: 2006, NEQ).

Влаштування заземлення повинно відповідати ГОСТ 12.1.030-81 «ССБТ. Електробезпечність. Захисне заземлення. Занулення».

Розділ з охорони праці.

Повинні бути передбачені необхідні заходи і засоби для забезпечення безпеки і нормальних санітарних умов праці, як при проведенні монтажних робіт, так і при експлуатації комплексної системи безпеки відповідно до нормативних документів:

- Закон України «Про охорону праці»;
- ДСТУ 7238: 2011 Системи стандартів безпеки праці. «Засоби колективного захисту працюючих. Загальні вимоги та класифікація»;
- ДСТУ 7239: 2011 Системи стандартів безпеки праці. «Засоби індивідуального захисту. Загальні вимоги та класифікація»;
- НПАОП 40.1-1.21-98 (ДНАОП 0.00-1.21-98) «Правила безпечної експлуатації електроустановок споживачів»;
- НПАОП 63.12-1.03-96. (ДНАОП 7.1.00-1.03-96) «Правила охорони праці при експлуатації баз, складів і сховищ, виконанні вантажо-розвантажувальних робіт на об'єктах оптової торгівлі».
- НПАОП 64.2-1.07-96 (ДНАОП 5.2.30-1.07-96) «Правила безпеки при роботах на кабельних лініях зв'язку і провідного мовлення»;
- НПАОП 64.2-1.08-96 (ДНАОП 5.2.30-1.08-96) «Правила безпеки при роботах на телефонних і телеграфних станціях»;
- НПАОП 0.00-1.71-13 «Правила охорони праці під час роботи з інструментом та пристроями»;
- НПАОП 40.1-1.07-01 (ДНАОП 1.1.10-1.07-01) «Правила експлуатації електрозахисних засобів»;
- ДСанПіН 3.3.2.007-98 «Державні санітарні правила и норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».

Безпечне обслуговування проєктованого обладнання забезпечується системою заходів, передбачених "Правилами улаштування електроустановок" ПУЕ-2009, ПТЕЕС "Правила технічної експлуатації електроустановок споживачів України".

Протипожежні заходи.

Обслуговуючий персонал зобов'язаний дотримуватися встановленого протипожежного режиму на об'єкті, виконувати встановлені правила і інші нормативні акти з питань пожежної безпеки.

Кожен працівник у разі виявлення пожежі або запаху диму, гару, надмірного підвищення температури зобов'язаний негайно повідомити про це в пожежну охорону (при цьому назвати адресу об'єкта, місце виникнення пожежі, наявність людей, а також повідомити своє прізвище) і вжити заходів щодо його ліквідації та рятування людей і майна.

Основні вимоги щодо пожежної безпеки було встановлено відповідно до НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні», НАПБ В.01.053-2016 / 520 «Правила пожежної безпеки в галузі зв'язку» і ДБН В.1.1-7 «Захист від пожежі. Пожежна безпека об'єктів будівництва».

Протипожежні системи, установки, устаткування будівель, споруд і приміщень (протидимний захист, пожежна автоматика, протипожежне водопостачання, протипожежні двері, клапани, інші захисні пристрої у протипожежних стінах і перекриттях і т.п.) повинні постійно утримуватися в справному стані.

Евакуація здійснюється по шляхах евакуації через евакуаційні виходи. Евакуаційні шляхи в межах приміщення повинні забезпечувати безпечну евакуацію людей через евакуаційні виходи з даного приміщення. Кількість і загальна ширина евакуаційних виходів з приміщень визначаються в залежності від максимально можливого числа евакуйованих через них людей і гранично допустимого відстані від найбільш віддаленого місця можливого перебування людей (робочого місця) до найближчого евакуаційного виходу.

Протидимний захист будівель повинна виконуватися відповідно з ДБН В.2.5-67. Система оповіщення про пожежу повинна виконуватися відповідно з ДБН В.1.1-7, ДБН 2.5-56-2014 і І 220-008-91.

Для прокладки кабелів зв'язку в приміщеннях слід застосовувати кабелі з негорючим покриттям, рекомендовані фірмами виробниками мережного

обладнання.

У приміщеннях, де розташовується телекомунікаційне обладнання, дозволяється зберігати для виробничих потреб не більше 0,15 л бензину, 0,25 л ацетону і 1 л спирту в розрахунку на 100 куб. м об'єму приміщення.

Приміщення, де розташовано телекомунікаційне обладнання, повинні бути обладнані первинними засобами пожежогасіння та протипожежним інвентарем відповідно до встановлених норм згідно НАПБ В.01.053-2016 / 520 "Правила пожежної безпеки в галузі зв'язку". На стіні у вихідній двері приміщення повинен встановлюватися порошковий або вуглекислотний вогнегасник так, щоб відкривається двері не ускладнювала його використання.

ДОДАТОК Б – План шахти

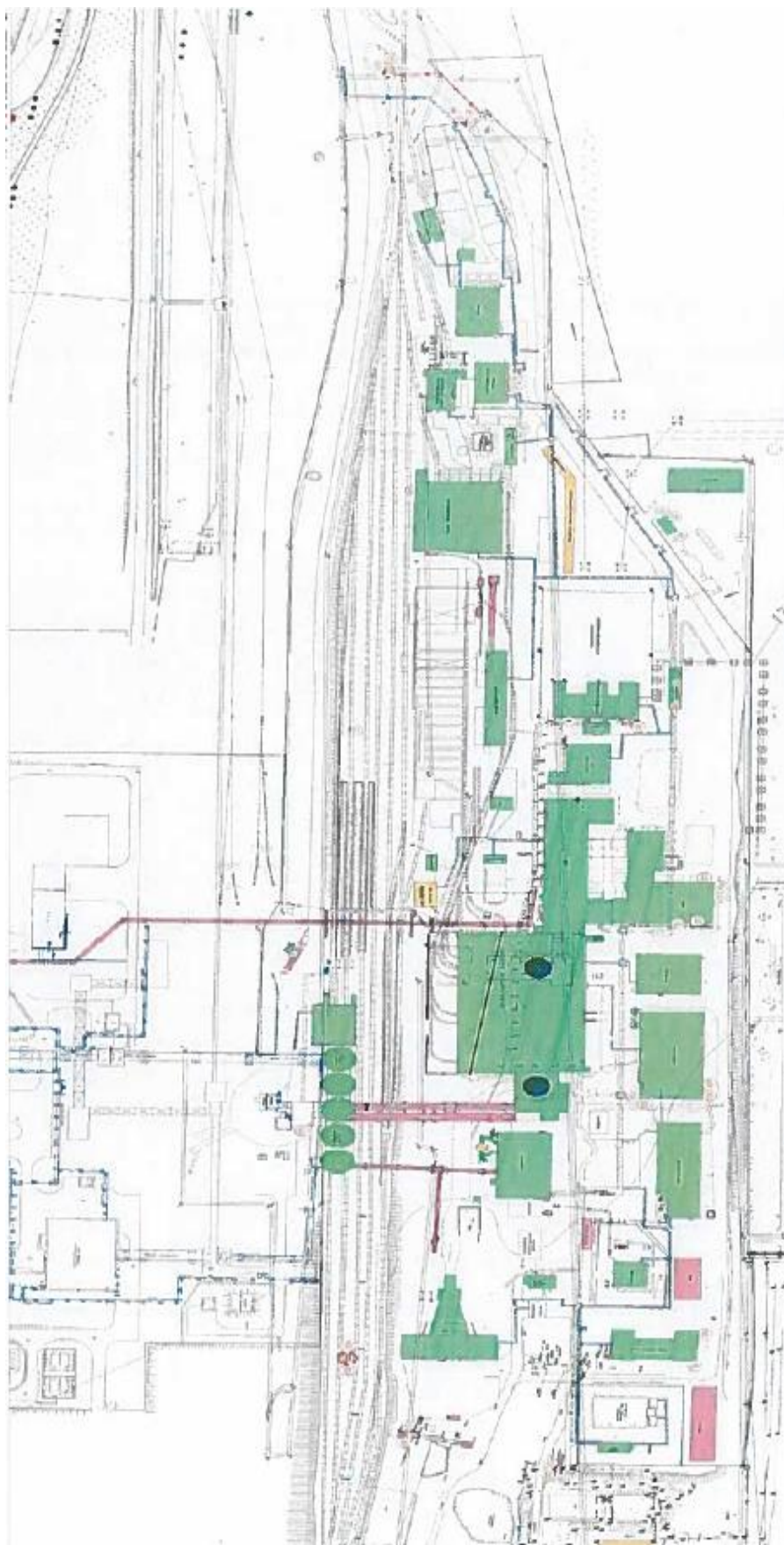


Рисунок Б.1 – План шахти

ДОДАТОК В – План будівлі АПК

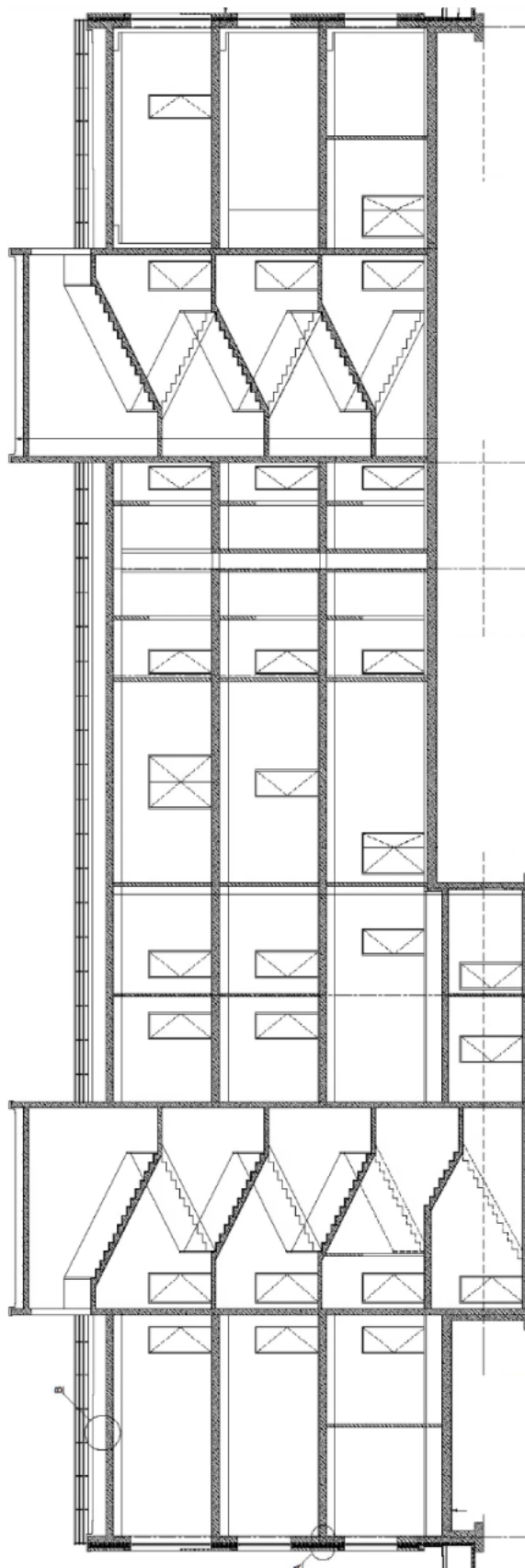


Рисунок В.1 – План будівлі АПК

ДОДАТОК Г – Характеристика приміщень АПК

Таблиця Г.1 – Характеристика приміщень АПК.

№	Назва приміщення	Площа м.кв.	№	Назва приміщення	Площа м.кв.
301	Сходи А	21,8	317	Пом. Директора	17
302	Балкон	8,6	318	Директор	66,8
303	Коридор	61,5	319	Сходи Б	21,8
304	ІТ відділ	31,5	320	Балкон	8,6
305	Серверна	16,8	321	Умивальна	5
306	Бухгалтерія	60	322	Тамбур	2,6
307	Каса	9,8	323	Вбиральня	1,3
308	Глав. Бух	22,4	324	Вбиральня	1,3
309	ЦПВН	22,6	325	Підсобне приміщення	4,6
310	Відділ закупівлі	17,4	326	Вбиральня	1,3
311	Відділ менеджменту	40	327	Вбиральня	1,3
312	Обідня	19,8	328	Тамбур	3,7
313	Переговорна	45,5	329	Умивальна	5,1
314	Приймальна	33,6	330	Актова зала	39,7
315	Підсобне приміщення	9,2	331	Юрист	15
316	Санвузол	7,3	332	Гардеробна	15

Таблиця Г.2 – Характеристика приміщень для розрахунку кількості датчиків.

№	Розміри		Площа (м.кв).	№	Розміри		Площа (м.кв).
	Довжина(м)	Ширина(м)			Довжина(м)	Ширина(м)	
303	38,43	1,6	61,5	317	4,6	3,7	17
304	7,45	4,23	31,5	318	8,96	7,45	66,8
305	6,32	2,66	16,8	321	2,38	2,1	5
306	10	6	60	322	2,4	1	2,6
307	3,34	3	9,8	325	2,2	2,1	4,6
308	6	3,7	22,4	328	2,4	1,54	3,7
309	6	3,8	22,6	329	2,46	2,1	5,1
310	5,7	3	17,4	330	6,6	6	39,7
311	5,7	7	40	331	4,2	3,6	15
312	5,7	3,47	19,8	332	4,23	3,54	15
313	6	6,5	45,5				
314	8,6	3,9	33,6				
315	3,7	2,5	9,2				

ДОДАТОК Д – План приміщень АПК

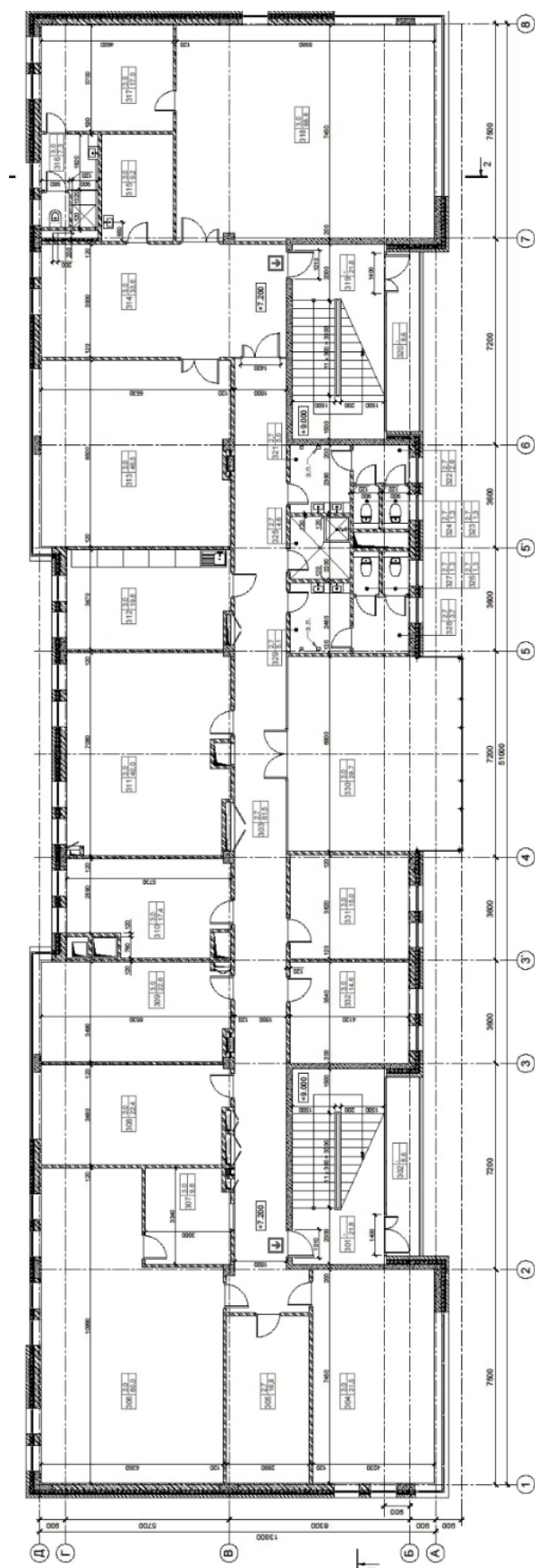


Рисунок Д.1 – План приміщень АПК

ДОДАТОК Е – Планування розташування системи відеоспостереження

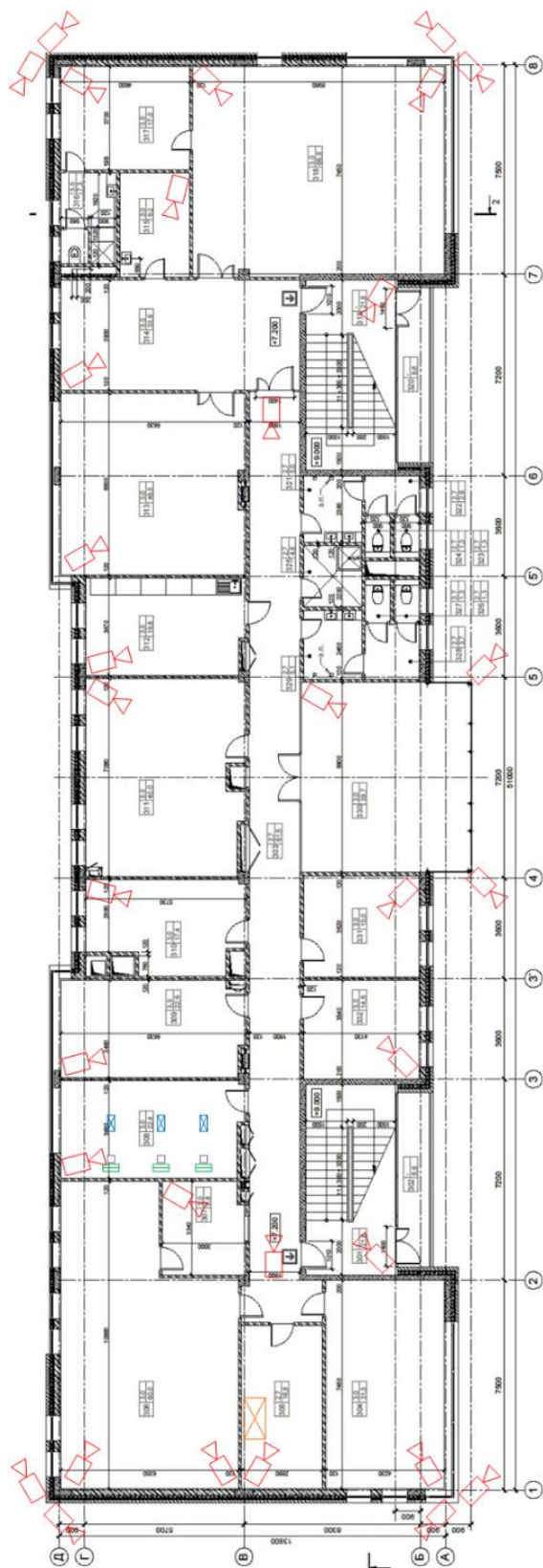


Рисунок Е.1 – Планування розташування системи відеоспостереження

Експлікація до рис.Е.1:

-  – камера відеоспостереження;
-  – реєстратор;
-  – декодер;
-  – комп'ютер;
-  – монітор.

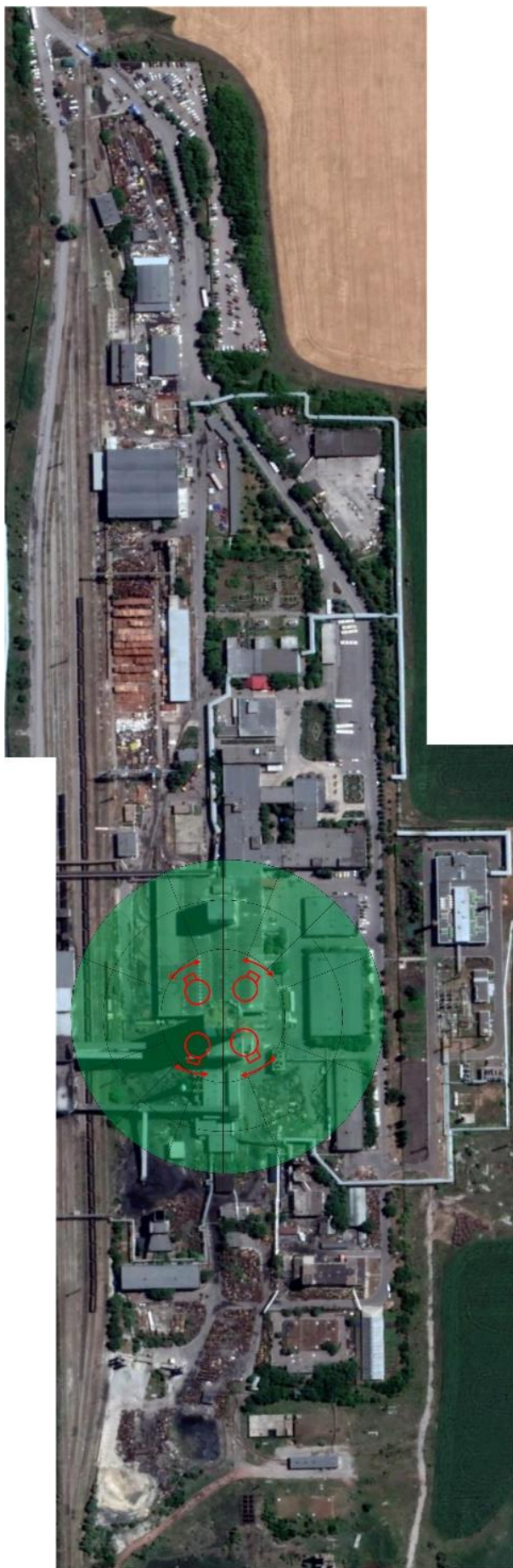


Рисунок Е.2 – План камер для охорони периметру

ДОДАТОК Ж – План розташування елементів СКУД

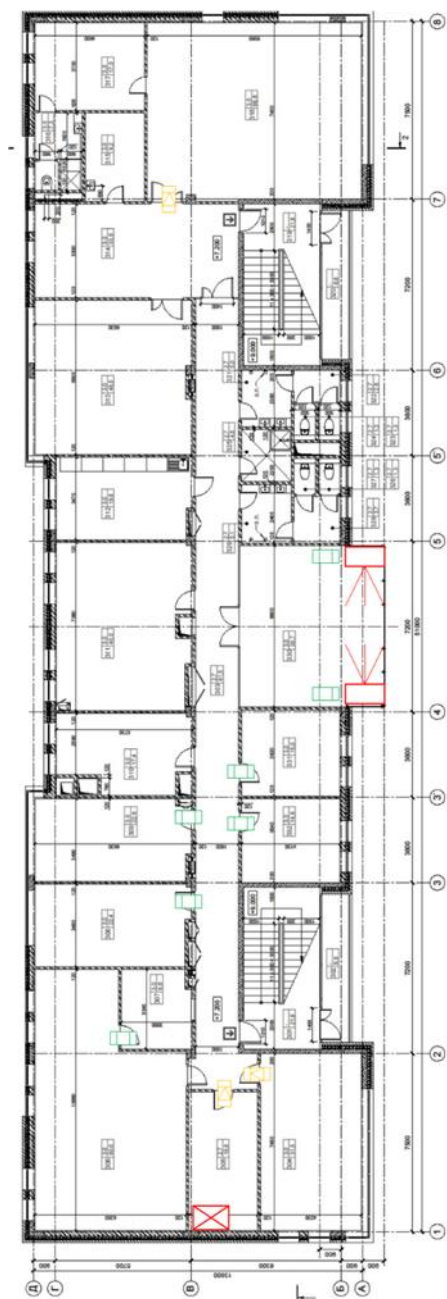


Рисунок Ж.1 – План розташування елементів
СКУД

Експлікація до рис.2.14:

-  – Контролер «CoreStation CS-40»;
-  – Зчитувач «XPass D2»;
-  – Зчитувач з відбитком пальця;
-  – Турнікет.

ДОДАТОК К – План розташування датчиків та ПКП

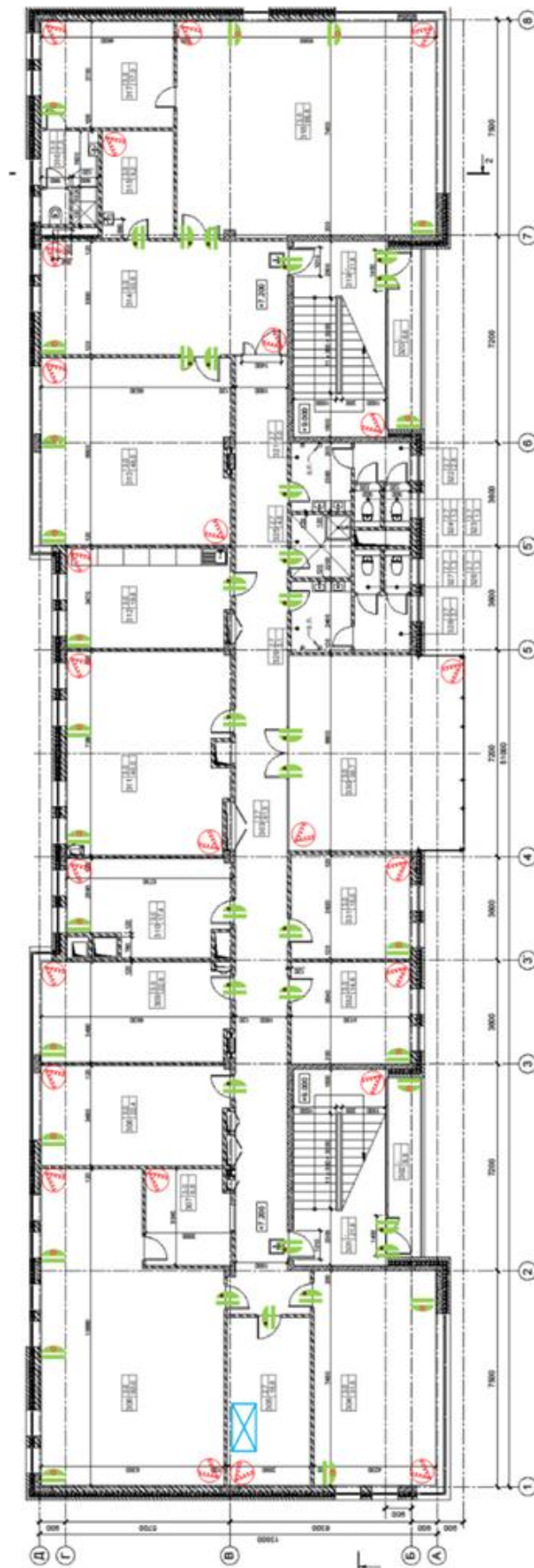


Рисунок К.1 – План розташування датчиків та ПКП

Експлікація до рис.К.1:



– Прилад ПКП;



– Датчик відкриття Ajax DoorProtect Fibra;



– Датчик розбиття Ajax GlassProtect Fibra;



– Датчики руху DS-PDC15-EG2 PIR Detector.

ДОДАТОК Л – План охорони периметру

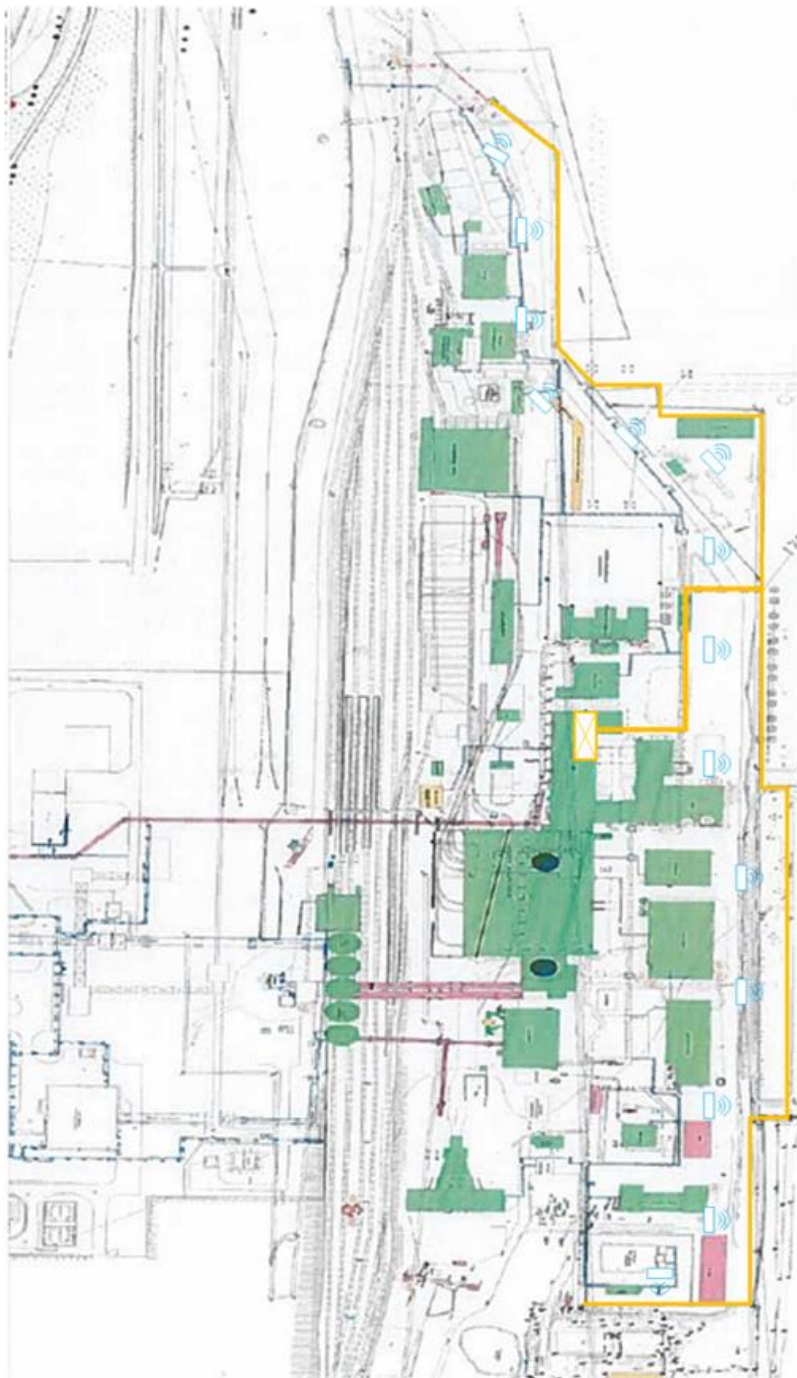


Рисунок Л.1 – План охорони периметру

Експлікація до рис.Л.1:

-  – Вібраційно-оптичний охоронний прилад TVF-VOC-Z8;
-  – Радар Hikvision DS-PRI120;
-  – Лінія ВОЛС.